須田 祐子
東京外国語大学　非常勤講師

暗号の国際標準化と情報セキュリティ政策

本研究は､暗号アルゴリズム国際標準である ISO/IEC 18033 の事例を中心に、「情報セキュリティの政治」と暗号国際標準化の展開を明らかにしようとするものである｡暗号アルゴリズムの国際標準化は 1980 年代には国家安全保障上の理由から頓挫したが、1990 年代半ば以降、一転して推進されるようになった。世界最大の標準制定機関である国際標準化機構（ISO）は、国際電気標準会議（IEC）と合同で ISO/IEC 18033 を制定し、2006 年から 2007 年にかけて発行した。このような変化はなぜ生じたのであろうか。本研究は各種資料の分析、さらに国内および海外（イギリスとドイツ）の関係者へのインタビューからこの疑問に対する答えを探ろうと試みた。調査によれば、暗号国際標準化への転換は直接的には､（１）アメリカの次世代暗号標準（AES）プロジェクト､（２）1998 年のワッセナー・アレンジメントの見直し、および（３）1997 年の OECD 暗号政策ガイドラインの採択を受けている。しかし全体的背景として重要なのは 1990 年代のインターネットの普及と電子商取引の発展であった。暗号は、かつては主に軍事と外交に関する国家機密を保護する手段として利用された。だが現在では、通信や個人情報（プライバシー）を保護する手段として、また企業や商取引の秘密を保護する手段として広く利用されている。要するに、暗号アルゴリズム国際標準の制定はインターネットをめぐる商業利益の台頭と情報セキュリティ標準の需要を反映した動きであったと考えられる。

研究成果

暗号アルゴリズムの国際標準化―情報セキュリティの政治と暗号標準―
国際政治　第 156 号, 2009

情報セキュリティ標準化と「私的権威」―暗号、ＩＴセキュリティ評価、情報システム管理―
成蹊大学一般研究報告書第 41 巻第 6 分冊, 2009