多面的安全性のための XML によるコンテンツ保護記述

金子 格[†]　　白井 克彦[‡]
[†] 早稲田大学理工学総合研究センター 嘱託
http://www.shirai.info.waseda.ac.jp:8000/~itaru-k/
[‡] 早稲田大学

[要旨]筆者等はデジタル放送、インターネット、コンピュータ等において統合的なデジタル AV サービスを実現する場合に、従来の閉じたシステムから開いたシステムへの転換が必要であり、そのためにコンテンツ保護システムに多面的な安全性が必要と考える。本論文では AV サービスの多面的安全性を定義し、そのために我々が提案している XML によるコンテンツ保護記述方式を示す。現在筆者等はこの方式を MPEG におけるコンテンツ保護フレームワークである MPEG-4/IPMP Extension に提案中である。

Multi-lateral security and Contents Protection using the XML description

Itaru Kaneko[†]　　Katsuhiko Shirai[‡]
[†]Advanced research institute for science and engineering, Waseda University
http://www.shirai.info.waseda.ac.jp:8000/~itaru-k/
[‡] Waseda University

Abstract:.
We think that the transition, from closed system to open system in the converged digital audio-visual system includes Digital Broadcasting, Internet and Computer, requires multilateral security. In this report, we will describe the definition of multilateral security and the XML based contents description for it. Authors are currently proposing this XML based system for the MPEG-4/IPMP Extension currently under developing in MPEG for the next MPEG's content protection framework.

1. はじめに

筆者等はデジタル放送、インターネット、コンピュータ等において統合的なデジタル AV サービスを実現する場合に、従来の閉じたシステムから開いたシステムへの転換が必要であり、そのためにコンテンツ保護システムに多面的な安全性が必要と考える。本報告では AV サービスの多面的安全性を定義し、その実現方法の一つとして、我々が提案している XML によるコンテンツ保護記述方式を示す。

現在(2001 年 6 月時点)ISO/IEC は MPEG-21-マルチメディア・フレームワークの標準化を進めている。またそれと連動して、MPEG におけるコンテンツ保護のフレームワークとして、MPEG-4/IPMP Extension の標準化を進めている。筆者等は NEDO の国際標準化支援プロジェクトの中で MPEG-4/IPMP Extension の検討を行い、XML による記述を MPEG に提案中である。

2. 多面的安全性の必要性

デジタル技術による大規模な AV サービスが現実のものとなろうとしている。デジタル方式の利点には、グローバルネットワーク、ワイヤレスアクセス、デジタル放送等の間で境界なく利用が可能、コンテンツ間の連携も自由に行なえる、などがある。これらのデジタル方式の利点が発揮されるためには、AV サービスのフレームワークが特定サービス内で閉じたシステムではなく、多数のサービスが連携できる開いたシステムとなる必要がある。筆者等は、そのような開いた

システムの実現には、閉じたシステムでは考慮されなかった様々な多面的安全性が必要になると考えている。

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てきた。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すでに数多く実用化され、応用が広がる中で、セキュリティに関する多くの新しい問題が意識されるようになった。たとえば名和[13]がデジタル時代の様々な課題を提示している。森[14]、井上[15]、O Connell[16] 、Lipinski[17] 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も企業活動にとっても重要な課題となった。

3. 多面的安全性が決すべき課題

筆者等が想定する、開いた AV サービスのコンテンツ保護では、一般的には以下の 3 つの面での強化が必要になると考えられる。

(1) グローバル・サービスへの対応
(2) インフラとしての永続性、汎用性
(3) フレキシビリティと拡張性

以下に、筆者等が想定している具体的問題点のいくつかを示す。

3.1. 競争的環境の維持

デジタル AV サービスには新しいビジネスモデルの可能性があり、その発展を抑制すべきではない。一方、ハードとソフトは一方の競争で優位に立てば他方の競争で優位に立てるという関係にあり、互換性の壁を設けることが競争優位に立つ手段になる。競争優位のために安易にシステムを非互換とすることは、技術やサービス品質の向上の妨げになる。従って、競争的環境維持のための互換性維持と、新しいサービス創出の自由度の両立が求められる。

3.2. 消費者保護

消費者が以下のような保証を得られることは常に重要である。

(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

AV サービスにおいては、従量課金や小額課金により、これらの確認がこれまでより煩雑、不透明なものになる可能性があり、何らかの対策が必要である。

3.3. 著作者の保護

コンテンツ保護機能を持った AV サービスでは、いわゆる盗作や無断使用による権利侵害も大きな問題となる可能性がある。サービスの規模拡大と内容の不透明さが、盗作等による権利侵害の発見や対策を困難にする可能性があるためである。

