講演録　情報セキュリティーの現状と動向

上田　正尚
経済団体連合会防衛生産委員会
事務局長代理

注：本章は、2001年９月17日に日本国際問題研究所において開催された研究会での講演内容を収録したものである。

１．はじめに──情報セキュリティーの背景

本日は、少し広い視野からITの問題と情報セキュリティーをめぐる枠組み、法制化の取り組みに関し、特に日米欧の対応を比較した部分を中心に説明し、今後のあるべき日本の対応についてお話ししたい。

IT革命とは、単に技術革新ではなく、社会の色々なシステム自体を変えていく原動力となるものである。ビジネスの世界で言えば、それによりビジネス・モデルが変わることであり、軍事の世界で言えばRMA（軍事革命）に相当するような世界である。実際、ビジネスの世界では、IT革命、特に情報技術の成果を用いた業務プロセスの革新が既に米国で行われ、生産性を高めた企業は成功し、次のフェーズに移るといったニュー・エコノミーでもあった。バブルが弾けても、IT革命がビジネス・モデルに大きな変革を齎したのは確かである。

その中で特に電子商取引を見ても、２年位前の数字だが、米国ではB to C（ビジネス対コンシューマー）のマーケットでは、大体２兆円強の規模があった。当時、日本は650億円と、かなり差があったが、日本でも大体2003年頃には４兆円規模になると言われている。電子商取引のマーケット自体もこれから非常に伸びていくと言われ、まだまだ潜在的成長力のある世界だが、その一方でIT革命には落とし穴もある。それは、スピードが速くなり便利になっている一方で、ITを支える法整備、管理、監査、情報セキュリティー、倫理といったインフラ整備が追いついていないという根本的な問題で、これに十分に対応出来ていないのが現状である。特に信頼性の部分で、B to B（ビジネス対ビジネス）の関係になってきた場合、ここにおけるセキュリティーの不安は致命的になる。やはり、これに関して技術的に解決していく方法と同時に、ルールづくりが重要なテーマとなる。今日は、その辺りを中心にお話しできればと考えている。

２．米国、欧州、日本における情報セキュリティーの施策

(1) 日本の情報セキュリティーの現状

日本は、情報セキュリティーにおいてかなり後進国のレベルにあると言わざるを得ない。一昨年６月に、ISOで電子商取引の国際共通評価基準（The Common Criteria for information Technology Security Evaluation）をつくった時にも、日本はその制定作業にほとんど加わっていなかった。要するに、この分野の世界標準づくりに参加出来ていない。また、ハッカー等の不正アクセス行為の禁止等に関する法律も昨年制定されたが、これも日本の対応は遅れており、後追い的に対応せざるを得なかった。世界の状況から見ると、欧米からかなり遅れた形で情報セキュリティーの整備を行っている状況にある。

わが国では、社会基盤の変化に伴い、高度なサービス提供、低コストシステムの構築といった非常に高い水準の基盤が要求されるようになった。例えば通信、電力、ガス、水道の安定供給の点では、今までのシステムでは現場と制御系ネットワーク、制御系の情報ネットワーク、そして情報系ネットワークは別々に運営されており、相互に干渉することはなかった。しかし、今後は相互に高度なシステム制御を行っていく状況の中で安定したサービスを行う為に、それぞれ別系統だった制御系や情報系ネットワークが全部結合されてゆく。それにより、管理制御システムがインターネットを通じて外部と接点を持ち出すのだが、こうした重要な社会ライフラインが今、非常に脅威に晒され易い環境にある。例えば、証券市場にハッカーが進入して攪乱し、そこが全部止まった場合の影響は、電力・情報通信のストップ等の様々な影響を考えると、９月11日の米国同時多発テロ事件にも匹敵するだろう。

情報システムにおける具体的な脆弱性の部分としては、物理的要素、ハードウエア、ソフトウエア、記録メディア、電磁放射、通信、要員を指摘できる。この中で、情報システムにおいて最も脆弱なのは、実は要員の管理だと言われている。

