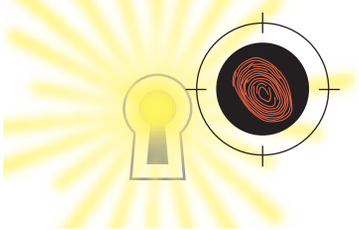
情報セキュリティ ―安全・安心な社会のために―

Information Security Technology for a Safe and Secure Society



今井秀樹

Abstract

この10年を特徴付けるのは社会の急速な情報化である．それに伴い，多くの情報セキュリティ問題が噴出し，いやおうなしにその対策が迫られ，それが情報セキュリティ技術の進展を促した．本稿では，情報セキュリティ技術のこの10年間における発展を振り返る．そこにはこの10年で大きく広がった情報セキュリティ分野の姿が見える．しかし，それは決して成熟したものではなく，むしろようやく本格的な発展のための基礎固めができたという段階である．情報セキュリティ分野は，社会の進展とともに今後更に成長していくべき分野なのである．

キーワード：情報セキュリティ，暗号，CRYPTREC，個人認証，実装評価

1. はじめに

筆者が情報セキュリティの研究を始めたのは1976年，IEEE情報理論誌に掲載されたディフィとヘルマンの論文[1]を読んでからである．この論文は公開鍵暗号の概念を初めて導入し，多くの研究者に衝撃を与えた．その後，暗号の研究は急速に進展し，情報化の普及も相まって，情報セキュリティの研究が活発に行われるようになってきた．そこで，筆者らは1984年に暗号と情報セキュリティ研究会を創設し，第一回を浜名湖畔で開催した．その後，この研究会は本会情報セキュリティ研究専門委員会主催の「暗号と情報セキュリティシンポジウム(SCIS)」として，毎年開催されている．

図1にSCISの参加者数と発表論文件数の推移を示す．この図で見るように，SCISは1990年代半ばまでは緩やかに成長しているが，それ以降の10年間急速な進展を遂げている．この曲線は我が国におけるパソコンやインターネットの普及拡大の曲線によく似ている．このことは，1990年代の後半以降，社会の情報化の進展に伴って，セキュリティ上の問題が次々と噴出し，情報セキュリティ対策が社会的要請となったため，情報セキュリティ研究分野が社会の情報化に連動して発展してきたという状況を示している．しかし，それだけではなく，情報セキュリティ技術の発展によって，情報化が推進されてきたことも見逃せない．つまり，社会の情報化と情報セキュリティの研究開発はほとんど一体化して進展してきたともいえるだろう．

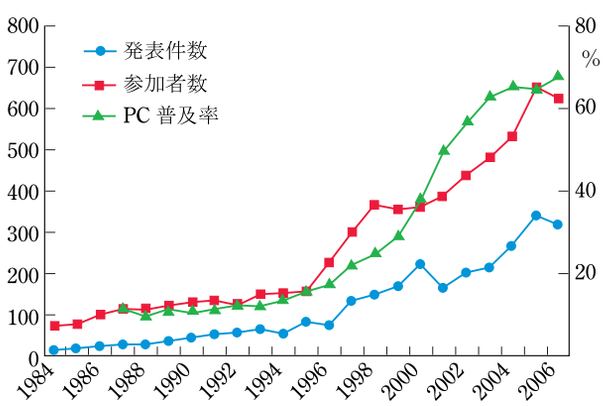


図1 SCISの参加者数と発表件数の推移　PC普及率は総務省資料による二人以上の所帯の普及率

本稿では，過去10年間の情報セキュリティ研究分野

今井秀樹　正員：フェロー　中央大学理工学部電気電子情報通信工学科
Hideki IMAI, Fellow (Faculty of Science and Engineering, Chuo University, Tokyo, 112-8551 Japan).
電子情報通信学会誌　Vol.90 No.5 pp.334-339 2007年5月

の発展を振り返るとともに，安全・安心な社会構築のために，情報セキュリティ分野の果たすべき役割について論じ，この分野の将来動向について述べる．

2. 情報セキュリティとは

情報セキュリティは「正当な権利を持つ個人や組織が情報システムを意図どおりに制御できる性質」と定義される．より具体的には，以下の三つの属性を維持することと定義されることが多い．

