

電子社会の信頼性向上と情報セキュリティ

辻井 重男 情報セキュリティ大学院大学/中央大学研究開発機構 tsujii@iisec.ac.jp

情報セキュリティを巡る社会環境と意識の変化

平成14年10月、中央大学COE「電子社会の信頼性向上と情報セキュリティ」が採択されて以来、2年余りが経過した¹⁾。この間、住民基本台帳ネットワークを始めとする電子政府・自治体の進展やさまざまな電子ビジネスの展開を受け、情報セキュリティに対する社会の意識は大きく高まってきた。中でも、繰り返される企業等からの情報漏洩は企業ブランドを落とし、場合によっては命取りになりかねないとの認識も広がり、2005年4月の個人情報保護法の全面的実施に対応して、各企業は手探りの努力を続けている。個人情報保護法の実施による民事訴訟や、刑事訴訟、あるいはリスクマネジメントへの対応のため、デジタルフォレンジックス（証拠情報論）のような技術・管理分野も成長してきた。

このように情報セキュリティもようやく市民権を得てきたことを実感している。

本COEは、上記の多岐にわたる社会システムの基盤的要素技術である超楕円暗号等、中央大学が国際的に実績を挙げてきたいくつかの要素技術を中心に申請したものであるが、これらの要素技術を含む電子社会の安全性向上という総論が必要であることを、我々は、当初より認識していた。研究開始後、事業推進担当者による討議を深める中で、より積極的に、セキュリティ技術、管理・組織運用、法制度、情報モラル等を相互に連携させて相乗効果を発揮するための学問体系としての学際的情報セキュリティ総合科学のダイナミックな構築の必要性を強く認識するようになり、そのためのシンポジウムも3度にわたり開催してきた（表-1 参照）。

審査員の側でも、総合的視点の必要性を意識されており、平成16年8月の中間評価では、要素技術に関する成果とともに、このような我々の活動を高く評価していただいた。

以下、IT社会と情報セキュリティの理念、およびCOE発足後の組織・人材の強化、各分野の研究成果、

人材育成などの状況について、概要を述べることにする。

IT社会の理念と情報セキュリティの階層構造

情報セキュリティはIT社会の基盤である。我々は、「IT社会の人類史的視点からの普遍的理念は、自由、平等、安心に要約される。そして情報セキュリティはこれらの理念を実現するためのインフラストラクチャである」との立場から、中央大学のCOE「電子社会の信頼性向上と情報セキュリティ」を推進してきた。まず、この点について、簡単に説明しておきたい²⁾。

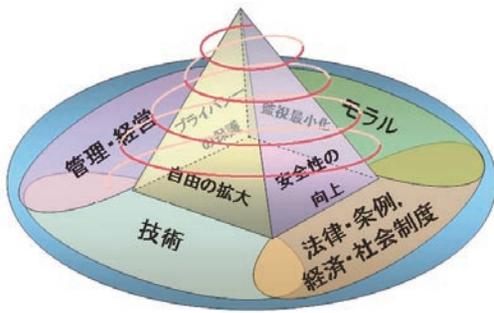
ITによる自由の拡大と情報セキュリティ

「歴史とは自由拡大の過程である。歴史とは自由の意識の進歩のことであり、そのことを我々は認識しなければならぬ」とヘーゲルは述べている。この、いわばヘーゲルの法則は、大哲学者の生きた時代と空間を越えて、現代においても1次近似的には成立するように思われる。もっとも、自由自体の定義は難しく、構造主義的思潮の中では、我々の自由や自律性は限定的なものであるとみなされているが、少なくとも自由実現のためのインフラ、すなわち、利便性・効率性はITなどにより単調増大しているといえよう。

そこで、ITによってもたらされる自由の拡大をできる限り損なうことなく、安全性・信頼性をどう保証するかが本質的な課題となる。初めから両者のバランスをとるという姿勢ではなく、この2項対立を乗り越え、可能な限り両立・止揚するための新たな解を見出さねばなら