また、情報システムに対する脅威を整理すると、あるシンクタンクの調査によれば、自然災害および物理的脅威（火災による被害等）は、現状では20%程度である。これに対し、意図しない事故（大半はハードウエアやソフトの不備や故障、他は使用者の誤操作）は55%と非常に多い。ハッカー等の意図的な攻撃が25%となっている。

現在、いろいろ問題になっているのは、いわゆるマリシャスコード、すなわちウイルス、ワーム、トロイの木馬といった悪意を持ったソフトウエア・プログラムである。ハッカーは、目立ちたい、憂さを晴らしたい、試してみようといった程度の動機でこうしたものをつくり、意図的な攻撃（攻撃とまで言えるかどうかわからないが）を行っている。

次の段階は情報戦である。今日、情報システムへの脅威を国家レベルで組織的に駆使する

ことも可能となっている。先述のようなライフラインに対する情報システムからの攻撃の可能性もあるので、それへの対応としてセキュリティーの確保が課題となる。

情報戦に関して米国防総省は、「おのれの情報と情報システムを防御しつつ、敵の情報と情報システムに影響を及ぼすことによって、国家の軍事戦略のための情報優位を達成するために行う活動」と定義している。実際の情報戦は民生、経済、政治、軍事まで跨る広範囲なものだ。最近はInformation Operationの中の軍事面だけをInformation Warと言うように、国防総省では定義されている。

また、国防大学の定義によれば、情報戦には次の７つの分類がある。

・指揮統制戦――敵の指揮系統を混乱させることを目的とした情報戦
・諜報基盤戦――情報システムから敵の指揮系統、敵の作戦や意思等を入手することを目的とした情報戦
・電子戦――敵の電磁波を妨害するような戦い
・心理戦――特にインターネット等を利用し、敵に心理的な動揺なり、煽動をする
・ハッカー戦――コンピューター・ネットワークへの攻撃
・経済情報戦――敵の経済基盤を混乱させる
・サイバー戦

また、情報戦には次のような特徴がある。まず、情報戦は国家基盤、特にエネルギー供給、通信、経済、輸送、生産といった部分に直接影響を与える。次に、地理的・空間的・政治的境界線がない、つまり従来の国境という概念がこの戦争では全くない。そして瞬時性を持ち、リアルタイムで行われる。テロとの関係で言えば、重要なのは低コストで遂行が可能なことである。パソコン１台で情報戦を仕掛けることが可能で、最も安い凶器となる。それから、これも非対称性の一つの例として、対象国の情報化の進展度合いによって、効果が全く違うという状況が生じる。情報化の非常に遅れた国に対しては、情報戦は全く仕掛けられない。逆に米国のような国の方が脆弱性を持っているという非対称性がある。

では、具体的に情報の保護とは何か。

・可用性（availability）――情報を利用者が適切に利用できること
・完全性（integrity）――情報内容が正しく維持されていること
・秘密性（confidentiality）――正規利用者以外情報にアクセスできないこと

これら３つをバランスよく維持することが、情報の保護である。

情報の保護に向けたセキュリティー対策として、管理的対策、運用的対策、技術的対策、

物理的対策といったものがある。

(2) 情報セキュリティーの施策――米・欧・日の比較

現状での米国、欧州、日本での情報セキュリティー施策を比べると、次のような特徴がある。米国の場合、情報セキュリティーは国家安全保障上の最重要項目であるとの観点から、国家レベルで統制をとって取り組んでおり、まず大統領令が出され、それに基づいて国防総省及びその他行政官庁が省令等を整備するといったトップダウンの仕組みになっている。欧州の場合は、米国への対抗上という感じもするが、米国とは異なる欧州域内での統合した情報セキュリティーの枠組みをつくろうとする動きが顕著に見られる。日本の場合は、各省庁がある種ばらばらに取り組んでおり、情報セキュリティーについて統一的な施策を米国並みに打ち出すまでには至っていない。

