電子行政・総合科学・現代社会と教養・人材育成

―情報セキュリティ視点からの起承転結―

7

辻井重男●中央大学研究開発機構

要素技術

起―国民的基盤としての電子行政と認証

我が国の電子政府・自治体への歩みが遅々として進まないのは，国民にとって不幸である．ここ数年来の年金に関するトラブルは，プライバシ保護の保証の下に，各自が個人情報を常時，確認できるシステムが完成していたら，避け得たであろう．年金に限らず，税金，医療，福祉，介護，電子投票などの個人情報を対象とする，このためのシステムとして電子私書箱が提案されている[1]．

電子私書箱の実現には，各省庁や自治体のバックオフィス連携，保有するデータベースの疎結合，および，認証，つまり各個人の本人確認を安全確実に行わなければならない．ここでは，後者の課題について考えてみよう．

2004年，公的個人認証サービス制度が発足した．これは，政府・自治体に対する住民からの税金などの申請を電子化するための制度であり，カード枚数は2009年現在で約113万件に達した．しかし，納税者総数から見れば，数パーセントに満たない．2008年夏，時の福田総理からの「行政の電子化を急げ」との指示の下に，内閣官房に，「電子政府ガイドライン作成検討委員会（須藤修座長）」が設置され，筆者は，セキュリティ分科会の主査を務めた．

署名も認証も，公開鍵暗号の技術的には似たようなものだが，文化的・法的観点からは，大きく異なる．認証とは本人確認であり，署名とはこの文書は確かに自分が書いたということの確認，および署名後に改竄されていないことの保証である．たとえば，電子行政の先進国，デンマークでは，認証は15歳からできるが，署名は文書に責任が持てるようになる18歳からと定められている．

電子私書箱の閲覧に際しては，署名は必要なく認証のみでよい．公的個人認証サービス制度に認証という文字が付されているのは，たとえば，税金の申告に際しては，まず，オンラインでの申告者に対して本人確認を行ったのち，申告書を受け付ける必要があるからである．しかし，公的個人認証サービス制度は，電子申請のために制定されたもので，電子私書箱のような認証用途には適用できないと法的には解釈されている．

また，金融機関や携帯通信業者などでは，預金者・顧客保護の立場から，本人確認・実在性確認の必要が高まる中で，そのためのコスト負担が問題となっており，本サービスを使用させてほしいとの要望も高まっている．税金を使用して構築したサービスを，国民的基盤として見直し，官民連携して有効活用すべきであろう．そのための方策は，筆者が座長を務めた総務省の「公的個人認証サービス普及拡大検討会」でさまざまな提案がなされているが，技術とその運用面のほかに，法制度，文化的・歴史的課題など総合的に考慮すべき課題が多い．

公的個人認証サービスを国民的基盤として，生活と産業に活用するためには，各個人に固有の番号を振ることが不可欠である．電子私書箱の例からも分かるように，これは，民主党政権も提唱していると言われる国民安心番号なのである．電子行政の先進国といわれるフィンランドでは，1634年（江戸初期）に国民情報登録制度が設けられて以来，自分の情報は公的機関に預けておけば安心だという文化が歴史的に根付いているそうである[2]．我が国も官民間の信頼関係を早く築きたいものである．大戦の後遺症もあり，一部の文化人や評論家が，国民番号に観念的に反対を繰り返し主張したことが，公的個人認証サービスの範囲を縮小した一因でもあった．このことは，3．転で述べるように，情報分野や世論をリードする人材に求められる教養について考えさせられる．

公的個人認証サービスを含め，電子行政システムの全体最適化が，クラウドに代表される情報技術・利用の新潮流を契機に，相互に矛盾する課題を乗り越えて，抜本的に進展することを期待したい．