名称	開催日
シンポジウム「電子社会の展望」	2003年 4月12日
シンポジウム「情報セキュリティにおける研究・人材育成拠点へ向けて」および特別研修コース	2003年 12月19～23日
学際的情報セキュリティ総合科学シンポジウム	2004年 11月21～27日

表-1 本COE主催シンポジウム開催実績



Copyright 2003 Shigeo TSUJII

図-1 情報セキュリティの理念

ない。そのため、技術、管理、監査、組織運営、法制度、情報倫理などを緊密に連携させて、相乗効果を挙げる工夫が求められる。

ネットワークの前の平等と情報セキュリティ文化

理念として平等を掲げるとき、権利的側面を指すことが多いが、ここでは、デジタルデバイドの解消というような権利の側面はもとより、ネットワークへの参加者すべてが、平等に、あるレベルの責任を負うことを含意している。卑近な例でいえば、インターネットの踏み台攻撃を防ぐには、ユーザの誰もが、ある程度の知識を持ち、相応の注意を払わねばならない。

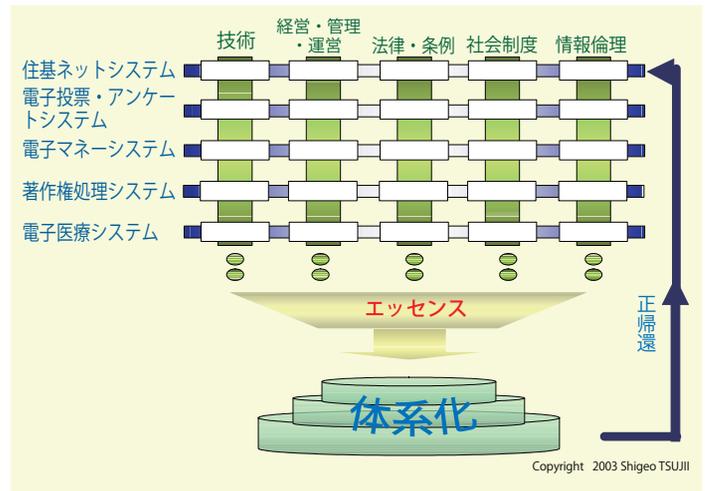
OECDの情報セキュリティガイドラインは、「ネットワークへの participants はすべからず情報セキュリティ文化を共有すべし」と謳っている。「情報セキュリティ文化の共有」という米国の提案に対し、当初、参加国間で、疑問の声もあったそうであるが、筆者は、文化とは、あるグループに属する人々に固有の価値観・モラルや、生活・行動様式等の総体であり、国境を越えてつながるネットワークへの地球上のすべての参加者が情報セキュリティ文化を共有することは当然と考えていたので、我が意を得たりという思いであった。

情報セキュリティ文化を共有するためには、情報セキュリティ教育の普及が不可欠である。

安心と安全

米国の交通事故死者数は年間でおおよそ4万人、約12分に1人が亡くなっているようである。日本は、年間おおよそ7千人、約1時間に1人の割合である。これほどの高率でも、人々はさほど不安を感じずに車に乗っている。2003年の、住民基本台帳ネットワークシステムの稼働に際しては、絶対安全を求める声が高く、時の総務大臣も絶対安全ですと答えざるを得なかった。この違いはどこから来るのか。

交通事故は、明治36年の1件から始まり徐々に増え始めたのに対し、ネットワークの大衆化は急速であった



Copyright 2003 Shigeo TSUJII

図-2 情報セキュリティ総合科学の構築へ向けて

こともあるが、見えざるものへの不安も大きいのではないだろうか。我々、情報セキュリティの研究・教育に携わる者は、客観化し得る安全性の向上への対応はもちろん、不安を軽減するための努力も続けねばならない。

一般に情報セキュリティには、技術や法律のように形式化・制度化できるレベルと、不安・安心やモラル、プライバシー感覚のような暗黙知のレベルがあること、そして、一般に形式知と暗黙知は固定したものではなく、暗黙知はやがて形式知となり、形式知から新たな暗黙知が生まれたりする流動的なものであることもわきまえておく必要がある。

