連載㉑

内海善雄（ITU前事務総局長）の やぶ睨み「ネット社会」論

サイバー・ウオー、防御が難しいDDoS攻撃

愉快犯からサイバー犯罪へ

最近、日本の防衛産業が狙われて話題になったサイバー攻撃は、どんどん新しい方法が生み出される。

原始的なものは、個人的な愉快犯である。ウイルスと呼ばれる特殊なソフトウエアを他人のPCに侵入させ、機能不全にさせるのである。ウイルスは、メールや特定のサイトを閲覧すること、あるいは特定のファイルをダウンロードすることなどにより感染する。PC内のファイルを次々とタコやイカの絵に書き換えてPCを機能不全にさせる「タコイカウイルス」が有名である。

この攻撃に対処するためには、PCで使用するソフトを最新版にアップデートして感染経路になる抜け穴を閉じ、また、最新のウイルス対策ソフト（ワクチン）をインストールして感染を予防すること、また、感染した場合はウイルスを早急に除去することが重要である。犯罪者は新種のウイルスを製造し、専門企業がその対策ソフトを作る、いわゆる「いたちごっこ」が起きているので、対策ソフトは最新のものにしておかなければならない。

次のレベルの犯罪は、明らかに窃盗を目的に行うものである。例えば、「トロイの木馬」と呼ばれるウイルスによりPC内に蓄積されたパスワード情報を取得して、他人の銀行預金を引き下ろす犯罪である。この犯罪行為から身を守るのも、前述の対策ソフトをインストールすることでほぼ可能だ。

安全度が低い日本の金融機関

日本の銀行では、パスワードと簡単な乱数表（カード）だけで本人確認をしている。使用したパスワードと乱数をウイルスなどを使って盗めば本人になりすますことが可能だ。それどころか、証券会社などは乱数表さえも使っていない。

ところがスイスの郵便局や銀行は、顧客に本人のICカードとパスワードがなければ使用できない乱数発生器を配布して、取引のつど異なった乱数で本人確認を行っている。したがって、ICカード自体を物理的に盗まない限り、本人になりすますことは不可能だ。日本の金融機関はまことに無用心だ。

最近起きている犯罪は、大量の個人情報を取り扱う企業のサーバー（中央のPC）から顧客情報を盗み出すというものである。アタックを受けた企業のみならず、情報を盗まれた多数の個人が被害を受ける。ソニーの海外子会社が襲われたケースが記憶に新しい。被害を被った個人は自分では防ぎようがないから、十分な対策をとっていなかった企業の責任は極めて重い。オンライン取引のように多数の顧客とインターネットを経由して重要な個人情報を扱わなければ成り立たない業種のシステムは、考え得る最高のセキュリティー対策をとる必要がある。日本の現状は決して十分とはいえまい。

最近の防衛産業へのサイバー・アタックは、もっぱら機密情報を狙うスパイ活動である。日常的にやり取りをしている人になりすました「標的型」と呼ばれる偽メールを送信する。安心してそのメールを開くとウイルスに感染して、システムがコントロールされ、知らないうちに情報が盗まれる。

しかし、実はこの種のサイバー・アタックに対する対策は極めて容易である。機密情報を取り扱うシステムを、端末も含めてすべて外部のインターネットと完全に遮断されたものにしておけばよいのだ。便利さを求めて外部と接続したり、経費を節減して端末を共用しているから、その隙を狙われるのである。

以上のように、インターネットを通じてウイルスを侵入させるサイバー・アタックは、鍵をかけたり、遮断したりする方法で自己防衛が可能である。要は防犯意識と経費の問題である。

ところが、専門家の間でDDoS攻撃と呼ばれているサイバー・アタックは自己防衛が難しい。これは能力以上の多数のアクセスを同時に行うことにより、システムを麻痺させるものである。防御するためには、外部からのアクセスをどこかで遮断しなければならない。アクセス源が少数であればそれも可能であるが、敵は世界各国、多数の場所から同時にアクセスを行うのである。

次々に新しい攻撃方法が生み出される

反撃したウィキリークス

暴露サイトのウィキリークスが米国の外交文書を暴露した時、何者かがウィキリークスのサイトにDDoS攻撃を仕掛けたため、誰もウィキリークスの記事が読めなくなった。ウィキリークスはコピーのサイトを各地に設置して対抗した。一方、米政府はウィキリークスの資金源を断つため金融機関に協力を要請した。怒った世界中のウィキリークス支持者たちは、DDoS攻撃のためのソフトを配布して仲間を募り、協力した金融機関にアクセス攻撃をして、金融機関のサービスを麻痺させてしまった。まさにサイバー・ウオーであった。

しかし、この種の攻撃は一人でも行える。他人のPCにウイルスを忍ばせ、持ち主の知らないうちにそのPCをリモコンして攻撃を行わせるのである。さらに、テレビや監視カメラなど、インターネットに接続された情報機器のコンピューターもウイルスに感染させ乗っ取るのである。あまり公にはなっていないが、各国で政府機関が麻痺させられたり、企業が恐喝されたりすることが頻発している。

残念ながら、皆が相乗りすることが前提のインターネット網では、DDoS攻撃を技術的に防御することは困難である。今、ITU（国際電気通信連合）を中心に開発普及を進めているNGN（次世代インターネット網）は、より安全度の高いネットワーク建設を目指しているが、これでも防御は難しい。

DDoS攻撃に対抗するためには、まずは、犯罪情報を共有し、犯罪者（組織）を絞り込んでいくことに被害者が協力し合うことが重要である。また、防犯意識を高め、世界中のコンピューターのセキュリティー・レベルを向上させて、知らぬ間にサイバー・アタックに加担していたという状況を避けなければならない。安全な情報社会のためには、これら、幅広い分野での国際的な連携と取り組みが求められている。

しかし、人権問題など政治的な問題に関連して、グーグルのメール・サーバーが特定の国からアタックを受けた事例などを考慮すると、国際的連携も容易ではない。

内海善雄（うつみ よしお）

1942年香川県高松市生まれ。東大法学部卒。東芝を経て66年郵政省（現総務省）入省。電気通信の自由化など、通信放送政策を長く担当。98年国際電気通信連合（ITU）事務総局長就任。現在は財団法人「海外通信・放送コンサルティング協力」理事長。早稲田大学客員教授。