① 完全性（Integrity：一貫性とも呼ぶ）：情報の正確性，一貫性を維持できるという性質
② 可用性（Availability）：システムを必要とする場合に所定の方法で利用及び制御できるという性質
③ 機密性（Confidentiality：守秘性とも呼ぶ）：情報の機密性が規定どおりに守られるという性質

しかし，これで情報セキュリティがすべて説明できるわけではなく，この三つの属性は代表的なものと考えるのが適当であろう．例えば，否認拒否性（Non-repudiation：否認できない証拠が存在するという性質），責任追跡性（Accountability：情報セキュリティ分野では，説明ができるための証拠が残るという性質），真正性（Authenticity：人や情報が想定しているとおりの本物であるという性質）などの属性が要求されることがあるが，更に，最近では，回復性（Recovery：被害を受けてもそれが回復できるという性質）も重要と考えられるようになってきた．情報セキュリティの内容は確定したものではなく，社会の状況によって変っていく．

以上のような情報セキュリティを達成するための対策は単純なものではない．それは，対処すべき脅威の主体が人であり，その行為を予測することが難しいからである．情報セキュリティ対策は，技術，施設・設備・装置，管理・運用，保険，法・制度，更には教育・啓発，倫理の面から総合的に施していかねばならない．更に，攻撃者はシステムの最も弱いところを攻撃してくるから，情報セキュリティ対策は一貫性を持って統合的に施す必要がある．

このような原則の下に実効性のある情報セキュリティ対策を施すには，何らかの組織的な方策を講じる必要がある．例えば，企業や団体などの組織で情報セキュリティ対策を施すには，図2に示すように，セキュリティ担当組織・責任体制を確立し，リスク評価を行い，セキュリティポリシーを策定し，それを達成するための基準・手順を整備し，その周知を図り，訓練を行う．更に監視・監査も必要である．そして，それを支えるのが情報セキュリティ技術である．また，このような対策は一度施せば終わるというものではない．設計，導入，運用，評価の4段階のサイクルを繰り返し，様々な新たな脅威にも対処できるようにしなければならない．

3. 情報セキュリティ技術

本章では，この10年の情報セキュリティ技術の発展について述べる．ただし，図2に見るように，情報セキュリティ技術は極めて多岐にわたる．ここでは，情報セキュリティの基盤となる暗号技術，個人認証技術，実装技術，そして今後極めて重要と考えられる評価技術について述べることにしよう．

3.1 暗号技術

本節では，この10年間における暗号技術の進展を共通鍵暗号と公開鍵暗号に分けて述べる．

共通鍵暗号については，米連邦政府標準暗号の地位にあったDESの解読の研究が進み，10年前には，その現

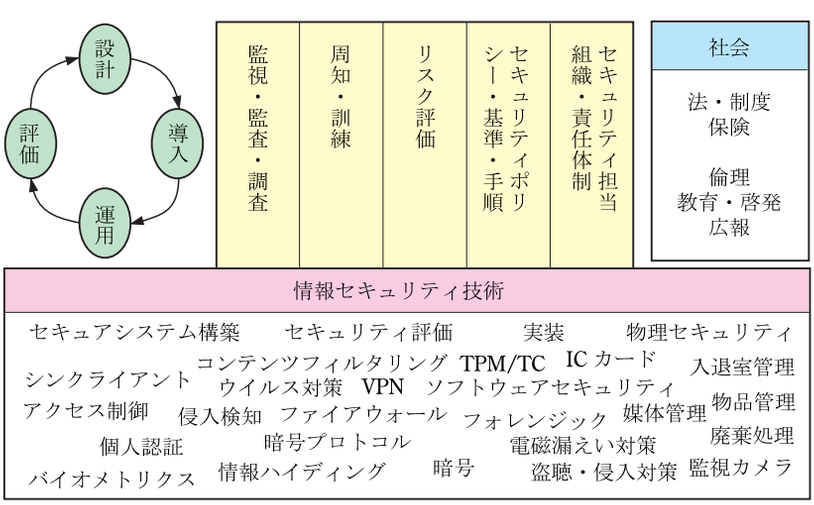


図2 情報セキュリティ対策の構造

実的な解読が時間の問題となっていた．この DES の危殆(たい)化を受けて，1997 年，NIST（米国国立標準技術研究所）は次世代米連邦政府標準暗号 AES の公募を行った．これは，新たな共通鍵暗号方式の設計と，それらに対する安全性解析に関し，世界中の多くの研究者に研究を促すこととなり，多くの優れた暗号方式が提案された．2001 年に AES が選定されるとこの動きは一段落し，以後今日に至るまでは，標準化と普及の時代だったといえよう．それを象徴するプロジェクトとして我が国の CRYPTREC と EU の NESSIE がある．CRYPTREC は 2001 年に電子政府推奨暗号の募集を行い，2003 年に電子政府推奨暗号リストを公表した．NESSIE においては，2000 年に利用推奨暗号が募集され，2003 年に選定結果が公表された．