3.4. プライバシー

デジタル AV サービスでは、利用者の利用状況を非常に詳細に記録することが可能である。プライバシー侵害からいかにして消費者を保護するかが、課題となっている。

3.5. 内部不良の防止

筆者等はシステムに内在する不良を「 内部不良」と総称し、これを検出、抑制することも重要であると考える。Landwehr 等はコンピュータシステムにおける過去のセキュリティ不良 50 例を分析し、で仕様と設計の不良が 37(74%)、意図的な不良が 18 例(36%)あったと報告している[18]。Java のセキュリティホールの事例[19][20][21][22]や、Bellovin のコメントも、セキュリティには継続的な検証と修正が重要であることを示唆している。

4. 多面的安全性の形式評価モデル

前節の事例の列挙は、そのままでは技術的に分析可能な達成基準とはならない。本章では Herzberg 等による安全性の形式評価モデルを元に、多面的安全性の形式評価モデルを構築することを試みる。

4.1. Herzberg モデル

Herzberg 等は 1987 年の論文[10]でソフトウエア配信システムの安全性の形式評価モデルを示した。このモデルはデジタルコンテンツの配信システムにもほぼそのまま適用できる。Herzberg は以下の仮定を採用した。(用語はデジタルコンテンツに合わせ読み替えている。)

通信路についての仮定

(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。

システムに関しての仮定

(1) デコーダ内の秘密情報は読めない
(2) デコーダ出力から原コンテンツを復元できない
(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

そして、この条件下で通信路の傍受、改竄により以下を行なうことを攻撃と定義した。

(a) 利用者が許可されないコンテンツを利用する

(b) 正当な利用者以外が成りすましにより、不正な行為を行なう。
(c) コンテンツ提供者が不正を行なう
(d) 正当なコンテンツ提供者以外のものが成りすましにより不正な操作を行なう

Herzberg は、プロトコルに基づくシステムの状態の到達可能性(reacheability)として安全性を定義した。

4.2. 多面的安全性モデルへの拡張

Herzberg はシステムをコンテンツ提供者、利用者、システム管理者という 3 種類の送受信者からなるものとしたが、多面的安全性モデルでは 4 種類の送受信者を想定する。表 1に 4 つの基本的な送受信者を示す。これらと通信路の関係を図 1に示す。楕円はメッセージの送受信者を、矢印は通信を示す。

表1　多面的安全性における送受信者

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

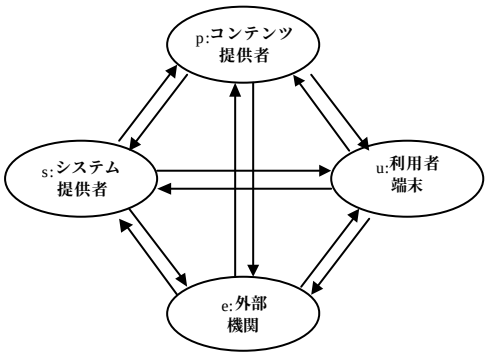

図1 multi-lateral security では 4 つの利害関係者を想定する。

外部機関をモデルに含めたことにより、たとえば著作者の侵害のような、特定のコンテンツの配信に直接関与しなかったものへの権利侵害をモデル化することができる。

Hertzberg モデルではセキュリティ管理者やデコーダに組込まれたプロトコルは無謬であるとした。多面的安全性モデルではこれらを不完全なものとして扱う。

この不完全性をモデル化するために、デコーダに組込まれているセキュリティ実行機能をセキュリティ・クライアント=SC と名付け、それ自体がメッセージとして伝送されるものとする。

