特集

「セキュリティとトラスト」にあたって†

井上 敦司*1

情報通信技術の飛躍的な発展はグローバル経済発展の基礎を形成し、人々の生活水準を少なくとも20年分は高めたと言われる。実際、日常生活で用いるサービス（銀行、証券取引、保険、クレジットカード、通販、各種チケット予約・購入、出前注文など）の多くがこの技術に依存しており、故意の種々攻撃と偶発的過失の両方に対する安全性、信頼性、生存可能性の向上が強く求められるようになった。事実、日本では総人口の80%が高速インターネット回線に接続可能な時代になっており、数年以内にその範囲を100%に近づける計画が日夜推進されている。

このようなインターネットの普及・使用状況を指して、「ネット社会」という言葉をよく耳にすることがある。この言葉の意味として、少なくとも「情報通信技術を基盤とする社会」と「インターネットそのものが仮想的な社会」が存在するといえる。後者は、ネットニュースやブログといった公共性の高いネットワークサービスにおいて、その利用に関する慣習や常識などが規定されることにより、利用者の間で自発的に発展した多くの独創的な仮想社会を指す。これに対して前者は、社会基盤として位置づけられたインターネットが日常生活に深く浸透した新たな一般の現実社会を指す。これら2つの対極的な性質を有し、かつ急速に発展したこの「ネット社会」では、現状の法体系や管理手法では対処仕切れない重要な問題（例えば、種々の情報漏洩事件や個人情報流出事件）が横行しており、これらに迅速かつ適切に対応するための技術開発や専門職の人材育成が強く望まれている。

米国のカーネギーメロン大学はこのようなニーズをいち早く認識し、情報セキュリティ研究所*2(CyLab)を設立し、セキュリティやトラストに関する研究を統括的にあらゆる角度から進めている。CyLabでは、こ

れら諸問題を技術問題単体として捉えるのではなく、社会学、法律、心理学、公共政策管理、経済学などを取り入れた複合横断型学問領域として捉えている。ここに、これら多くの異なる分野から世界の第一線で活躍する研究者を集い、実践的な研究・開発及び教育活動を日夜行っている。CyLabは、同大学の情報ネットワーク研究所(INI)、コンピュータ緊急対応センター(CERT/CC)、ソフトウェア工学研究所(SEI)、公共政策管理学部(Heinz School)、ビジネススクール(Tepper School)、電気工学部、情報科学部などと緊密に協賛しており、そこには世界中から集まった400人以上の教員、研究者、大学院生などが在籍する。

一方、兵庫県は、CyLabの活動に共感、いち早く注目した井戸知事主導の下、2005年にカーネギーメロン大学日本校(Carnegie Mellon CyLab Japan)を神戸ハーバーランドに開校し、兵庫県のみならず日本全体、ひいてはアジア諸国への貢献を視野に入れた研究・開発及び教育活動を開始した。ここで開講している情報セキュリティ大学院修士課程は、INIの直接統括下で米国本校と同等の水準を有する教育*3をおこない、協賛企業や団体から派遣されたセキュリティ専門職を志す社員に加え、アジア、欧州、米国などから学生が集い、国際的な雰囲気の中で日夜、訓練、研究、そして実践プロジェクトに取り組んでいる。更に、県下一般市民や多忙な諸企業のIT担当者に向けて、セキュリティやトラストに関する独自のセミナーや訓練プログラムも提供している。

本特集の解説では、CyLabの有望な若手研究者や先見の目を持った指導者の方々を中心に、研究と教育に関して幅広く執筆・協力をお願いした。第一稿は、最近のセキュリティやトラストの動向について武田圭史先生らに執筆をお願いした。暗号論など技術のみに偏った研究ではなく、大きな複合研究領域の一つと捉える考えがより大切であることをご理解頂ければ幸いである。二稿目では、インターネット上でニーズが高いマルチメディアへの暗号論の応用について、米国ワシントン州で鋭意活躍中のKoh先生らに解説をお願いした。三稿目では、当学会の核心技術分野である機械学習へ、セキュリティやプライバシーへの応用研究に

† Security and Trust

*1 Atsushi INOUE

カーネギーメロン大学日本校
(財団法人ひょうご情報教育機構)
Carnegie Mellon CyLab Japan
On-leave from Eastern Washington University

*2 <http://www.cylab.cmu.edu/>

*3 カーネギーメロン大学キャンパスの一部ということで英語を公用語としている。

において注目と期待が集まっていることをCyLab研究者の研究紹介を通じて解説した。最終稿では、本分野の専門職教育とユニークな取り組みについて、その最前線で活躍中のツアミティス先生らに解説をお願いした。

投稿原稿は、村山先生らのユーザの満足度という視点からのトラストとピシュバ先生の生体情報に基づく実践的なセキュリティ測度に関するショートノート、そして内海先生らのウェブの信頼性に関する研究論文を収録するに至った。

解説記事と収録論文全般を見渡すと、純粋な技術開発に始まり、教育、人間的因子に関するものまで、当学会誌に相応しい領域横断型に仕上がったと自負している。また、CyLabと兵庫県の取り組みを反映して、著者陣も国際色豊かである。一人でも多くの読者が、現在最も注目される社会問題の一つである「セキュリティとトラスト」に興味を持ち、一つでも多くの実践的な成果が生れることを願いつつ筆を置くことにする。