情報セキュリティは上に述べたように、技術、管理運用、法制度、情報倫理、組織論などからなる総合科学である。図-1、図-2に示すように、これらを連携させつつ、互いに相乗効果を挙げるように、そして、技術の進展や人々の意識の変化など時代の動きに合わせて、ダイナミックな体系化を絶えず進めていかねばならない。

また、図-3のように、情報セキュリティを、要素技術、システム技術、社会システムに階層化してとらえることもできる。本COEで、これらのすべてを研究することはもとより不可能であるが、このような、総合科学性や階層を視野に入れながら、中央大学の持てる力を選択的に注いで、研究と人材育成を進めてきた。

COE採択後の研究者の増強と組織の強化

本COEでは、採択以降、表-2に示す組織の強化を行った。

(1) 研究者の採用

表-3に示すように、COEの資金により、若手を中心に、多くの研究者・PD(Post Doctor)を時限付きで採用して、研究活動の活性化、人材の育成に努めている。また、現代暗号を開花させた数学的土壌である数論の世界

的指導者、伊原康隆博士(学士院賞受賞)を若手の指導者としてCOE研究員に迎えている。COE発足後、図-4に示すように博士後期課程学生数は大幅に増加している。

② RA (Research Assistant) の採用

博士後期課程学生の育成はCOEの大きな目標であり、表-3に示すように、多数のRAをCOEの資金により、採用している。

③ コンピュータ・ネットワークセキュリティ分野の強化

暗号と並ぶ情報セキュリティ技術の太い柱である、セキュアOS、脆弱性データベース、ファイアウォールなどの分野を強化するため、平成16年度から土居範久教授を中央大学に迎えて、研究の充実と人材の育成強化を図っている。

④ 情報セキュリティ副専攻の設置

上に述べたように、情報セキュリティは学際的総合科学であり、その観点から大学院学生を育成すべく、平成15年度より、学際的カリキュラムによる電子社会・情報セキュリティ副専攻を設置した(表-4参照)。情報セキュリティ法制やシステム監査にも多数の理工系学生の受講者があり、平成15年度の修了者が27名に上ったのは嬉しい誤算であった。

⑤ 文部科学省科学技術振興調整費「情報セキュリティ・情報保証 人材育成」の採択

平成16年度の上記調整費に応募し、採択された。

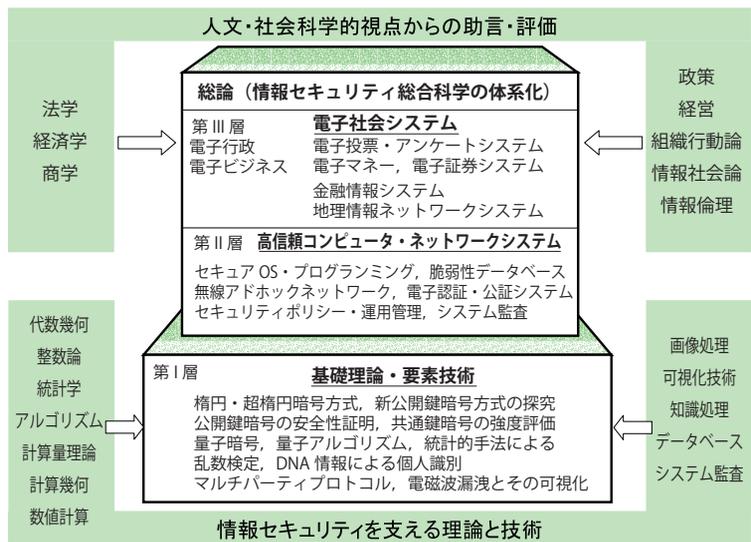


図-3 情報セキュリティの階層構造

研究員等の採用	COE研究員9名、PD1名、RA12名 (COE経費の約70%)
副専攻の設置	電子社会・情報セキュリティ副専攻の設置(平成15年4月~)
文部科学省人材育成拠点	平成15年度文部科学省科学技術振興調整費採択「情報セキュリティ・情報保証 人材育成拠点」
コンピュータ・ネットワークセキュリティ強化	土居範久教授を事業推進担当者に加え、脆弱性データベースなど、コンピュータ・ネットワークセキュリティ分野の研究・大学院学生の指導体制を強化
法制面の強化	個人情報保護法等で著名な堀部政男教授(中央大学法学部)を事業推進担当者に加える