承―情報セキュリティ総合科学の構築

「利便性と安全性のバランスですね」という表現はしばしば聞かれる．確かに，ある時点での利用環境を固定し

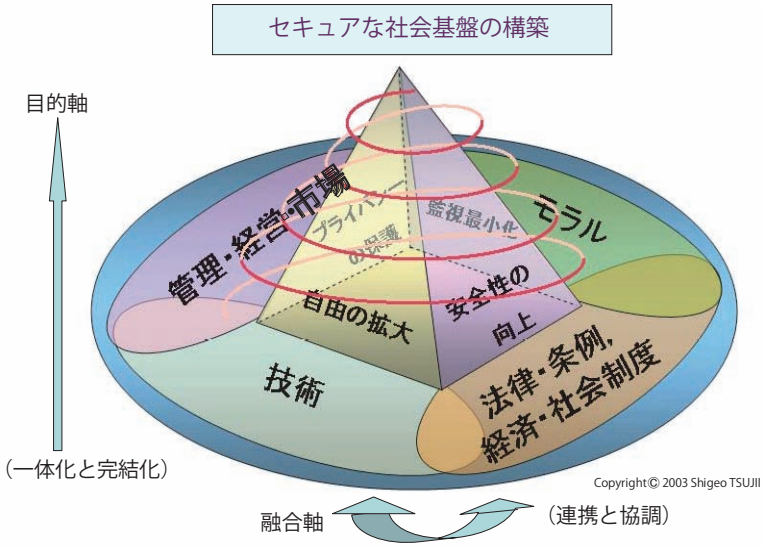

図 -1　情報セキュリティの理念

て考えれば，両者はトレードオフの関係にあるといえる．しかし，単なるバランスは妥協である．情報セキュリティにとって本質的に大事なことは，可能な限り矛盾を超克して，より高い均衡を実現することである．情報セキュリティの視点からは，社会的価値として自由，安全，プライバシの 3 つが重要である．自由の定義は難しいが，低い次元では利便性・効率性を指すものとしておこう．哲学者 Hegel は，「歴史とは，自由拡大の過程である」と述べているが，情報化により拡大される自由の拡大と安全性の向上・プライバシの保護はしばしば矛盾する．安全性とプライバシ保護は必ずしも相反するものではないが，安全性にのみ留意して監視を強めすぎれば，プライバシが損なわれ，プライバシ保護の名の下に匿名性が強まれば犯罪が増加する．

電子選挙を例にとって，安全性（不正の防止）とプライバシ保護の両立について考えてみよう．投票内容はプライバシに属するが，それを良いことに水増し投票が行われても困る．この矛盾は，ゼロ知識相互証明という暗号プロトコルを適用すれば，完全に解決される．これは，技術のみで，矛盾が解消される例であるが，電子選挙を円滑に実施するためには，技術評価基準，情報セキュリティマネジメントシステム，監査，法制度，モラルなどの面から総合的・止揚的対策が必要となる．

また，企業経営において，利便性・効率性を上げるように組織を再構築した結果，情報漏洩が減少することもあるだろうから，利便性・効率性と安全性向上やプライバシ保護が，常に相克するわけではない．

こうしたことを考え，筆者は，情報セキュリティの理念を次のように規定している．「技術，管理・経営・市場メカニズム，法制度，倫理，心理，行動論などを強く連携・密結合させて，自由の拡大，安全性の向上，プライバシの保護という相互に矛盾しがちな 3 つの価値を可能な限り，同時に満たすような総合的対策を定常的に行うプロセスである」（図 -1）．

次に，このような情報セキュリティを学問的立場から考えてみよう．筆者は，1993 年以来，情報セキュリティ総合科学の構築を提唱してきたが [3]，特に，2004 年，21 世紀 COE のリーダや情報セキュリティ大学院大学の学長を務めながら，情報セキュリティ総合科学について考え続けている [4, 5]．さて，科学とはなんだろうか．科学を自然科学に限れば，神は自然を無矛盾に造ったという信念から，矛盾にぶつかるたびに，それを解消するように理論を構築してきた面が強い [6]．しかし，情報セキュリティ技術は，自然法則を直接利用することは多くない．情報セキュリティを支える理工系分野は，数学，論理学，数理科学，情報科学，ソフトウェア科学，システム科学などであり，これらをまとめて論理・システム科学と仮称することとする．

Weyl が「多くの数学者は，Gödel の不完全性定理など，辺境地帯の国境紛争くらいにしか考えていない」と言ったように，不完全性定理を重く見ることはないにしても，論理・システム科学を無矛盾世界観の下に進めることはできない．暗号理論について言えば，なんらかの仮定，たとえば，「NP　not ＝ P」，あるいは「現在の計算機では，素因数分解は多項式時間では不可能」など，証明がなされていない仮定の上に理論を作り社会に提供せねばならない．膨大なソフトウェアに論理的誤りがないことを証明することも実際上，困難であろう．しかし，矛盾根在世界観を持ちながらも，ほぼ無矛盾なシステムを構築することは可能である．

