巻/頭/言

三菱電機の暗号研究者たちとの想い出

Recollections on Collaborating with Cryptographers at Mitsubishi Electric

太田和夫
Kazuo Ohta

“安心・安全な社会”を目指して情報セキュリティがますます重要になっている。三菱電機を始めとして情報通信機器メーカーや通信事業会社のセキュリティ研究者・技術者は多忙を極め,“嬉(うれ)しい悲鳴”を上げているように見える。この特集号も,このような背景を踏まえて,日ごろの研究開発の成果を世の中にアナウンスするためのものであろう。

電子政府で使用する暗号技術をCRYPTREC(CRYPTography Research and Evaluation Committees)プロジェクトが評価し,「電子政府推奨暗号リスト」を制定した。また,IPA(Information-technology Promotion Agency, Japan)を中心に,「ITセキュリティ評価及び認証制度」や「暗号モジュール試験及び認証制度」が発足し,暗号技術を利用したITセキュリティ製品やシステムの第三者評価の体制も整いつつある。

小生が電電公社時代に暗号研究を開始した25年前を思い出すと,情報セキュリティ分野の盛況には隔世の感がある。当時(1980年代初め),暗号研究に取り組んでいたのは,国内ではごく少数の組織であった。三菱電機では情報セキュリティグループにおられた井上徹さん(現 広島修道大学教授)と山岸篤弘さんで,私の“暗号研究の同志”であった。創成期の熱気の中,ワークショップで深夜まで議論に熱中したことを懐かしく思い出す。自社の利益はさておき,真実を追究する企業の研究者,行司役として信頼のおける大学の先生方,だれもが自由に意見を交換でき,一種の連帯感が醸し出されていたように思える。今から思えば,“産学連携の理想的な姿”だったと言えよう。

三菱電機の研究所の方々とはこんなことがあった。1990年代初め,NTTは社を挙げてFEAL(Fast data Encipherment ALgorithm)というブロック暗号の普及に熱心であった。その安全性評価が私の担当であった。RSA(Rivest, Shamir, Adleman)(注1)暗号で有名なShamir教授の研究グループがFEALの安全性に問題があることを指摘した(差分解読法)。当然のことながら,NTTの研究所では大騒ぎになった。一方,三菱電機では新進気鋭の松井充さんが,差分解読の追試をこつこつと続けながら,いろいろな観点からFEALの攻撃を試みていた。

日ごろの交流を通じて,松井さんが新しい攻撃(線形解読法)を発見したことを察知した私は,上司に“FEALの安全性評価”のために“三菱電機との共同研究の必要性”を進言した。自社の商品の安全性評価(言い方を代えれば暗号解読)を他社の研究者と行いたいという型破りな提案に対して,GOサインを出した上司は偉かったと思う。それにも増して,三菱電機の部長さんは若輩者の私の話に真剣に耳を傾けて快諾し,励ましてくださった。見識のある方だと,感服した。

さて,小生は5年前に大学に移り,教育者としての人生をスタートした。“社会で通用する研究者,技術者の育成”が目標である。仕事の段取りを自分で整え,自立的かつ自律的に行動できる人材を社会に送り出したいと考えている。“調査・分析”問題点の発見”報告書書き”論文発表”を経験させることにより,“擬似的”成功体験を積ませるように努めている。“真”の成功体験は,就職後の企業にお願いすることになる。若者の能力を開花させるべく,人材の一貫教育を実現するための“産学連携”を成功させてみたいと意気込んでいる。

(注1) RSAは,RSA Security Inc.の登録商標である。

◆電気通信大学 教授 Professor, University of Electro-Communications