表-2 研究システム・組織の強化(平成16年度)

分野	テーマ	メンバ	
		事業推進担当者	研究員・PD・RA等
総論	I 情報セキュリティ総合科学の概念形成	辻井 重男 内田 勝也 土居 範久 久米 均	石崎
暗号理論	II 楕円・超楕円暗号理論とそれを支える代数曲線	趙 晋輝 関口 力 松尾 和人 百瀬 文之 辻井 重男 諏訪 紀幸	伊原、土屋 志村、谷戸 原口、新妻 飯島
	III 公開鍵暗号の新方式探究と証明可能安全性	辻井 重男 岡本 龍明 土井 洋	小林
	IV 計量量・アルゴリズム	浅野 孝夫 山村 清隆 今井 桂子	只木
	V 量子暗号・量子アルゴリズム	広田 修	只木、津田 加藤
	VI 乱数と共通鍵暗号	藤井 光昭 杉山 高一	竹田、前田

表-3 研究推進組織

分野	テーマ	メンバ	
		事業推進担当者	研究員・PD・RA等
識個人	VII DNA情報と識別・認証	板倉 征男 辻井 重男	橋谷田
コンピュータ・ネットワークセキュリティ	VIII ソフトウェアの信頼性・安全性脆弱性とデータベース	土居 範久 内田 勝也	
ネットワークの信頼性	IX 無線ネットワークの信頼性と電磁波漏洩	篠田 庄司 齊藤 忠夫 白井 宏 牧野 光則	関口、示沢 曹、船田 望月、相良
電子社会システムの信頼性	X 電子社会システム	辻井 重男 細野 助博 今井 桂子 今野 浩 土井 洋 田口 東	宇津木 鳥海
	XI 情報セキュリティマネジメント	内田 勝也 土居 範久 久米 均 中條 武志	
	XII 電子データの信頼性向上	杉山 高一 鎌倉 稔成	竹田、李

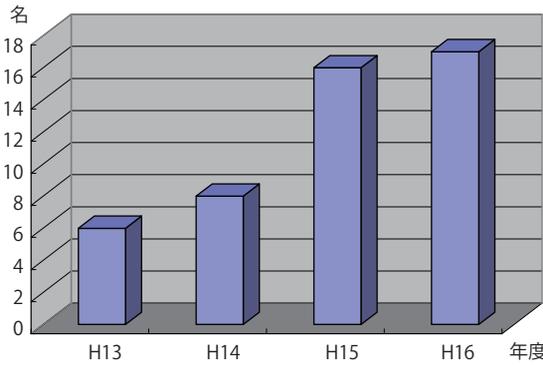


図-4 情報工学専攻 博士後期課程在籍者数の推移

カリキュラム 平成 15 年度

科目	単位	開講	必修 選択	講師
電子社会と 情報セキュリティ	2	半	必	辻井重男教授 土井洋 機構助教授
暗号と電子認証	2	半	必	趙晋輝 教授
ネットワーク セキュリティ	2	半	必	土居範久 教授 内田勝也 機構助教授
システム監査Ⅰ	2	半	必	大井正浩客員教授 (朝日大学教授)
システム監査Ⅱ	2	半	選	
情報セキュリティ法制Ⅰ	2	半	必	安富潔 客員教授 (慶應義塾大学教授)
情報セキュリティ法制Ⅱ	2	半	選	
情報セキュリティ 特別演習	2 2	半 半	必 必	各 講師

表-4 中央大学情報セキュリティ副専攻

COEが研究と博士後期課程の人材育成を主眼としているのに対し、本調整費では、コンピュータセキュリティの実践面などを中心に、情報セキュリティ教育を精力的に実施しており、図-5に示すようにCOEと表裏一体の活動を続けている。