情報セキュリティーへの米国の取り組みをもう少し詳細に紹介すると、米国において、情報は、大きく「秘密区分指定情報」と「センシティブ情報」という２つに分けられている。秘密区分指定情報とは、よりセキュリティーの高い、軍事情報に近いものであり、センシティブ情報とは、軍事情報以外の民間、あるいはプライバシーに関わる情報を含むものである。基本的には秘密区分指定情報については国防総省、センシティブ情報については商務省が中心になってそれぞれ規則、基準、ガイドラインを定めている。この枠組みは、コンピューター・セキュリティー法が出来た時につくられた。

米国の情報セキュリティーを施行する際の最高法規は、1995年の「秘密の保全に関する大統領令 Executive Order 12958」である。実はレーガン時代にも情報セキュリティーに関する大統領令が出されているが、これは基本的には国家として秘密を秘匿するための施策という位置づけが強かった。これに対し、この1995年の大統領令では時代情勢を反映し、秘密情報を国民にある程度開示していく仕組みと同時に、ITの進展、技術革新に対応したセキュリティー対策をきちんとやるべしといった内容になっている。

具体的には、秘密指定期間、秘密区分指定の自動解除に見られるように情報の開示性を高める一方で、不正アクセスに対しては技術的・法的に十分な措置をとる指令が出されている。これを受ける形で国防総省、およびそれ以外の政府の対応が出されている。国防総省からは同省のセキュリティー要求事項DoD5200.28が出され、これに基づいて軍のセキュリティー対策が出来ていく仕組みになっている。

また、国防総省内部だけでなく、企業に対するセキュリティー要求事項もある。NISPOM（National Industrial Security Program Operating Manual）では、国防総省と契約関係にある企業に対しても、国家機密情報の保全について細かい規則が制定されている。米国の場

合は、トップダウンでセキュリティー対策がつくられていく流れになっている。

米国の取り組みをまとめると、時代情勢に応じてセキュリティーのあり方が変わっていることがわかる。トップダウンで情報セキュリティーを指令する。それに加え、関連組織の充実や民間の参加、教育がある。ビジネス・スクールでも情報セキュリティーを教えている。それに基づいて規則、標準、ガイドラインを作成するとともに、併せて監督、評価・認定もする。省庁間の責任と権限を明確にしていくプロセスがとられている。

欧州の方は、欧州連合（EU）の誕生もあり、欧州内での統合した情報セキュリティーの枠組みづくりに非常に熱心である。特に電子商取引に関する規則、標準への取り組みが大変進んでいる。例えば、電子商取引に関する欧州のイニシアチブや、デジタル署名と暗号に関する欧州の枠組み等々が挙げられる。その一方、OECD加盟国が多いので、OECDのガイドラインの策定と合わせていく感じがあり、欧州と米国による電子商取引等をめぐるグローバル・スタンダードのせめぎ合いといった様相を呈している。自分が出席したOECDの認証に関する標準づくりの国際会合では、やはり米国対欧州という構図になりがちだった。米国は大統領令という形ではじまり、最後の規制を行う段階になると、民間団体の自主的なコードが導入されるのに対し、欧州の場合は国家による規制を行うトーンが強い。

さて、情報セキュリティーに関するわが国の取り組みだが、わが国は1980年代後半から郵政省、通産省、日銀が個別に動き出し、1990年代に入り省庁間電子文書交換システム、電子政府の構築関連で各省が検討を開始している。現在、電子政府の基盤づくりのためということで、総務省や法務省でも電子認証の仕組みが検討されている。ただ、米国のような情報セキュリティーに対する統一的取り組みではなく、個別対応で来ており、国家安全保障的な観点があまり強く出ていない。防衛庁でも、内部での情報のやり取りに関するセキュリティーの話だけをしていて、国として防衛庁がそれを全部総括しているわけでもなく、それは内閣府でもしていない。IT戦略会議でも、インフラ整備の話や電子政府に向けたいろいろな規制緩和の話は出ているが、どちらかと言えば、電子政府あるいは電子商取引、不正アクセス防止等に個々に対応している状況で、情報セキュリティーに対するアプローチや意識にかなり差が見られる。

