

## コンテンツ流通サービスにおけるセキュリティ課題 (パネル討議)

モデレータ 中村逸一†

パネラー 佐々木良一†† 西垣正勝‡

小塚誠一郎†‡ 姫崎光昭‡‡

† 株式会社 NTT データ IT セキュリティ 推進センター  
〒212-0058 川崎市鹿島田 890-12 新川崎三井ビル

†† 東京電機大学工学部情報通信工学科

‡ 静岡大学情報学部情報科学科

†‡ マックス・インターナショナル株式会社

‡‡ 日本ベリサイン株式会社マーケティング部

E-mail: † nakamuraitk@nttdata.co.jp

### あらまし

コンテンツ流通サービスは、最近の常時接続やネットワークの高速化によって一層注目されている。コンテンツ流通サービスの成長の課題は大きく2つある。一つが法および制度的な課題、もう一つが技術的な課題であり、両課題が共に解決しなければ本サービスの成長は難しい。本パネル討論では、コンテンツ流通における技術的な課題のうち特にセキュリティに関する課題を取り上げ、現状の問題点と解決策を議論する。

キーワード コンテンツ情報流通サービス, セキュリティ

## Security Issues of Digital Contents Distribution Services

Itsukazu NAKAMURA†, Ryouichi Sasaki††, Masakazu NISHIGAKI‡, Seiichiro KOTSUKA†‡,  
and Mitsuaki HIMEZAKI‡‡

† NTT DATA CORPORATION IT SECURITY CENTER

†† Tokyo Denki University Department of Information and Communication Engineering

‡ Shizuoka University Department of Computer Science

†‡ MAX INTERNATIONAL

‡‡ VeriSign Japan K.K. Marketing Department

E-mail: † nakamuraitk@nttdata.co.jp

### Abstract

With wide spread of constant Internet access environment and broadband network, digital contents distribution services are expected to become major business. There are two major issues which hinder growth of these services. One is legal and institutional issue, the other is technical issue. Thus, we must solve both issues to make digital contents distribution services a success. In this panel discussion, we focus on the technical issues for digital contents distribution, especially pertaining to security issues. We will point out the security issues and discuss about solutions for these issues.

Key words digital contents distribution services, security

## 1. まえがき

コンテンツ流通サービスは、最近の各家庭への常時接続の普及やネットワークの高速化によって一層注目されている。

ネットワークの利用価格等の環境面の問題を除けば、コンテンツ流通サービスの成長の課題は大きく2つある。一つが法および制度的な課題、もう一つが技術的な課題である。技術的な課題は、さらに著作権問題を解決するための課題と不正使用を防止するために課題に分類される。これらの課題を解決する方法にセキュリティ技術を利用した解決方法が多数提案され、一部商用化もされてきている。しかし、本サービスをビジネス的に成立させ個人レベルでストレスなく使いこなせるためには、更なる課題解決が必要であろう。たとえば、違法コピー防止においては、最終的にユーザがコンテンツを視聴する瞬間を捉えたアナログ的な不正コピーの可能性があり現状の技術では十分に解決できない。

本パネル討議では、それらの問題解決の糸口をつかむためコンテンツ流通サービスの技術的な課題に詳しい方を研究分野および産業界からそれぞれ2名づつお招きし解決方法の提案と議論をしていく。

1986年 日本ビクター入社 コンテンツ流通システムの研究開発に従事

2000年 ベンチャー企業のマックス・インターナショナル入社 コンテンツ流通セキュリティシステムの商用化に従事

2001年 ヒューコム技研 を設立 代表

・テーマに関する意見の要旨（キーフレーズ）

- ①有償コンテンツの流通（音楽コンテンツを例に）
- ②利用者の使い勝手とフェアユース（多様化への対応）
- ③権利者業界と流通関連業界の利害対立（妥協への道筋）
- ④権利者は自己責任の下で権益を守れ（鍵は自ら掛ける）
- ⑤権利者の権益と利用者の使い勝手の両立（実現可能か）
- ⑥P2P型ファイル交換と著作権の保護（保護と転送を分離）
- ⑦技術進歩に著作権は追い付けるか（迂回防止法等が有効）

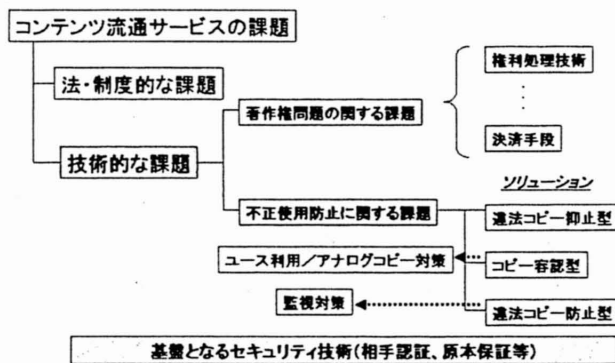
## 2.2 佐々木良一氏

昭和46年3月東京大学卒業。同年4月日立製作所入所。システム開発研究所にてシステム高信頼化技術、セキュリティ技術、ネットワーク管理システム等の研究開発に従事し、ネットワーク管理システムNETMや各種セキュリティシステム等の製品化に貢献。同研究所第4部（ネットワーク関連部）部長やセキュリティシステム研究センタ長、主管研究長などを経て2001年4月より東京電機大学工学部教授。