⑥個人情報保護法など法制面の強化

平成 17 年度から、本COEに堀部政男教授を事業推進担当者として加えることとした。堀部教授は、冒頭に述べたような国民的関心事である個人情報保護法などの情報法制の創設に、1980年当時からOECDなど国際の場で活躍しており、本COEへの参加によって、学際的研究をより活発に進めることとしたい。

研究グループの構成とその成果

本COEは、表-3に示す12のグループにより、研究を推進している。そのうちのいくつかを紹介する。

①超楕円曲線上の公開鍵暗号

公開鍵暗号の発明以来、最も多く使われてきたのは、RSA暗号である。次いで、RSA暗号より安全性・実装性に優る楕円暗号の実用化が進められている。本COEで研究を進めている超楕円暗号は、64ビットプロセッサに向けてはいるものの、数学的概念装置が楕円暗号より遥かに高度で難解になる割には、演算速度が楕円暗号より遅いなどの点で実用性は低いというのが、本COE発足1、2年前の国際的認識であった。趙、松尾らの中央大学暗号研究グループはこの常識を覆し、超楕円暗号の演算速度を楕円暗号の数倍以上（パラメータによる）に高速化し、また、世界で初めて実用的な位数を持つ曲線の生成に成功した^{3), 4)}。我々の先駆的成果を見て、



図-5 研究体制

ドイツ、フランスなどの研究者が競い合うようにして研究を続けており、本COEが中心となって、毎年、これらの海外の研究者たちを招いたシンポジウムを行っている（表-5参照）。

②新しい公開鍵暗号の追求

現在の公開鍵暗号は、その解読困難性の数学的根拠を、素因数分解の困難性、あるいは離散対数問題の困難性においている。これらの困難性は、量子コンピュータの出現には原理的に対抗できないとされている。量子コンピュータが実現し得るか否かは不明であるが、情報セキュリティの立場からは、そのような場合も想定しておかねばならない。量子コンピュータの出現に対抗できる1つの候補として、多次多変数型公開鍵暗号方式が考えられ、さまざまな方式が提案されている。筆者は、2003年、これらの方式の安全性を向上させる汎用的な概念装置として、持駒行列を提案し、特許も出願していたが、2004年に入り、只木COE研究員や大学院学生藤田の協力を得て、その理論的構築を進めている⁵⁾。

③個人識別方式

IT社会では、本人確認がきわめて重要である。特に、本人とカードの対応の真正性が問題となる。本COEでは、板倉・辻井がDNAのSTR (Short Tandem Repeat) と呼ばれる(病気などには関係のない)数値列が、人間が持つ唯一のデジタル情報であることに着目して、これを公開鍵暗号の秘密鍵に組み込むことにより、上記の課題を解決する方法を提案している⁶⁾。また、DNAと合わせて、虹彩による個人識別技術の研究を続けている。

④光通信量子暗号方式

量子効果を利用した暗号は1984年以来、内外で進められてきた。それはBB84方式と呼ばれ、光子を1個ずつ送ることを原則とする方式である。物理学の応用としては興味深い、冷却装置の必要性など加入者線なども含めた光通信全般への普及には実用的制約があることに加えて、平文自体を暗号化することはできず、鍵の配送のみに用途が制約されるという本質的限界がある。

これに対して、Yuenが2000年に提案した方式は、高速光通信システムにおいて、平文自体を暗号化し、量子効果を利用してこれを誤りなく盗聴することを不可能にする方式であり、Y00方式と呼ばれている。盗聴者が通信路を流れる暗号文を読むときの誤り率は光子数と変調方式の組合せによって決まるので、その最適化を図るという工学的システムである。

広田(事業推進担当者)と加藤(COE研究員)は、民生用への普及を考慮し、Yuenと異なる変調方式を考察し、Y00最適設計理論を構築している⁷⁾。

このほか、土居をリーダーとするコンピュータセキュリティ・グループや2人のIBM賞受賞者(浅野、山村)を擁するアルゴリズムグループ、そして総合政策学部の細野からも顕著な成果を挙げ、活発な活動を展開している⁸⁾。