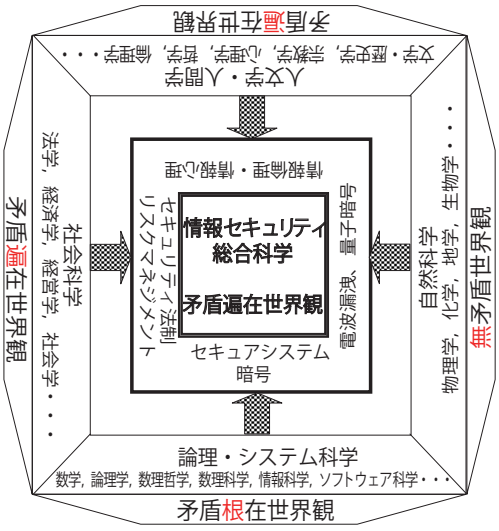

図 -2　矛盾という視点から見た情報セキュリティ総合科学の諸学の中の位置付け

これに対して，社会科学の場合はどうであろうか．理論経済学では，市場原理主義全盛の頃，自然科学たらんとする思考が重ねられたが，結局，それでは，現実の経済との整合性がとれないので，心理学や行動論，歴史，文化を総合的に見る中で，学問構築を進めるべきだとの認識が主流となっているように見受けられる．法学についても，現実社会と無矛盾な法制度を築くことは見果てぬ夢であろう．しかし，経済学も法学も，社会との矛盾を軽減し，超克すべく努力が重ねられていることは間違いない．

人間そのものを探求する学問である人文科学は，分野にもよるが，矛盾の超克というより，矛盾多き人間についての考察を掘り下げていると言うべきであるが，情報セキュリティの立場からは，人間の持つ矛盾も含めて，先に述べた理念を追求すべきであろう．たとえば，Street View は，利便性とプライバシ侵害が裏と表に張り付いているが，これは，自分のプライバシは守りたし，他人のプライバシは覗きたいという，人間の矛盾が，情報化によって拡大した面が大きい．

情報セキュリティを総合科学として捉えるとき，科学とは，叶わぬまでも現実世界との矛盾を超克するための理論を客観的な論理性をもって構築する学問であると考えられる．自然科学，論理・システム科学，社会科学，人文科学を強く連携し，総合的止揚力をもってダイナミックに構築する学問が情報セキュリティ総合科学であると筆者は考えている[7)〜9)]（図 -2）．

転―現代情報社会の教養

話題を転じよう．文芸評論の神様と言われる小林秀雄は，雑誌，文学界の昭和 17 年（1942）10 月号の座談会「近代の超克」で，「米国の機械文明は大和魂には勝てないのだよ」と述べている．同年 6 月，日本海軍は，暗号解読が大きな原因となってミッドウェイ海戦で壊滅的打撃を受けるのだが，国民は連戦連勝の大本営発表に酔っていた頃である．この座談会には当時の文化人たちが勢揃いした感があるが，多くの参加者も小林と同じ論調であり，数理哲学者，下村寅太郎の「いや，機械をつくった精神が問題なのだ」という声は少数にとどまった．

また，大平洋戦争の始まる 1 年前の昭和 15 年（1940 年），大哲学者西田幾多郎は，「自己矛盾的同一的世界の形成原理を見出すことによって世界に貢献しなければならい．そのことが，皇道の発揮と言うことであり，八紘一宇の真の意義でなければならない」と述べている．八紘一宇とは，「神の国である日本を中心として世界は 1 つ屋根の下」という狂信的な世界観である．西洋列強によるアジア侵略の歴史を考えれば，当時の庶民感情からは無理からぬところもあったのだが，理念やイデオロギーの問題は措くとして，筆者が問題にしたいのは，西田，小林に限らず，多くの評論家や文化人たちの，経済や技術に関する現実感覚である．無名の会社員でも，日米の経済力に 1 桁の開きがあることを知っていた人々は，戦勝に沸いていた頃から日本の敗戦を予想していた．