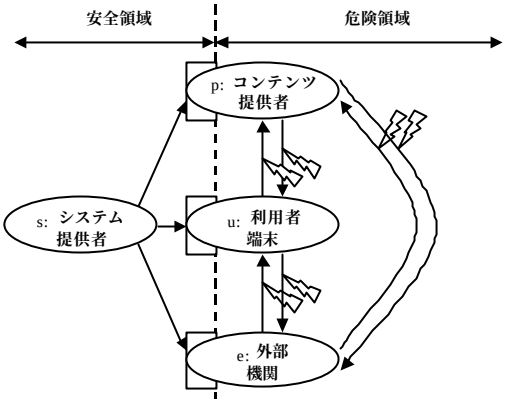

図2 uni-lateral security では、コンテンツの伝送のみが妨害を受ける。

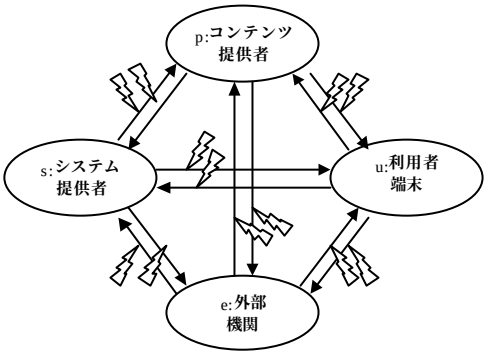

図3 multi-lateral security では、すべての通信に対し妨害が可能であると想定する。

Herzberg モデルは図 2に示すように、s が完全な SC を p,u,e に配布することと等価で、SC の配信には攻撃が存在しない。

前述の不完全性は SC の伝送路への攻撃によりモデル化することができ、図 3に示すように s から p,u,e への SC の伝送に改竄や成りすまし等の攻撃を想定すれば、セキュリティ管理者やプロトコルの様々な不完全性をモデル化することが可能となる。

Hertzberg は「到達可能性(reacheability)」を安全性の基準とした。すわなち図 4に示すように、初期状態 S からスタートしたシステムが仮定された通信路の改竄や妨害によって Ni の範囲でのみ状態遷移し、セキュリティ侵害の状態 Vi に到達できなければ、安全とした。

多面的安全性モデルでは SC の無謬性を破棄したのでどのような状態にも到達可能となる。そこで到達可能性に代えて到達の利得確率分布を指標とする。

たとえば、半導体部品の分析によりシステムの暗号鍵を取得して違法利用を行なう場合、利用による利得と鍵の取得に要する費用が生じ、違法であれば一定の確率で罰則が課せられる。それらの確率と利得(罰則の場合負の利得)を図 5に示すように状態遷移や状態に関連付けると、ある状態遷移列に対して利得 g に対する確率 P(g)分布を求めることができる。多面的安全性では、このような確率分布を安全性の基準とする。

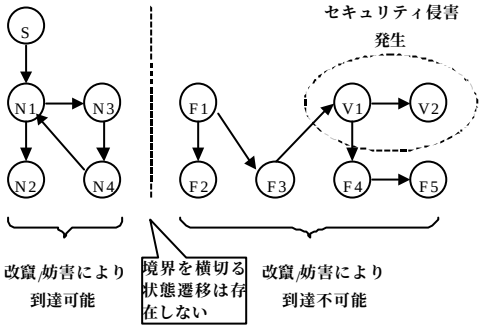

図4 Herzberg モデルでは、セキュリティ侵害の状態への到達経路の有無で安全性を評価する。図ではセキュリティ侵害への経路が存在しない。

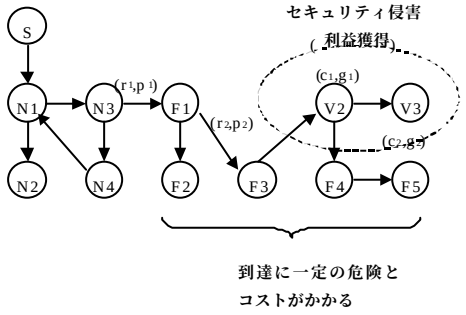

図5 多面的安全性では、セキュリティ侵害に至る経路の利潤で安全性を評価する。

4.3. まとめ

以上の拡張を表 2にまとめる。下線部が多面的安全性モデルで拡張された部分である。また多面的安全性モデルの詳細は金子等によって報告されている。[24)]

5. 多面的安全性のためのコンテンツ保護記述

本章では、多面的安全性を配慮する場合にどのようなコンテンツ保護記述が適切であるかを考察し、筆者等が提案している XML による記述方式を示す。

多面的安全性モデルでは、完全な安全性は存在せず、常に有限の内部不良のリスクが生じる。また、攻撃が成功した際の利潤が大きいほどシステムへの攻撃の可能性が高まる。従って、多数のシステムを併用でき、一つのシステムへの攻撃で得られる利潤を小額に押さえられることが好ましい。

表 2 従来モデルとの比較．下線部が多面的安全性モデルで拡張された部分

	従来モデル	多面的モデル
通信	2 点間の通信	4 点間の通信
メッセージ	コンテンツ、決済、契約	セキュリティ・クライアント、コンテンツ、決済、契約、報告
攻撃者	ユーザー、偽のユーザー、コンテンツ提供者、偽のコンテンツ提供者	ユーザー、偽のユーザー、コンテンツ提供者、偽のコンテンツ提供者、外部機関、偽の外部機関、システム提供者、偽のシステム提供者
被攻撃者	ユーザー、コンテンツ提供者	ユーザー、コンテンツ提供者、外部機関、システム提供者
安全性の基準	到達可能性	到達の経済性