研究文化の共有

以上、本COEの理念、組織、成果などについての概要を紹介した。

具体的成果については、4つの分野に関して研究状況を説明したが、いずれも未来開拓的な挑戦的研究であり、また学問体系構築の観点からも、進めるべき研究であると考えている。

超楕円暗号については、楕円暗号に勝てるのかという批判もあるが、楕円暗号も10年前にはRSAに勝てるのかと言われたものである。DNAについても、現在のところ、識別に時間とコストがかかり過ぎるといわれているが、技術は日々進んでおり、10年後には広く用いられよう。

Yuen—広田の量子暗号も、米国とは異なり、我が国

名 称	開催日
次世代暗号と関連する数学に関する国際シンポジウム	2003年2月11～13日
暗号と関連する数学に関する国際ワークショップ2003	2003年9月9～11日
2004 Workshop on Cryptography and Related Mathematics	2004年8月6～8日

表-5 本COE主催国際シンポジウム開催実績

では定説になっているわけではないが、多くの優れた研究は異端から正統へ道を歩むものである。本COEでは、資金などの制約から、理論研究のみに限定されるが、米国では、すでに、毎秒650メガビットで、200kmの実証実験を行っている。また、広田は欧米から数度にわたり、講演を依頼されている。

西澤首都大学東京学長は「ユダヤ人は全員が賛成したテーマは採択しない」とよく言われる。我が国では、挑戦的研究を奨励する一方で、全員賛成型の評価をするという矛盾を犯し勝ちである。研究は計画することも管理することも難しいという研究文化を共有することが、国民的課題であろう。

今後、COEとして残された2年間、学際的情報セキュリティ総合科学のダイナミックな体系化と個々の要素技術の研究を推進して、中央大学における研究拠点の確立に繋げたい。

これまでの関係各位のご支援に感謝するとともに、今後とも一層のご指導をお願いする次第である。

参考文献

- 1) 辻井重男: 中央大学「電子社会の信頼性向上と情報セキュリティ」、電子情報通信学会誌, Vol.86, No.11, pp.900-905 (Nov. 2003).
- 2) 辻井重男: 電子社会を推進する情報セキュリティ総合科学のパラダイム, 電子情報通信学会論文誌, Vol.J87-A, No.6, pp.710-720 (June 2004).
- 3) Gonda, M., Matsuo, K., Aoki, K., Chao, J. and Tsujii, S.: Improvements of Addition Algorithm on Genus 3 Hyperelliptic Curves and Their Implementation, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E88-A(1), pp.9-96 (2005).
- 4) Matsuo, K. and Chao, J. and Tsujii, S.: An Improved Baby Step Giant Step Algorithm for Point Counting on Hyperelliptic Curves over Finite Fields, The 5th Symposium on Algorithmic Number Theory, ANTS-V, C. Fieker and D.R. Kohel (Ed), Vol.LNCS-2369, pp.461-474, Springer-Verlag (2002).
- 5) Tsujii, S., Tadaki, K. and Fujita, R.: Piece in Hand Concept for Enhancing the Security of Multivariate Type Public Key Cryptosystems; Public Key without Containing All the Information of Secret Key, Cryptology ePrint Archive, Report 2004/366 (Dec. 2004). Available at URL: <http://eprint.iacr.org/2004/366/>
- 6) Itakura, Y. and Tsujii, S.: Proposal on a Multifactor Biometric Authentication Method Based on Cryptosystem Keys Containing Biometric Signatures, International Journal of Information Security (IJIS) (2005).
- 7) Hirota, O., Kato, K., Sohma, M., Usuda, T. and Harasawa, K.: Quantum Stream Cipher Based on Optical Communications, Denver, Proc. SPIE, Vol.#5551, pp.206-219 (2004).
- 8) Terada, M. and Doi, N.: Proposal of the Security Information Sharing System with RDF Site Summary, The 8th World Multi-Conference on Systemics, Cybernetics and Informatics, Vol.X, pp.40-46 (July 18-21, 2004).

(平成17年2月25日受付)