文化人たちにもそのような現実感覚があれば，敗戦必至の戦争を理論武装することはなかったであろう．

古い話を持ち出したのは，行政電子化の必然性を見ず，

前向きな提言をしない現在の評論家や作家たちと上記の文化人たちとが，重なって筆者の目に映るからである．

さて，現代人の教養とはなんだろうか．大正教養主義は個人的人格形成に重きがおかれ，戦後は大学の教養課程を中心とする大衆教養主義の時代が続いた．1990 年代の教養課程の縮退に伴って，教養の没落という文化現象が起きたが，最近，また，教養論議が復活している．

筆者は，情報セキュリティの視点から，「教養とは，遍在化する矛盾相克を超克するための総合的止揚力を涵養すること」と定義している．総合的という表現には文理連携と同時に，理念的世界と現実的世界の融合という 2 重の意味を込めたつもりである．

結―総合的止揚能力を有する人材の育成

情報化の普及に伴って，たとえば，これまで異なる価値観の下に共存していた放送と通信の連携・融合が深まっていることからも分かるように，社会のさまざまな面で，組織的・機能的連続化が進んでいる．このように複雑化し，矛盾が遍在化する社会をリードする人材の 1 つの理想像を筆者は次の 3 階層として描いている．

第 1 層　ある分野についての深い専門的学識を有すること例；暗号理論，OS，ネットワークセキュリティ等

第 2 層　専門分野とは価値観や学問的手法を異にする分野の副専門の修得による学際的能力
例；システム監査，個人情報保護法など，

第 3 層　社会システムについて総合的止揚能力
例;電子選挙に関する総合的知見から，効率性・安全性，プライバシー保護という矛盾を超克する能力

ヘーゲル哲学や応用倫理学が専門の加藤尚武鳥取環境大学元学長から，「総合的止揚能力の涵養とは面白い提案だが，実際には難しいな」と言われたが，佐々木良一(電機大) により開発されているリスクコミュニケータ [10] などの実システムの援用も含め，少しでもその方向へ展開することを期待している．

昨今，ポスドク問題が深刻になっている．筆者は現在，情報基礎論では国際的評価の高いドクター取得者らを擁して総務省の競争的資金により，「量子コンピュータに対抗し得る公開鍵暗号の研究」を進めているが，ポスドク等の就職難に窮している．専門を深く追求する研究者は，もちろん，必要であるが，一般論としては，これまでの博士課程教育が広士ではなく狭士に偏りすぎたことが社会的需要との不整合を生じた面も大学人として反省すべきであろう．上記の提案が，この問題解決の一助となれば幸いである．

参考文献

1) 電子私書箱（仮称）構想の実現に向けた基盤整備に関する検討会, http://www.kantei.go.jp/jp/singi/it2/epo-box2/index.html
2) 松崎　淳, http://www.matsujun.com
3) 辻井重男：展望―情報セキュリティ総合科学の確立を，テレビジョン学会誌，Vol.47, No.2, pp.12-15 (Feb. 1993).
4) 辻井重男：21 世紀 COE プログラム，電子情報通信学会誌，Vol.86, No.11, pp.900-905 (Nov. 2003).
5) 辻井重男：電子社会の信頼性向上と情報セキュリティ，情報処理，Vol.46, No.4, pp.405-409 (Apr. 2005).
6) 市川惇信：科学が進化する 5 つの条件，岩波書店 (July 2008).
7) 辻井重男：私の研究者歴　アナログからディジタルへそして有限体へ―総合と止揚，電子情報通信学会，通信ソサイエティマガジン，No.2, pp.4-13 (Sep. 2007).
8) 辻井重男：情報セキュリティ総合科学と現代人の教養，電子情報通信学会　基礎境界ソサイエティ，Fundamenntal Review (Jan. 2010).
9) 笠原正雄：情報技術の人間学―情報倫理へのプロローグ.
10) 佐々木他：多重リスクコミュニケータの開発と適用，情報処理学会論文誌，No.9, Vol.49. pp.3180-3190 (Sep. 2008).

(平成 21 年 11 月 30 日受付)

辻井　重男（正会員）

tsujii@tamacc.chuo-u.ac.jp

昭和 33 年東工大卒業．同大教授・名誉教授，中大教授を経て，平成 16 年～21 年情報セキュリティ大学院大学学長．中大研究開発機構教授．(財) マルチメディア振興センター理事長．工博．NHK 放送文化賞．平成 21 年春，瑞宝中綬章．著書「暗号と情報社会」等．電子情報通信学会会長，総務省電波監理審議会会長，日本学術会議会員等歴任．日本ペンクラブ会員．