これらの推奨暗号の選定以降，共通鍵暗号に関する研究規模は縮小していった．その結果，この分野の研究者たちは共通鍵暗号の周辺に位置する技術に目を向けるようになり，ハッシュ関数に関する安全性解析の一連の結果を生むことになる．最も衝撃的であったのは，2005 年，Wang らによって，ハッシュ関数 SHA-1 の安全性の欠陥が指摘されたことであろう[2]．SHA-1 は電子署名や様々な認証に広く利用されている基本的な関数であるため，この結果は産業界にも大きな動揺を与えた．この事態を重く見た NIST は，次世代ハッシュ関数の募集を行うこととした．また，国内においても CRYPTREC が，安全なハッシュ関数への円滑な移行などについて検討を始めている．

一方，公開鍵暗号に関しては，この 10 年間は大きな発展の時期であった．中でも，1998 年に実際に広く利用されている RSA 暗号の実装形態である PKCS ＃ 1 ver．1.5 がある種の攻撃に対しぜい弱であることが示されたことは，それまで産業界の関心を引くことがなかった証明可能安全性の概念が極めて重要なものであると認識される契機となった[3]．また，同じ年に，Bellare らにより公開鍵暗号における安全性の概念の整理がなされ，公開鍵暗号が満たすべき安全性の要件が明らかとなった[4]．更に，この年に，最強の安全性を標準的な仮定の下に証明可能な初めての実用的公開鍵暗号方式が提案され[5]，広く話題を呼んだ．その後，証明可能安全性の理論は急速に発展し，産業界にも大きな影響を与えることになった．この発展には，最強の安全性を持つ公開鍵暗号構成に極めて有用な藤崎・岡本変換[6]など，我が国の貢献も少なくない．

安全性に関する論議に関し，2001 年に提案された安全性の概念であるはん用結合性[7]は今後の一つの方向を示すものとして，特筆に値する．これは，ほとんどすべての暗号技術に関する安全性を包括的に扱う画期的な概念であり，その後提案された暗号プロトコルの多くについて，この概念の上で安全性に関する議論が行われている．

以上のように，この 10 年における公開鍵暗号研究の前半は，安全性の概念とその具体的実現法の確立が中心であった．それが収束するに従い，効率の良い公開鍵暗号や今までにない有用な付加的機能を持つ暗号の設計法についての研究も広くなされるようになってきた．特に，同報通信暗号の新たな発展[8]とその次世代 DVD の著作権保護への応用は，暗号技術の発明から実用化までの期間の短さを示す典型例として興味深い．また，新たな性質を持つ暗号技術のうち，量子計算機など強力な計算能力を持つ攻撃者が現れても破れることのない，長期的に安全な方式は，安全・安心な情報化社会の構築のために重要である．これには様々な方式があるが，更に将来を考えれば，無限の計算能力を持つ攻撃者に対しても安全な暗号技術が不可欠なものとなるであろう．そのような例として，2002 年に無条件安全性を持つ電子署名方式の概念が確立され，具体的な構成方法が提案された[9]．

2001 年，高機能な公開鍵暗号の研究は一層加速される．これは，上記のとおり，通常の公開鍵暗号の安全な設計方法に関する一連の研究が収束していったことに加え，暗号技術の設計において双線形写像の利用が極めて有用となることが発見されたためである．双線形写像を暗号に初めて用いたのは境ら[10]であったが，Boneh，Franklin[11]は，初めて証明可能安全性を持つ ID ベース暗号を提案し，暗号研究者の間で広く認知され，多くがこれに追随することとなった．ID ベース暗号は，公開鍵として任意の ID を用い得る方式であり，それ自体が従来の公開鍵基盤（PKI）に影響を与えるだけでなく，これを構成要素として用いることで新たに有用な暗号技術の創出も可能となった．