多面的安全性では複数の利害関係者を仮定する。これら複数の利害関係者のすべてが完全に合意する、包括的な統一的ルールを最初に策定することはあまり現実的ではない。たとえば国ごとに著作権に対する規定は異なり、毎年といっていいほど改定される。また、消費者、サービス提供者、行政等、立場によってもシステムが従うべきルールに関する見解が異なる。これらの異なる見解をすべて調整し、統一ルールを策定してからそれに基づくデジタルコンテンツ保護方式を構築するというアプローチは現実的ではない。

筆者等は、デジタルコンテンツ保護以外の実社会でもそうであるように、様々な利害関係者がそれぞれの見解によるルールを構築し、システムはそれらの共存を許し、それらが相互に許容できる領域でシステムを運用するというアプローチが現実的な対処方法と考える。

このような仕組みを可能とするために、コンテンツ保護記述は複数のシステムの情報を効率的に共有でき、システム毎の独自の拡張も可能であることが望ましい。

ISO/IEC JTC1/SC29/WG11 通称 MPEG では現在マルチメディア・フレームワークにおけるコンテンツ保護のフレームワークとしても採用することを視野に入れて MPEG-4/IPMP extension の標準化作業を行っており、筆者等もこの標準化作業に参加している。

図 6に IPMP extension で検討中の新しい IPMP のフレームワークを示す。MPEG-4/IPMP では従来 MPEG-4 ビットストリームに保護記述情報が含まれ

るということだけが規定として盛り込まれており、その具体的機能は全く規定されていなかった。IPMP extension ではコンテンツ保護機能がいくつかの IPMP tool からなるものとし、IPMP tool 間のメッセージを細かく規定することで、コンテンツと IPMP tool のインタフェース、IPMP tool と端末のインタフェース等を明確に定義しようとしている。これにより、様々なコンテンツ保護方式を MPEG-4 端末に組み込む事が極めて容易になり、また方式間の互換性容易に取れるようになると考えられる。

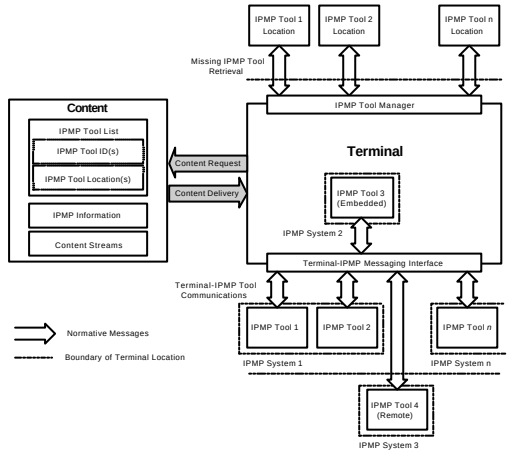

図6 IPMP extension. MPEG-4/IPMP extension で検討中の新しいコンテンツ保護フレームワーク。

筆者は、さらにこのメッセージを XML 言語で記述することを提案している。IPMP ツール間通信用の XML 記述は、通常の XML のタグ構造に図 7に示すような暗号化タグ、署名タグを組み合わせたものである。Sign は署名を表し、Crypt は暗号化を表す。これらのタグと XML の DTD を利用して、既存のコンテンツ保護方式のほとんどについて、そのデータ構造を XML 化することが可能である。

```
<Sign algid="aaaa", type=”asym”, param=”pppp”, sign="qqqq" >
        signatured message
</Sign>
<Sign algid="aaaa", type=”sym”, param=”pppp”, sign="qqqq" >
        signatured message
</Sign>
<Crypt algid=”aaaa”,type=”asym”,param=”pppp”>
        ciphered message
</Crypt>
<Crypt algid=”aaaa”,type=”sym”,param=”pppp”>
        ciphered message
</Crypt>
```

図7 IPMP XML 記述. Sign は署名を、Crypt で暗号化されたメッセージを示す。

表 3 複数IPMP のIPMP/XML 記述。XML 表現により複数IPMP 方式間の共通化が容易になる。

	IPMP System A	IPMP System B
Function	購入価格	購入価格
	1 分毎利用価格	月毎利用価格
Attribute	ISRN	ISRN
	リージョン ID(optional)	
	有効期限(optional)	
バイナリ	0x128abc9ac912518	0xab313131
IPMP/XML	<ISRN> IPMP/A/1234 </ISRN> <Price> $123 </Price> <PerMinutes> $1 </PerMinutes>	<ISRN> IPMP/B/3323 </ISRN> <Price> $123 </Price> <PerMonth> $10 </PerMonth>

