

### Point

不測の事態が発生した際に組織として対応するべく、リスクマネジメントや、危機管理といった安全性・信頼性確保の手法が確立されてきた。一方、インターネットの爆発的な普及を背景に、近年ますます活発になりつつあるサイバービジネス分野では、事故や犯罪が急増し続けており、経営的、法律的、社会的、国際的問題として顕著化している。

これらの問題を解決するために、自然災害や事故などの偶発的なリスクを対象として考えられてきたこれまでの危機管理の発想を、改める必要はないだろうか。そのような見地から、IT時代の問題点、本質、想定される危機と災害の形、そして対応策を検討・分析し、IT時代にふさわしい危機管理の在り方を探る。

この記事は、2001年11月10日に開催されたシステム監査学会主催の「設立15周年記念公開シンポジウム」で発表された講演の内容を一部改訂して掲載するものです。

## 『e社会の危機管理』

- 増幅されるリアルな社会の問題 -

放送大学教授 林 敏彦

「e社会には、普通の社会とは違う危機管理の発想が必要か」という問題意識から考えてみたい。結論からいえば、e社会特有の危機管理の難しさがあり、また、e社会であるがゆえに、リアルな社会に潜在的に存在している危機問題が増幅されるという問題がある。

### e社会の問題点とインパクト

e社会という言葉は、2001年1月に政府が「e-Japan 戦略」という計画を発表したことが基になっている。この計画で影響を受ける分野として、教育、芸術・科学、医療・介護、就労、産業、環境、生活、移動・交通、社会参加、行政が挙げられているが、一つだけ政治の分野が抜けている。それは政府が作る文書だからであるが、アメリカの州議会などでは、すでにネットを使った議会運営がなされている。ただ、これにより、国民、住民の意思がリアルに反映される反面、議場での迫力あるディベートが失われてきているという問題点を指摘する声もある。

総務大臣の諮問機関である情報通信審議会では、2001年7月に、「21世紀におけるインターネット政策の在り方」を報告書としてまとめているが、そこでは、インターネット利用の高度化、インターネット基盤の高度化の観点から報告が行われており、セキュリティ

や個人情報保護等も、問題点として意識されている。

e社会がもたらすビジネスや暮らしへのインパクトとしては、ネットワーク競争、電子商取引と消費者保護、情報公開と電子政府が挙げられる。

例えば、ネットワーク競争においては、昔の市場競争のように、単品対単品の競争ではなくなってきた。またVHS陣営対陣営のように、強ければ勝つというものでもない。ネットワーク競争では、味方の多いほうが勝つことになる。いい物を作っても味方が多くないと勝てない。従って、これからは標準を巡る競争になるといい。

電子商取引において、契約はどの時点で成立したことになるのだろうか。また、クーリングオフなど消費者の権利はどこまで守られるのだろうか。それに、一度ネットワークに入った情報は、人為的にそこへのアクセスを制限したとしても、情報そのものが消滅するわけではない以上、どこかの誰かがアクセスできるのではないだろうか。

個人のプライバシー保護はどこまで貫徹されるのだろうか。

情報公開と電子政府について、今盛んにいわれている電子化は、電子行政ないし電子行政サービスに過ぎない。では、電子国会や電子裁判所はどうなるのだろうか。

恐らくテクノロジーとしては、もうかなりのことが出来るのだろうが、民主主義の本質との兼ね合いで、社会としては重要な決断が必要になるだろう。

## IT革命の本質

「IT革命」という言葉がよく使われるようになったが、革命の本質は何かといえば、非常に大きな変革を伴うものであり、また「権利の再定義」ということでもある。

IT革命も、歴史上の他の革命と同様に、権力および財産権の大幅な移動が引き起こされるものである。これまで権力や財産と考えられていたものが、そうではなくなり、逆にこれまで何の価値もなかったものが新たな価値を生み出すというように、財産権の大幅な移動というところに、IT革命の本質がある。いわゆる組織における中間管理職の悲哀や流通システムの短縮化、産業構造が変化し求められる人材が変わってくることも、その例といえる。

もうITバブルは終わったと、よくいわれるが、人々がITを口にしなくなった時、つまりポストIT社会が本物のe社会であり、ITが社会の基本的なインフラになり、それこそ水や空気のような存在になった時こそが、本当のe社会と考えることが出来る。今はIT化、デジタル化していこうとしている過渡期にあると考えてよい。

## 緊急時には役立つ「マニュアル」

危機管理はサイクルで対応すべきであるといわれている。そのサイクルとは、危機発生  
緊急対応 復旧・復興 被害軽減 予防対策（危機発生）ということである。

このうち、緊急対応や復旧・復興は、起こってしまった危機に対する事後的対応であり、被害軽減や予防対策は、予想される危機に対する事前のプランニングに当たる。つまり、危機管理は、事後的なレスポンスの局面と事前のプランニングがサイクルで回ることが必要である。

日本におけるこれまでの自然災害への対応の基本的な考え方は、どちらかといえば、事前の対応にウェイトがおかれていた。それは、「起こらないようにする」、「予知する」ということであり、そのために地震予知などに膨大な人や予算が注ぎ込まれてきた。しかし阪神大震災で分かったことは、起こったらどうするかということ、だれも考えていなかったということである。

