

善玉ハッカー、悪玉ハッカー

コレステロールにも善玉と悪玉があるように、ハッカーにも善玉と悪玉があるようです。

最近、大量のデータを送りつけて相手のコンピューターに障害を与えたり、ウイルスを送ったり、相手のコンピューターに忍び込んで勝手に情報を書き換えたり、国家や企業の機密情報を盗んだりといった深刻な犯罪が横行していますので、ハッカーといえばコンピューター犯罪と結びつけて考えてしまいがちですが、元来ハッカーというのは、コンピューター技術に長けた人のことを指しています。

彼らは、その知識技術を生かしてコンピューターの技術開発に貢献して来たのですが、中には、コンピューター技術を悪用して犯罪行為を行う者がいて、それらは本来クラッカーと呼ぶべきですが、今では、そういう人達にまでハッカーという呼び名が誤って使用されているようです。

コンピューター犯罪に立ち向かうハッカーを「ホワイトハッカー（善玉ハッカー）」と呼ぶそうですが、日本には、そうした専門の技術者が非常に不足しているといわれており、情報処理推進機構（IPA）によると、日本ではサイバー攻撃に対処する専門家が約2万5千人足りないそうです（8月14日付朝日新聞）。

今や、インターネットは、個人と個人を繋ぐコミュニケーションの道具だけではなく企業や国までひとつながりに繋げていく地球規模のネット社会を形成させるパワーを持っています。この為、コンピューターの技術を使えば、たった一人の人間の力でも企業活動を阻害し、国家の安全さえも脅かすことが可能となっています。

現に、世界ではサイバー攻撃が55億件ともいわれておりますが、悪玉ハッカーに対するセキュリティを向上させる為には国家的な規模で善玉ハッカーを養成していく必要に迫られているといえるでしょう。

この為、欧米諸国や中国、韓国などは、政府機関や企業が情報技術者の養成に力を入れており、米国のラスベガスでは、先月、世界最大のハッカーの祭典

「デフコン」が開催されました。20年目の節目に当たる今回、世界中から1万5千人ものハッカーたちが参加したそうです（8月5日付読売新聞）。

この祭典には米国安全保障局（NSA）のアレキサンダー長官が出席し、次世代の防衛網構築にハッカーの力が欠かせないと訴えたそうですが、これは、ネット犯罪に対する米国の危機感の表れであると同時に、人材確保の難しさを象徴してもいます。

一方、日本でも、経産省とIPAの主催による「セキュリティ・キャンプ」が開催されており、全国から選抜された若者を対象にコンピューターウイルスの解析法等について教育が行われていますが、ハッキングなどの攻撃方法は対象外とされているとの事です（8月14日付読売新聞）。

受講生からは「高度な技術で防御力を極める事が国や社会を守ると教えられた」との声もあり、善玉ハッカー養成に向けた第1歩としては意義があると思います。しかし、「攻撃は最大の防御」という言葉があるように、セキュリティ対策を学ぶだけでは不十分で、強力な攻撃力を身に付けてこそ、より効果的な防御方法の構築が可能といえるでしょう。

「泥棒に縄をなわせる」と諺がありますが、日本ではハッカーは犯罪者というイメージが強すぎるせいもあって、犯罪につながるような技術は教えないという考え方が依然として強いようです。しかし、企業のみならず国家に対してもサイバー攻撃が行われる状況の中では、危険な事は避けるといっていたのでは、真の安全を確保することはできません。

日本薬科大学の船山教授は、「薬毒同源」という言葉を使っておられますが、コンピューター技術はまさに、使い方によっては人類の役に立ち、犯罪の道具にもなります。その意味では、モラル教育を徹底し、情報活用能力を高めるだけではなく、善玉ハッカーの養成にも官民挙げて積極的に取り組むべきだと思います。（塾頭 吉田 洋一）