以上の暗号技術発展の概要を図 3 に示しておこう．なお，これらとは別に，極めて高い安全性を持つ暗号として量子暗号も重要であるが，これについては本特集「2．量子情報学――物理学と情報学の融合と展開――」を参照されたい．

3.2　個人認証技術

本節ではこの 10 年間に急速な進展を遂げている，人を対象とし端末を介して行う個人認証について述べる．これは，知識，所持物，生体，所在地のそれぞれに基づく 4 通りに分類される．所在地認証は郵便配達による確認や GPS を用いる認証などがあるが，余り一般的ではないので，ここでは割愛する．

知識認証は，パスワードや暗証番号など古くから用いられているものが多い．しかし，かなりの長さの文字列を記憶する必要があり，のぞき見にも弱いという欠点を改善するために，様々な方式が提案されている．例えば，孫やペットの写真など忘れることのできない画像を用いる方式や，のぞき見に強くするための質問応答方式など

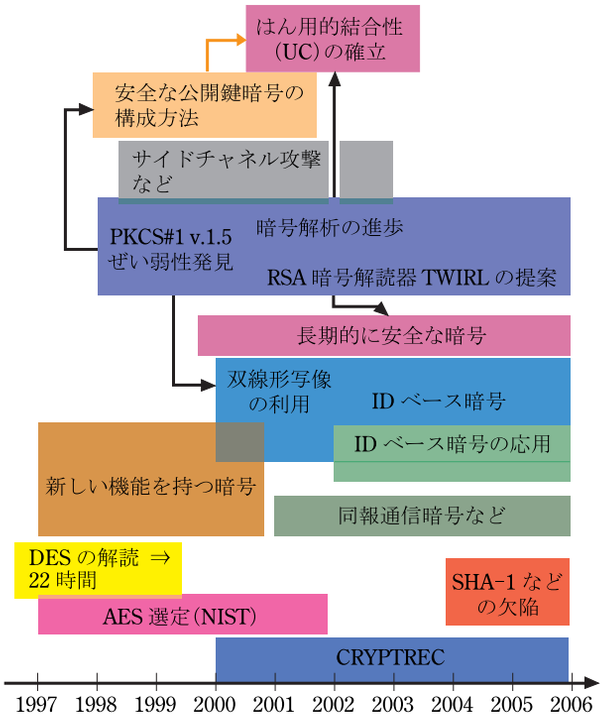


図 3　暗号分野 10 年史

がある．更に，パスワードを用いて，暗号鍵を安全に共有するパスワード認証鍵交換方式や，情報漏えいに強く，複数のシステムで同じパスワードを用いても安全性を損なうことのない方式[12]は，ユーザの負担を減らし高い安全性を達成できるという点で興味深い．

所持物認証も極めて古くからあるが，最近は IC カードを用いる方式が広がっている．磁気カードに比べて IC カードはスキミングなどの攻撃に対し強く，安全性が高いとされているが，これは方式に依存する．IC カードを用いた認証でも，リーダが IC カードの記憶を読み取って認証するだけであれば，その安全性は磁気カードとそれほど変らない．しかし，適切に設計された質問応答方式であれば，安全性がかなり高くなることは事実である．ただし，IC カードの耐タンパ性（記憶されている情報に不正にアクセスするのが極めて難しいという性質）は磐石なものではないので，強力な攻撃者には IC カードの内部情報が読み取られる可能性も想定しておかねばらなない．したがってその漏えいがシステム全体を損なうような秘密情報を，IC カードに格納するのは危険である．

IC カードのもう一つの問題点は表示装置がなく，利用者との間の直接の認証ができない点にある．これに対し，携帯電話など表示装置と計算機能を持つ携帯機器は，より高い安全性を持つ認証機能を実現することができる．しかし，携帯電話なども耐タンパ性については，まだ十分なものとはいえない．

個人認証における最近の最大の話題は生体認証であろう．指紋照合器の付いた携帯電話やパソコンは当たり前のものとなってきたし，銀行の現金支払い機では静脈認証を行うものも広がっている．確かに生体認証は，パスワードを記憶しなくてもよいし，認証用の特別な所持物も不要であるため，利用者にやさしい方式である．