システムに関しても、起こったらどうするかという緊急対応をプランニングする必要があるが、危機が起こったときの対応として一番大事なことは、マニュアルが役に立たないということである。

危機の本質は予想もしないことが起こることであり、マニュアルは予想し得るコンティンジェンシに対する対応策をあらかじめ考えておくものであるが、危機というものは、必ず、あらかじめ考えておいたコンティンジェンシの範囲を超えて起こるものである。このことを理解しておく必要がある。

緊急対応で重要なことは、マニュアルを熟知しておいて、さあ実行するというのではなくて、予想もしない事態に対してどのように対応するかであり、これを判断するのは、究極のところ人間の頭であり、現場の人間であり、また動物的直感、人類愛でもある。

最後は、マニュアルを超えた人間性や信念、勇気が大切になってくる。危機対応マニュアルを作成したら、最後に一行、「本当に危機がきたら、このマニュアルを無視しなさい」と書いておくべきである。

## e 社会の危機要因

次に危機と災害について考えてみたい。

危機というのは、人間の生活・組織・社会システムを不安定にする重大な作用であると考えられる。また、災害というのは、社会的許容水準を超える資産価値（物的資

産、人的資産すべてを含む)の減少をいう。すなわち、人間生活に大きな影響があるときに、これを災害という。

e社会における危機要因としては、例えば、ハードとネットワーク、OS(オペレーティングシステム)と社会経済システム、アプリケーションと文化、過敏社会の病理が考えられる。

ハードとネットワークはだんだん複雑化、高度化してきており、インターコネクションで出来ているため、当然危機が潜んでいると考えるべきである。ネットワークではシステムダウンを起こすと部分的な危機にとどまらない。よくネットワークは、掛け算で出来ているといわれるが、実際、どこか一つの要素がゼロになると、ネットワーク全体がゼロになる。

OSと社会経済システムでは、例えばeコマースでは相手が見えない環境の中で、大量の注文がきたと喜んでいたら、実は向こう側では、キーボードの上を猫が歩き回っていたということが十分あり得る。こうしたところにも危機要因がある。

パソコンのOSが1社によって独占されれば、社会はそのOSにロックインされてしまい、次世代のOSへの転換が進みにくくなる。同じことは、ミドルウェアやプラットフォームにも当てはまる。

コンテンツと文化の面では、ポルノの映像がイスラム圏に入っていったらどうなるかなど、社会的な軋轢、摩擦の原因になる。電子ネットワークは社会全体を画一化、均一化の方向に向わせる傾向があると同時に、文化の衝突が起こる可能性がある。

高度情報化社会では、情報流通に関する限り、摩擦がない社会になっていくことになるが、物理的システムで完全に摩擦がなくなればシステムは非常に不安定になるのと同様に、情報流通に完全に摩擦がなくなれば、社会としては、非常に落ち着かない、不安定な社会になる。そのため、わずかなことにも過敏に反応する、過敏社会になる可能性があるとともに、スピードについていけない人も出てくる社会になる。

### 危機される複合災害

もう一つ重要なこととして、複合危機が挙げられる。これは、e社会ではいろいろなことが複合して災害を生むということである。

例えば、技術的な意味での不具合の発生と、人為的なミスが重なって大きな被害になることが考えられる。ネット災害の多くは複合災害である。

また、技術的な意味での不具合という点では、技術の制御不可能性ということも考えておかなければならない。技術を知っているのは、本当に開発の最先端の人だけになってしまうことになるため、システムのシビリアンコントロールを考える必要がある。医学における倫理委員会のようなものがネット技術においても必要になってくるかもしれない。科学の暴走、技術の暴走をどのようにコントロールするかということは非常に重要なことである。

またバーチャルな危機とリアルな危機の複合も起こり得る。例えば、戦争において、ウイルスなどにより、その国の金融システムを一時的に混乱させ、ミサイルと打ち込むというように、バーチャルティに攻撃して、その国の中枢的な産業なり、政治・指揮命令システムを混乱させ、リアルなものに被害をあたえるというようなことが考えられる。

またサイバー空間のガバナンス（統治）が重要な問題となってくる。サイバー空間は無政府空間である。ステークホルダーである企業の従業員、取引先、地域社会の人々は、サイバー空間に影響を受ける人が、非常に広範囲にわたっていることを意識しておかなければならない。そうしたステークホルダーに出来ることは、ボランタリーコンプライアンス、すなわち、自発的、自主的に、ある基準に従うということである、しかし、世界中が同じ意志で動いていないこともあり、このことは大きな課題となっている。

### 社会的、技術的研究のバランス

Garett Hardin という生物学者が 1967 年に、「共有地の悲劇」という論文を書いている。そこでは、「科学者の通弊は、あらゆる問題に技術的解決策があると誤認することであり、最後は倫理や道德の問題である」といっている。

危機管理を問題とするならば、Hardin がいうように、技術的な解決策でアプローチするには限界があり、また社会全体のことを考えていかなければならず、文系的な要素が非常に重要になってくる。

e 社会においては、「ぜひとも、社会的側面と技術的側面を同じウェイトで危機管理を研究していく必要がある」ということを最後に強調しておきたい。