わが国の取り組みを総括するにあたり、わが国の場合、もう一つ問題なのが電子認証等である。米国と欧州はグローバル・スタンダードで覇権を争っているが、日本の場合は必ずしも国際的な協調を狙った施策に打って出ることはなく、完全に欧米諸国から遅れをとっている。本当はこうした仕組みづくりに参加していかないと、今後こうした分野ではなかなかリ

ードできないのだが、ひとつに各省庁ばらばらということにも原因があろうかと思う。

情報セキュリティーへの取り組みに関する各省庁の指針は、基本的には企業の情報システムに対するセキュリティー慣行について、基準やガイドラインの形で示しているのが現状である。実際、電子商取引を除くと、情報セキュリティーへの国家レベルの施策は著しく遅れている。ちなみにわが国が肩を並べている分野は、暗号アルゴリズムと電子商取引関連施策の一部分である。

３．情報セキュリティーの法的問題──情報化の進展と法制度

セキュリティー技術、これは、ハッカー対策やその他もろもろの攻撃から情報社会を守る一つの手段だが、その存在と同時に、秩序形成の手段としては法的な保護がある。しかし、保護と規制のバランスは非常に難しい。一方で技術革新が猛スピードで進んでいる。電子商取引、暗号、電子認証等のグローバル・スタンダードをつくる際にも、技術がかなり動いているので、そこで固定してしまうと止まってしまう。暗号も常に上の段階にどんどん進んで行く。その辺りの保護と規制のバランスが、情報セキュリティーの分野では非常に難しいと言われている。

ペーパーレスということで、契約書をはじめ、ネットあるいはデジタル的に処理していく時に問題になってくるのが、認証・電子署名である。電子署名は、紙の世界で言うと印鑑になるのだが、それに相当する印鑑証明書を発行する機関がある。今は公開鍵が一般的なので、各国ともその公開鍵の基盤整備を一生懸命行っているのが現状である。

プライバシー保護については今、欧州とアメリカ、日本で大分軸が分かれている。欧州はEU指令により公的分野・民間分野を含めて、国による保護と法律で規制しようという状況にある。これに対し、日本・米国では、公的分野はプライバシー保護法で、民間分野については民間のガイドラインで行う状況にある。

不正アクセス防止については、OECDから1986年に「コンピューター犯罪－立法政策の分析」というペーパーが出ている。そこで不正アクセスを含むコンピューター犯罪に対し、各国の刑法でどういう対応ができるかが検討され、欧米各国とも法制化がかなり進んでいる。1998年のバーミンガム・サミットで急速な法整備が義務づけられ、日本も1999年にいわゆる不正アクセス法を制定している。

情報化社会の秩序形成において、暗号は最も重要な技術的ファクターであり、犯罪や不正行為を防ぐにはこの暗号が非常に重要となる。そして、その使用や輸出を規制しようという考えと、緩めようという両方の考えがある。当初は安全保障的な観点から、デュアル・ユースの対象ということでかなり規制をしていたが、1998年のワッセナー・アレンジメントの暗号関連の輸出に関する規制緩和により、かなり緩められた。実際、認証や電子署名を実行する為の製品、衛星放送受信機等がそうした規制から除外されるようになり、一定強度以下の暗号製品も規定から除外さ

れた。ある程度の暗号の普及をあまり行うと、それが悪用されてしまうというジレンマはあるが、今は若干緩和の方向にある。情報セキュリティーにおける法律問題の難しさは、技術進歩と規制のバランスをどう取るかにあり、スタンダードをつくる際にもどこで打ち止めするかが課題となっている。