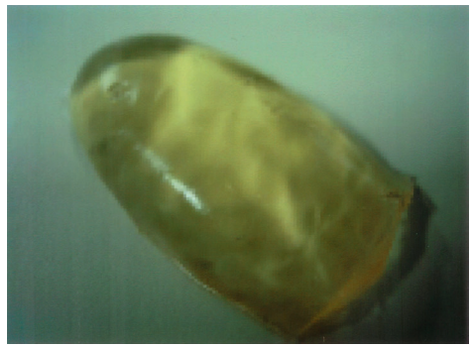


図 4　指紋付き人工指（出典：松本勉「生体部分でない対象物の展示による脆弱性評価の方法」（http://www.nmda.or.jp/nmda/bio/pdf/yokohama.pdf））

更に生体認証は安全性の高さを強調されることが多く，時には絶対安全な認証方式と宣伝されることもあった．しかし，これは 2000 年代初頭，ゼラチンなどを用いて作られた人工指（図 4）を，ほとんどの指紋照合器が正当と判定するという松本らの研究[13]により，見直しを迫られることになった．その後，静脈認証器に関しても同様な研究が行われている．

生体認証はまた，正当な利用者を拒否する確率を 0 にはできないという問題もある．この場合にどのような対処をするかによって，生体認証システムの安全性は大きく変る．このような点も含め，意図的で知的な攻撃者のなりすまし攻撃も考慮し，システム全体の安全性を評価する方法を確立することが今後の重要な課題である．

個人認証で忘れてはならないのは，多くの場合，個人がシステムを認証することも必要だということである．これまでの多くのシステムでは，一般ユーザがシステムを簡単にしかも安全に認証できる方法は組み込まれていない．しかし，それがフィッシング詐欺などの要因となることもある．様々な状況にあるユーザがシステムを簡単かつ安全に認証できる方式の開発も重要な課題である．

個人認証に関し，もう一つ考えねばならない問題は本来信頼されるべき機関から認証用個人情報の漏えいする事件が後を絶たないということである．これに対処するには，個人情報漏えいの防止を図ることはもちろんであるが，同時に仮に認証用個人情報が漏えいしても，被害が最小限に止まるような認証方式を用いることも重要である．

3.3　実装技術

CRYPTREC や NESSIE などの活動によって，暗号ア

ルゴリズムとしては安全なものが使われるようになってきたため，今日では暗号アルゴリズムが破れることはまれである．しかし，依然として暗号システムが破れたり，ぜい弱性が指摘されたりすることは少なくない．その一つの要因は実装にある．暗号機能を実現するためのハードウェアやソフトウェアの欠陥やこれらに対する想定外の攻撃によって破れてしまうのである．このため，暗号の実装評価が重要な課題となり，その評価認証システムとしてCMVP（暗号モジュール検証プログラム）が米国のNIST（米国国立標準技術研究所）によって始められた．我が国でもCRYPTRECやINSTAC（日本規格協会）などの協力を得てIPA（情報処理推進機構）が日本版のCMVPを2007年に開始した．

CMVPでは実装に欠陥がないかを検証するのであるが，このほかに様々な攻撃に対する耐性も検査しなければならない．近年盛んに研究されている強力な攻撃はサイドチャネル攻撃である．これは，実装された暗号システムから観測可能な数値を用いて暗号解読を行う手法であり，秘密鍵による処理に要する消費電力や処理時間の変動から秘密鍵に関する情報を得るという差分電力解析やタイミング攻撃が代表的である．

情報システムの実装の評価は仕様どおりに動作するかの検証はもちろんであるが，ぜい弱性がなく信頼性・安全性が確保されているかの検証も欠かせない．特にソフトウェアに関しては，これは長い歴史を持つ研究分野であるが，最近，理論化，体系化の面でかなりの進展が認められる．しかし，なお残された課題は多い．

情報セキュリティシステムでは，ハードウェアに対し耐タンパ性を要求することが少なくない．その場合には，耐タンパ性の評価が重要である．しかし，耐タンパ技術は非公開の場合が多く，その評価も難しい．したがって，現状では，耐タンパ性に過度に依存したシステムはぜい弱性があると考えねばならない．耐タンパ性に対する信頼できる評価が可能となるような仕組みを作ることも含め，評価技術を確立し，今後，耐タンパ性の評価・認証制度を構築していくことが望まれる．