工学博士（東京大学）。昭和58年電気学会論文賞受賞。平成10年電気学会著作賞受賞。

著書に、「情報科学入門 教養としてのコンピュータ」日本理工出版会 1995年、「インターネットセキュリティ 基礎と対策技術」（共著）オーム社 1996年、「インターネットセキュリティ入門」岩波新書 1999年、「インターネットコマース 新動向と技術」（共編著）共立出版 2000年、等。IEEE、情報処理学会、電子情報通信学会、電気学会等の会員。情報処理学会コンピュータセキュリティ研究会主査。コンテンツIDフォーラム技術WG議長。

コンテンツ流通サービスの課題



(東京電機大 佐々木教授 講演資料を参考に作成)

図1 コンテンツ流通の課題整理

## 2. パネリスト紹介（五十音順）と論点紹介

### 2.1 小塚誠一郎氏

マックス・インターナショナル株式会社（横浜小塚研究室）

1963年NTT入社 伝送システムの研究開発に従事

## 2.3 西垣正勝氏

静岡大学情報学部情報科学科助教授

平成7年3月、静岡大学大学院電子科学研究科博士課程修了 博士(工学)

平成7年4月 日本学術振興会特別研究員 (PD)

平成8年4月 静岡大学情報学部助手

平成11年4月 同講師

平成13年10月 同助教授

研究分野：情報セキュリティ、ニューラルネットワークの耐故障性

### ・テーマに関する意見の要旨

#### 1. コンテンツのユースコントロール

暗号技術により、コンテンツを暗号化し、復号鍵を有する購入者にのみコンテンツを配信することが可能である。しかし、暗号化コンテンツは購入者の手元では復号されてオリジナルコンテンツに戻るため、購入者が悪意を持っていた場合には、購入者からコンテンツの不正コピーが流出する。すなわち暗号化は、コンテンツのディストリビューションコントロールは可能であるが、コンテンツのユースコントロールを行うことはできない。コンテンツのユースコントロールを行う技術・社会的枠組みが必要である。

#### 2. 自律分散型のコンテンツ管理

インターネットには無数のホームページが存在する。著作コンテンツの数も膨大である。よって、著作コンテンツを不正に掲載しているホームページを発見しようと思ったら、無数にあるホームページの一つ一つを訪問し、膨大に存在する著作コンテンツの全てがそこに違法に掲載されていないかをチェックする必要がある。すなわち、ホームページの監視を一局集中型で行うには限界がある。自律分散型のコンテンツ管理が必要である。

## 2.4 姫崎光昭氏

日本ベリサイン株式会社 マーケティング部テクノ

ロジーマーケティング 課長

研究分野：PKIの啓蒙活動および次世代PKI

### ・テーマに関する意見の要旨

1980年代に始まったパーソナルコンピュータの普及、および昨今のコンピューティングパワーの増大は、書籍、音楽、画像などのデジタル化を推し進める要因となった。また、インターネットの拡大、特に近年のxDSLの隆盛に見られる常時接続化/広帯域化の流れは、デジタルコンテンツの流通インフラとして大きな可能性を見せ、様々な実証実験が行われ、一部では商用化の動きも見られている。

こうしたメディアのデジタル化やインターネットを通じた配布は、既存の世界では考えられなかった新たな問題点を提起することとなった。これらの問題点は主に 1) デジタルデータであることによる複製の簡易さ、2) インターネットの特性によるなりすまし、改ざん等のセキュリティ上の問題、3) これらの結果として生ずる課金や著作権保護の問題、などに見ることができる。

コンテンツ自体の保護(複製/改ざん防止)のためには、電子透かしなどが有効と考えられるが、コンテンツ流通サービスという視点から見たセキュリティについて検討すべき課題として、以下のような点が考えられる。

- コンテンツの配信者が実在しているかどうか？  
あるコンテンツをエンドユーザがWebからダウンロードしようとしたときに、そのWebサイトが確かに実在し、かつ悪意のある第三者によって運営されていないことを確認できるようにする仕組みが必要である。
- アクセスを承認されたクライアントがアクセスをしているか？  
特に金銭取引があった後アクセス/ダウンロードを承認し、ユーザにコンテンツをダウンロードさせるとき、本当にそのクライアントがアクセスしているかどうか、確認する仕組みが必要である。いわば、ユーザに対してサーバ側でアクセスコントロールを行う仕組みが必要である。
- コンテンツが改ざんされていないか？  
インターネット上にあるコンテンツは常に盗聴され、改ざんされる危険にさらされている。ある

時点でのコンテンツの内容を保証することによって、改ざんされていないことを保証できる仕組みが必要である。

### 2.5 中村 逸一 (モデレータ)

株式会社 NTT データビジネス企画開発本部 IT セキュリティ推進センター部長

昭和62年茨城大学工学部情報工学科 大学院修了

研究分野：バイオメトリクス認証技術、ポリシーコンピューティングによるセキュリティ管理方式等

### 3. お願い

本パネル討論は、時間の関係上参加者全員が納得できる解決方法を導き出すことは難しいが、参加者全員の意見を出し合い今後の研究や開発の参考になることが目的である。したがってパネリストのみでなく参加者からの意見、質問を歓迎する。