４．セキュリティー評価制度

利用者がIT製品を安心して選定あるいは利用できるようにするためには、IT製品に対するセキュリティー評価制度が必要になってくる。

ここで言うセキュリティー評価とは、予め定められた評価基準にしたがって、開発者あるいは利用者とは独立した第三者が製品を評価する仕組みである。一般的には、その評価（Evaluation）と認証（Certification）をすることである。開発者側からすると、そうした信任に基づいて信頼できる製品開発ができ、製品の信頼性と市場流出が高まるという効果がある。欧米ではもう80年代後半から次第に確立されてきているが、日本では残念ながら、このIT製品のセキュリティー評価制度が確立されていない。

米国では既に1985年、国防総省がTCSEC（Trusted Computer Security Evaluation Criteria）をつくっている。これは通称「オレンジブック」と言われており、国防総省に納入されるIT製品についてはこの評価に基づいてランク付けがなされている。

米国の動きを受けて、欧州でも同じような欧州標準が整備されている。

最後に、国際的な形で、国際共通評価基準がある。1993年、米英独仏蘭加によるCC（Common Criteria） Projectが始動する。96年にその第１版ができ、これが国際的な共通評価基準となった。99年にはISO15408が制定され、これがIT製品の評価基準のCriteriaとなったわけだが、残念ながら日本はこの制定作業に参加できなかった。

評価とは製品が開発された段階での評価・認証ということだが、情報セキュリティーで重要なのは１回限りの評価ではなく、ライフサイクル・セキュリティー管理という概念である。ライフサイクル・セキュリティー管理とは、システムの開発、運用、廃棄に至るまでのセキュリティー管理であり、継続して評価・認定をしていくことである。実際システム自身もアプリケーション、基本ソフトも含めて、バージョンアップし、変化していく。さらに脅威自体も変化するし、情報技術の進化もある。そして当然、脆弱性も増していく。こうした中で、一つのライフサイクルを通じて評価・認定を継続していくことが今、非常に重要視されている。

日本ではシステム開発とセキュリティー対策が一緒になっているが、米国の場合はシステム開発とセキュリティー対策を別のグループが行っている。当然、国防総省でも別々の組織でやっている。システムの運用責任者がセキュリティーの責任者ということで、権限を別々に分け、管理する形になっている。

なお、情報セキュリティー管理に用いられるセキュリティー技術としては、暗号技術、デジタル署名技術、識別認証技術、マルチレベル・セキュリティー技術（資格に応じて、どこまで入っていけるかの峻別）、ネットワーク・セキュリティー技術、ウイルス対策技術などがある。

５．わが国の情報セキュリティーへの提言

最後に、基本的にわが国の情報セキュリティーはどうあるべきかについて、日本の課題を５つほど指摘したい。まず、第１にITの発展、それを使ったエレクトリック・コマース、電子ビジネス産業の勃興というのは非常にめざましいが、利便性、効率性、効果といった技術的な成果に目を奪われて、その落とし穴である情報セキュリティーへの取り組みが非常に遅れている。

第２に、いわゆる印鑑とか紙ベースの保全から脱却しなければならないのに、わが国では依然としてその辺りの認識がないのではないか。ビジネス・モデルも変わりつつあり、技術は変わったが、仕事の仕方の変革に対する意識が弱い。

第３に、日本の場合、やはり情報セキュリティーに対するトップの認識が低い。IT導入については、トップも旗を振っているが、情報セキュリティーに関しては経営トップの認識がほとんど無いとは言わないが、危機意識はほとんど無いのが日本の現状である。欧米の経営トップの意識とはかなり違いがあるのではないか。

第４に、国際社会に貢献するルールづくりにおいて非常に遅れを取っているので、他の国と連携してイニシアチブをとってもいいのではないか。ITの技術分野では先進国だが、情報セキュリティーに関しては後進国状態である。ビジネス・モデルも含めて、カルチャーが変わっているのだが、そこにインフラが意識として追いついていないのではないか。

そして第５に、日本では国民に対する情報セキュリティー意識の教育がまだあまりなされていない。

従って、やはりもう少しIT全般の法、規則、標準といった辺りの整備を至急やらないと非常にまずいのではないか。政府はIT戦略を打ち出しているが、それを進めていく上でのインフラ部分は、日本の場合必ずしもまだ整っていない。