3.4 セキュリティ評価技術

情報セキュリティを達成するためには，評価が極めて重要である．図5に示すように，情報セキュリティ評価は暗号の評価から大規模システムの評価まで幅広い．暗号アルゴリズムの評価は3.1で述べたように，AESプロジェクトやCRYPTREC，NESSIEなどで行われ，特に公開鍵暗号の場合，安全性は（ある仮定の下に）理論的に保証されるようになってきた．また，そうでなくても，公開された暗号アルゴリズムに対し，公的な場で多数の専門家により評価された結果の信頼性は高い．暗号アルゴリズムに関しては，十分信頼できる評価が行えるようになってきたといえるだろう．CRYPTRECでは更に，暗号実装や暗号プロトコルに対する評価も同様な手法で行っていくことを計画している．

これに対し，大規模システムの評価は，良いと思われるシステムと同等なことが行われているかをチェックする適合性評価か，あるいは何らかの攻撃を仕掛け，それに対する反応を見る侵入試験などによる評価に止まっている．これらの評価によって安全性が高いということはできるが，保証することはできない．今後，安全性を理論的に保証できる範囲を拡大していくことが望まれる．

また，情報システムのセキュリティ評価はいったん安全と判断されても，それで安心というわけにはいかない．

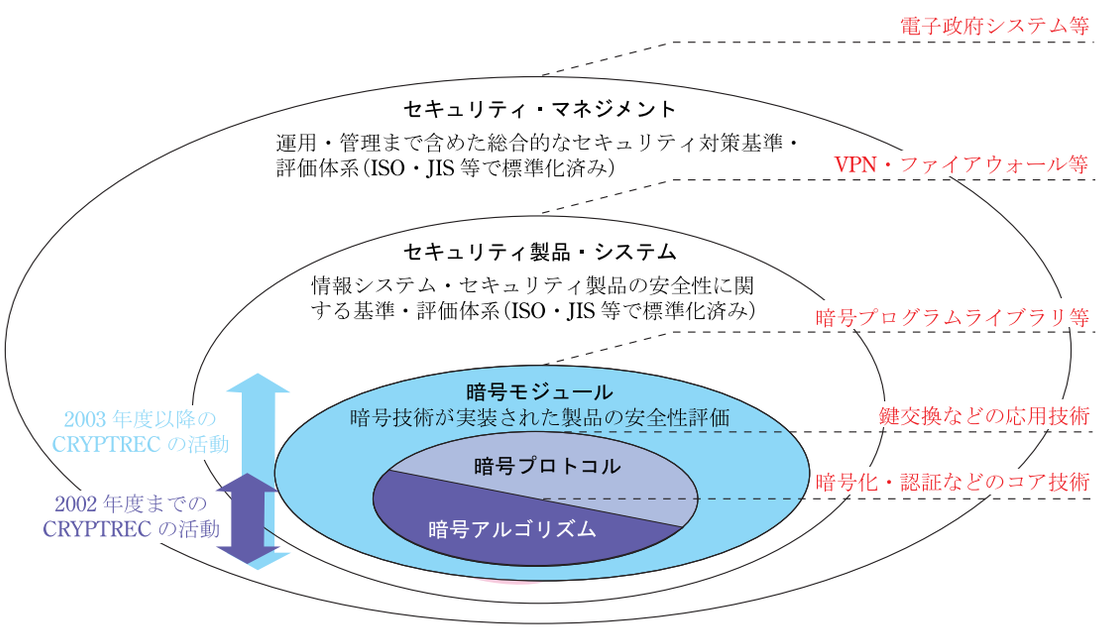


図5 情報セキュリティ評価

何もしなければ時間の経過とともに，攻撃法の進歩や利用環境の変化のため，セキュリティレベルは低下していく．このため，セキュリティの劣化を常に監視し，必要なときに再評価する必要がある．CRYPTREC でも電子政府推奨暗号のセキュリティレベルを監視し，劣化が認められれば必要な処置をとることとしている．

4. 情報セキュリティの今後の展開

この 10 年の情報セキュリティ技術の歴史は，それらが現実の社会の安全・安心の実現を目指し，人や社会との接点をより広く，深くしつつある過程であったということができる．今後も，情報セキュリティにおける人的側面，社会的側面の比重は大きくなる一方であろう．

筆者は 1990 年代の初めに，人と情報システムのかかわりの部分における暗号技術をヒューマンクリプトと名付け，その重要性を強調してきた．それは例えば，知識認証において，3.2 で述べたような成果を生んできた．また，最近米国の電子投票において，自分の票がカウントされていることを実感できないことが大きな欠陥として指摘され，それに対するヒューマンクリプト的な立場からの改善策が提案されている．

