氏名	吉田真紀（よしだまき）
博士の専攻分野の名称	博士（工学）
学位記番号	第16332号
学位授与年月日	平成13年3月23日
学位授与の要件	学位規則第4条第1項該当 基礎工学研究科情報数理系専攻
学位論文名	Protocol Design for Subscriber-Excluding and Traitor-Tracing Contents Broadcast and World Wide Web Audience Rating Survey （加入者の一時排除と不正者の追跡が可能なコンテンツ配信法およびWorld Wide Webにおける視聴度数調査法の設計）
論文審査委員	（主査） 教授 藤原 融 （副査） 教授 柏原 敏伸　教授 増澤 利光　教授 村田 正幸

論文内容の要旨

近年、デジタル放送の開始やインターネットの普及と高速・高品質の通信の実現より、デジタルコンテンツの配信サービスが盛んになっている。コンテンツ配信サービスには、その運営費用が（I）pay-TVのようにサービス利用者（加入者）自身が払う利用料で賄われるものと（II）World Wide Web（WWW）コンテンツサービスのようにスポンサーの広告掲載料で賄われるものとの二種類がみられる。

コンテンツ配信サービスは新しいビジネスの一つと考えられる。しかしビジネスとして成功するためにはいくつかの問題を解決する必要がある。タイプ（I）では加入者の海賊行為によるコンテンツ流出が問題となり、それに対する何らかの対策が要求される。対策の一つとして、海賊行為を行った加入者（不正者）を追跡可能とし、加入者をサービスから排除可能とすることがあげられる。一方、タイプ（II）では広告効果を調査する視聴度数調査が重要な役割を果たす。

本論文では、加入者の一時排除と不正者の追跡が可能な放送型コンテンツ配信法とWWWにおける視聴度数調査法を提案する。

放送型コンテンツ配信では、非加入者がコンテンツにアクセスすることを防ぐため、加入者にあらかじめ復号鍵が入ったデコーダを配布しておき、コンテンツを暗号化して放送する。このようなシステムでは、復号鍵を漏洩した加入者を追跡対象（不正者）とする。本論文では、特定の暗号系の安全性に依存しない配信法と、El Gamal暗号系の安全性に依存する配信法の二つを提案している。いずれの手法も以下に述べる性質を全て満たす最初の手法である：加入者の排除と不正者の追跡の両方が可能；海賊版デコーダから、その作成に携わった全ての加入者を特定可能；海賊版デコーダの入出力の解析だけから不正者の特定が可能。また提案手法は、特定の暗号系の安全性に依存する配信法と依存しない配信法それぞれの中で、最も良い効率を実現している。

WWW視聴度数調査法は、広告効果を測定することを目標とし、各Webサイトへのアクセス数と視聴者の統計情報を正しく公平に調査する手法である。なお、ここで“正しく”というのは、Webサイトによるアクセスの水増しや虚偽の不正を防止すること、“公平に”というのはWebサイト間で共通のアクセス数評価の基準を確立することを意味する。本研究では、アクセス数の評価基準にパラメータを導入することで、状況に応じたアクセス数評価の基準を選択可能とした。また、提案手法では、Webサイトが保持すべきデータ量が増えてはいるが、Webサイトが報告するときに必要とする通信量を従来に比べて大幅に削減されている。また、調査が1年間など長期にわたる場合に

は従来手法ではシステムで保持すべきデータ量が大幅に増加するため、提案手法がメモリ量に関してもすぐれた手法となる。

論文審査の結果の要旨

本論文では、情報の有料提供サービスにおける情報セキュリティの問題を扱っている。放送でデジタルコンテンツの配信サービスを行う場合、通常、サービス加入者にあらかじめ復号器を配布する。不正に作成されたいわゆる海賊版の復号器からその作成元（不正者）を割り出すこと、また、発見した海賊版復号器と同型の海賊版復号器の無効化を行うことが重要な問題の一つである。

本論文では、まず、これを行うための手法が二つ提案されている。提案手法の一方は、効率を重視した手法であり、特定の暗号系の安全性を仮定している。他方は、安全性を重視した手法であり、特定の暗号系の安全性に依存しない。それぞれ、同じ安全性をもつ手法の中では最も効率のよい手法となっている。さらに、いずれの手法も海賊版復号器の入出力の解析だけから作成元の特定が可能であることなど、多くの望ましい性質も備えている。

次に、広告効果を測定することを目標とし、各 Web サイトへのアクセス頻度と視聴者の統計情報を調査する WWW 視聴度数調査法が提案されている。セキュリティの観点からは、調査において、Web サイトによるアクセス頻度の水増し等の不正を防止することが必要であり、最近の電子商取引の普及と共に、実用上、重要な研究である。提案手法では、従来防止できていなかった Web サイト同士の結託によるアクセス頻度の水増しが防止されている。また、Web サイトが保持すべきデータ量が小規模調査の場合は従来に比べて増えてはいるが、Web サイトが報告するときに必要とする通信量を従来に比べて大幅に削減している。調査が 1 年間など長期にわたる場合には、従来手法では保持すべきデータ量が大幅に増加するので、提案法が優れている。よって、大規模な調査に対しては従来法より提案法が向いている。

以上のように、これらの結果は、情報セキュリティ技術に対する多大な貢献である。よって、本論文は博士（工学）の学位論文として価値があるものと認められる。