XML 記述により、一部分異なる IPMP ツール間符号の共通化が容易となる。たとえば、表 3に示す例では、IPMP System A と IPMP System B の内容は一部共通である。従来の MPEG-4/IPMP では IPMP データはそれぞれ独自のバイナリー形式を持っており、2 方式のデータには全く互換性をもつ余地がない。しかし XML 記述を採用すれば、同一の目的を持つフィールドの共通化は比較的容易に行える。また一部異なる形式である場合も、相互変換が容易となる。

多面的安全性ではコンテンツの正当性、課金情報の正当性を多面的に検証する必要がある。IPMP メッセージの共通化が図られていなければコンテンツ記述の正当性を統一的に検査することは難しいが、共通化によりそれも容易になる。たとえば、有効な ISRN が付されているか、というようなチェックは、表 3の IPMP/XML 表現がなされていれば、異なる IPMP 方式間でも共通化することが可能である。

XML 形式では、フィールドの追加、パラメータの追加が容易である。このため、セキュリティ不良が発見された場合に必要であれば XML 形式による記述データを柔軟に拡張し、新たなセキュリティ・機能を追加して、脆弱性を解消することができる。

IPMP/XML を端末自体が利用する必要は必ずしもない。図 8に示すように、デジタルコンテンツの配信サービスでは、異なった端末タイプごとに様々なサー互換性のないサービスシステムが運用されることが避けられない。たとえば、デジタル放送とブロードバンド化された携帯電話が共通のコンテンツを利用する場合も、基本的なセキュリティ方式は共通化できる

とは限らない。そのような場合、XML によるコンテンツ記述を中間形式として利用することにより、同一コンテンツの複数領域での利用が容易となる。

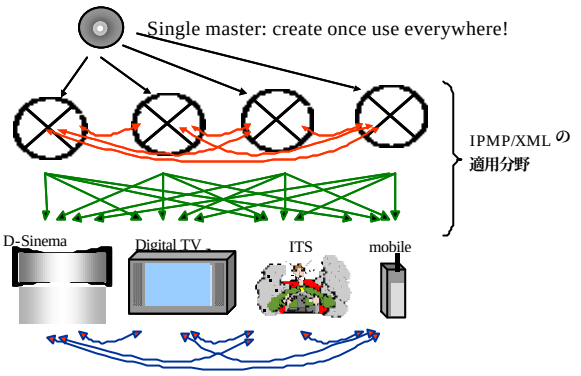

図8 IPMP XML 記述.を各サービス間の共通データ構造として利用することで、様々なメディア間でデジタルコンテンツの共通利用が可能となる。

6. まとめ

本報告では、前半でデジタルコンテンツ保護の安全性について議論し、多面的な安全性の概要を示した。後半では多面的安全性に適したコンテンツ保護記述形式について考察し、筆者等が提案している XML によるコンテンツ保護記述方式を紹介した。

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、本論文で示した XML をーベースとしたコンテンツ保護記述方式は、簡単な構造であるが、様々なセキュリティメカニズムを必要に応じて自由に追加、拡張することが可能である、という点でこれまでにない新しい考え方ではないかと思われる。

謝辞: 本研究に多大な支援をいただいた、前勤務先の株式会社アスキーの多くの方々、社会人博士課程として在籍した早稲田大学白井研究室の多くの方々、MPEG-PF プロジェクトにおいて共に標準化の推進に関わった多くの方々に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) 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
19) Gary McGraw, Edward Felten, "Java Security", John Wiley and Sons, 1997
20) CERT, "Ca-96.05:Java security manager", CERT Ca, Carnegie Mellon University, 1996
21) CERT, "Ca-96.07:Java security bytecode verifier", CERT Ca, Carnegie Mellon University, 1996
22) 高木浩光、米田英一、棟上昭男、小林正彦、高木浩光、"インタラクティブエッセイ-Java セキュリティ・ホールにみる.…", 情報処理学会誌, Vol 41, No. 8, 2000
23) S. M. Bellovin,"Computer Security-An End State",CACM, Vol. 44, No. 3, pp 131,2001
24) 金子格,白井克彦," 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",情報処理学会論文誌,Vol.41, No. 11,2000