博士請求論文審査要旨

情報セキュリティ大学院大学
情報セキュリティ研究科

論文題目　：　放送・通信連携サービスのためのセキュリティ技術の研究
申請者　：　大竹剛
審査委員会　：　主査　教授　辻井重男
副査　教授　田中英彦
副査　教授　有田正剛
副査　教授　趙晋輝(中央大学)
副査　教授　土井洋

Ⅰ．論文内容の要旨

博士後期課程学生、大竹剛君の博士請求論文は「放送・通信連携サービスのためのセキュリティ技術の研究」と題し、5 章からなっている。

第１章「序論」では、本論文の研究背景と課題、および本論文の構成を述べている。まず、ハイビジョン番組等の高品質なデジタルコンテンツを通信ネットワークを用いて各家庭に配信するサービスや、デジタル放送受信機を通信ネットワークに接続して視聴者から放送局への情報伝達を可能とする双方向放送サービスを「放送・通信連携サービス」と定義している。次に、放送・通信連携サービスにおける安心・安全なコンテンツ流通を実現するための課題、特に従来の通信サービスとの違いから生じる課題として、「高品質なコンテンツの保護」、「膨大な視聴者の個人情報漏洩対策」、「１対多の放送受信機向けサービスにおける、計算量・伝送量等のコスト削減」、「従来の放送にない、きめ細やかなサービスの提供」を挙げている。そして、本論文の目的は、第２章以降に述べる３つのセキュリティ技術を用いて、これらの課題を解決することにあると述べている。

第２章「コンテンツ保護」は、インターネット上に違法流通する放送番組を自動的に識別することを目的とし、「動画像特徴量抽出方式」および「位相限定相関方式」の２種類の違法流通コンテンツ識別方式を提案している。従来の特徴量抽出方式は映像に対する時間的な編集に弱いのに対し、提案方式は編集耐性を有する。本研究では各々の方式及び両方式を組み合わせる方式についての実験環境を構築した後、放送番組を用いた識別実験による性能評価を行い、両方式を組み合わせることにより、高精度かつ短時間にコンテンツの識別が可能であることを示している。

第３章「プロバイダ認証」は、双方向放送サービスにおいて視聴者の個人情報を放送局に提供する際、放送局へのなりすましによる個人情報漏洩の被害を最小限にすることを目的とし、Key-Insulated 署名（KIS）を用いた鍵漏洩耐性を有するプロバイダ認証システム、および安全かつ効率的な Strong KIS を提案している。提案システムは、PKI において署名鍵更新の際に負荷が大きいという問題を、KIS を用いたプロバイダ認証を行うことで解決している。また、提案する Strong KIS は、従来方式よりも特に署名長が短いため、双方向放送サービスにおいて署名付きメッセージの送受信による通信コストを低減することが可能である。また、提案する Strong KIS の安全性に関するフォーマルな証明も与えている。この結果、Strong KIS を前述のシステムに適用することにより、安全かつ効率的なプロバイダ認証を実現できることを示している。

第４章「属性ベース暗号」は、多数のユーザが存在する IP マルチキャスト放送において、複数の事業者が共通のインフラを用いて視聴者の属性（住所・性別・年齢・会員種別など）に応じたきめ細やかなコンテン

ツ配信サービスを提供することを目的とし、属性ベース暗号（ABE）の軽量化について検討を行っている。従来の ABE の機能の一部を削減することにより、計算量や暗号文サイズにおいて効率的な属性ベース暗号の構成が可能であることを述べている。また、属性を管理する複数の Authority が存在可能な Multi-Authority ABE への拡張方法も述べている。この結果、IP マルチキャスト放送への適用例として、複数の事業者による会員限定サービス等が可能であることを示している。

第５章は「結論」では、以上の成果を要約し、第１章で示した課題の解決を達成したと述べている。

Ⅱ. 論文審査結果の要旨

本論文では、放送・通信連携サービスにおける安心・安全なコンテンツ流通を実現するための課題として、「高品質なコンテンツの保護」、「膨大な視聴者の個人情報漏洩対策」、「１対多の放送受信機向けサービスにおける、計算量・伝送量等のコスト削減」、「従来の放送にない、きめ細やかなサービスの提供」を挙げている。これらの課題に対して、違法流通コンテンツ識別方式、Strong KIS を用いた安全かつ効率的なプロバイダ認証方式、複数の Authority が存在可能な属性ベース暗号方式の３つのセキュリティ技術により解決策を示したものであって、情報学並びに情報社会の発展に貢献するところが大きい。よって、本論文は情報学における博士論文として十分価値のあるものと認める。

Ⅲ. 審査経過

本審査委員会は、2009 年 01 月 30 日に論文内容とこれに関連する事項について口述試問を行い、申請者が学位取得にふさわしい知見を持つものと判断した。