ＩＴ社会を左右するサイバー犯罪（２００１・７・３）

昨年十二月末、約八千人に送信されたマザーズ市場の情報を提供するメールマガジンがウィルスに汚染されており多数の会員が被害にあった。今年一月、約二万人に送信された各種学校のダイレクトメールもウィルスに感染しており生徒から抗議が殺到した。これらは氷山の一角であり、昨年一年で情報処理振興事業協会に報告されたコンピュータ・ウィルスの発見情報は一万以上になっている。

これとは別種の問題も発生している。昨年一月、日本政府の官庁のホームページに何者かが侵入して改変したことはまだ記憶にあるが、本年三月には産経新聞のホームページが韓国から攻撃されたり、五月には中国のハッカー集団である中国紅客連盟が多数の日本企業のホームページを改竄したりと問題が続出している。さらに四月に発生した米国と中国の軍事用航空機の接触事故を契機に相互の情報攻撃が激化しているといわれる。

ＩＴ革命が進展し、生活や仕事が便利になる裏側で、サイバー犯罪とかサイバー戦争などといわれる問題が急増しているが、それらは従来の犯罪や戦争とは様相が大幅に相違している。第一に被害が広範で膨大になることである。一昨年春に台湾から発生したチェルノブイリ・ウィルスではアジア全域で数十万台のコンピュータが停止し、被害総額は数千億円と推定されている。巨大台風の被害に匹敵する規模である。第二に発生場所や発生時間が広範に拡散することである。現在ではインターネットに接続されているコンピュータは国内だけでも五千万台以上、世界全体では四億とも五億とも推定されているが、それら二十四時間中利用されている端末装置すべてが犯罪の拠点になりえる。また能力さえあれば子供でも老人でも女性でも可能であるし、メールを転送するということでは意識せずに犯罪に荷担する場合も出現する。

このような問題が発生するからといってＩＴ社会の進展を阻止することはできない。どのように管理していくかという今後の社会の課題として理解するべきである。第一には安全保障の視点を導入する必要がある。一見するとサイバー犯罪は子供のイタズラのようでもあるし、直接は人命に影響がないので深刻に理解されないが、ネットワークの破壊は道路を爆撃する以上に社会基盤を破壊し、社会全体を一気に麻痺させるほどの事件である。

第二はすべてが国際問題であるという視点をもつことである。管理が杜撰なコンピュータから侵入したハッカーは、そこを拠点に地球の裏側にある企業を攻撃することも可能である。侵入されたコンピュータには被害はなくても、結果として犯罪に荷担することにもなりかねない。最悪の場合、事件にまったく関係しなくても膨大な賠償を請求されることさえありえる。外交問題にも発展することもありえないことではない。

対策を検討する必要がある。被害を阻止する技術を用意することは当然であり、官庁も企業も研究を開始し、対応する組織を用意しているが、これは矛盾（ホコとタテ）の世界であり、完全な阻止はありえない。制度として対応する必要もある。米国は個人のプライバシー保護も一部は抑制して捜査できる法案を検討しているし、欧州が中心になって「サイバー犯罪防止条約」が提案され、日本や米国も今年後半には調印する方向にある。

逆説のようであるが、ある比率以下であれば、サイバー犯罪が発生する社会を健全とする視点も必要である。現在でも郵便や電話は脅迫や詐欺に利用されている。一種のサイバー犯罪である。しかし、それらの情報が周知されることにより、大抵は見破ることができている。一病息災という言葉もあるように、完全な管理社会よりは、病気や犯罪と共生する社会を維持するほうが健全なのだと理解することが重要である。