人という要素は，適切に扱わないとシステムの安全性を損なうという点は確かにあるが，逆にシステムの安全性を高める要素ともなる．人は機械では代替できない能力を持ち，また，意外に頑健な面もあるからである．更に，人は気配や勘で危険性を察知してきた．まだ，十分には解明できないリスクセンサを持っているといえるかもしれない．今後，情報セキュリティシステムはこのような点で，人に学ぶことも必要であろう．

既に述べたように，情報セキュリティは本質的に社会とのかかわりが深い．このため，情報セキュリティには社会科学的アプローチも必須であるが，まだ余り進んでいない．更に，より近い分野にも，連携すべき相手として，ディペンダビリティ分野がある．情報セキュリティが意図的で知的な攻撃を主たる対象にするのに対し，ディペンダビリティでは，故障や災害や人のミスを主たる対象にするという点で異なる面があったが，安全・安心を実現するには両者に対し総合的に対処していかねばならないという認識から，情報セキュリティ，ディペンダビリティの両者を含む新分野が形成されつつある．そこでは，人的側面や社会的側面に対し，正面から取り組んでいくために，社会科学の多くの分野と連携していくことが必須とされる．このような新分野から，安全・安心の実践的な学問体系が生まれることを期待したい．

最後に，情報セキュリティと社会との深い関係を考えると，情報セキュリティの研究者・技術者には社会とのコミュニケーションを積極的に拡大していく責務があることを付け加えておこう．社会が情報セキュリティ及びその技術に関し，正しい理解を持つことが安全・安心な社会を構築する上で極めて重要だからである．このような点で，本稿が少しでも役立てば幸いである．

文　　献

（1） W. Diffie and M.E. Hellman, “New directions of cryptography,” IEEE Trans. Inf. Theory, vol.22, no.6, pp.644-654, 1976.

（2） X. Wang, Y.L. Yin, and H. Yu, “Finding collisions in the full SHA-1,” Proc. of CRYPTO ’05, pp.17-36, 2005.

（3） D. Bleichenbacher, “Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS ＃1,” Proc. of CRYPTO’98, pp.1-12, 1998.

（4） M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, “Relations among notions of security for public-key encryption schemes,” Proc. of CRYPTO ’98, pp.26-45, 1998.

（5） R. Cramer and V. Shoup, “A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack,” Proc. of CRYPTO’98, pp.13-25, 1998.

（6） E. Fujisaki and T. Okamoto, “Secure integration of asymmetric and symmetric encryption schemes,” Proc. of CRYPTO ’99, pp.537-554, 1999.

（7） R. Canetti, “Universally composable security: A new paradigm for cryptographic protocols,” Proc. of FOCS ’01, pp.136-145, 2001.

（8） D. Naor, M. Naor, and J. Lotspiech, “Revocation and tracing schemes for stateless receivers,” Proc. of CRYPTO ’01, pp.41-62, 2001.

（9） J. Shikata, G. Hanaoka, Y. Zheng, and H. Imai, “Security notions for unconditionally secure signature schemes,” Proc. of EUROCRYPT ’02, pp.434-449, 2002.

（10） R. Sakai, K. Ohgishi, and M. Kasahara, “Cryptosystems based on pairing,” Proc. of SCIS ’00, no.C20, 2000.

（11） D. Boneh and M.K. Franklin, “Identity-based encryption from the Weil pairing,” Proc. of CRYPTO ’01, pp.213-229, 2001.

（12） S. Shin, K. Kobara, and H. Imai, “A simple leakage-resilient authenticated key establishment protocol, its extensions, and applications,” IEICE Trans. Fundamentals, vol.E88-A, no.3, pp.736-754, March 2005.

（13） T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, “Impact of artificial “Gummy fingers” on fingerprint systems,” Proceedings of SPIE, vol.4677, pp.275-289, 2002.

（平成 18 年 12 月 4 日受付　平成 18 年 12 月 29 日最終受付）

今井　秀樹（正員：フェロー）

昭 46 東大大学院工学系研究科電気工学専攻博士課程了．工博．昭 59 横浜国大教授．平 4 東大教授．平 18 中大教授・東大名誉教授．平 17 産総研 RCIS センター長兼務．本会理事，監事，IEEE IT-SOC 会長，IACR 理事等歴任．CRYPTREC 委員長．日本学術会議会員．IEEE フェロー，IACR フェロー．