社 説

Wanted : cyber-czars

サイバーセキュリティー強化の牽引役

Nature Vol.458(945)/23 April 2009

世界は今、コンピューターと通信網の安全性を確保するために、より強力なリーダーシップを発揮する存在を待ち望んでいる。それには研究機関も含まれる。

サイバー攻撃は、経済危機、気候変動、インフルエンザの世界的流行などと比べると話題になることは少ないが、これらに匹敵する脅威を世界に与えている。こうした脅威から市民を守るためには、足並みの揃った対策と政府によるリーダーシップが欠かせない。政府には、コンピューター・ネットワークの安全に関する研究を推進していく義務がある。しかし研究機関もまた、この問題に積極的に取り組む必要がある。最も効果的な対策の採用と普及を促し、現場の研究者に危機意識を醸成するカギを握っているのが、まさに研究機関であるからだ。

最近の大規模なサイバー攻撃の例としてはConfickerがある。このワームは昨年10月に最初に発見されて以来、全世界で1500万台ものコンピューターに侵入した。ネットワーク攻撃の回数は1990年代から急増しているが、変化はそれだけではない。以前は、こうした攻撃をしかけるのは仲間内での名声を求めるティーンエイジャーのハッカーと相場が決まっていたが、今日では、組織犯罪ネットワークが増えてきている。彼らは大量のスパムメールを送りつけ、フィッシングをし、産業スパイ活動や科学スパイ活動をして利益を得る。さらに不気味なのは、国家やその他の組織が、情報ネットワークや送電網のようなきわめて重要なインフラをサイバー攻撃の標的として見るようになってきた点だ。

米国は、サイバーアタッカーによる攻撃や、彼らの最大の資金源となっているサイバー詐欺と戦う特別な責任を負っている。ブッシュ旧政権は2008年1月に包括的国家サイバーセキュリティーイニシアチブ（Comprehensive National Cyber Security Initiative）という省庁横断的な機関を立ち上げてサイバーセキュリティーの強化に乗り出したが、この機関についての大半は機密扱いになっている。オバマ新政権は今年4月の中旬に米国のサイバーセキュリティーへの取り組みに関する独自の調査を完了した。その結果はまだ公表されていないが、おそらく、それぞれ独自のサイバーセキュリティー対策を進めている連邦機関と民間部門の間にホワイトハウスが入り、両者の調整役をつとめることを勧告する内容になると思われる。

現在、サイバーセキュリティー問題に関する2つの法案が米国上院に提出されている。1つは、サイバーセキュリティーの基準を確立し、それを施行する権限を大統領に与えるというもの。もう1つは、米国科学財団（NSF）にサイバーセキュリティー関連の連邦研究を支援させ、今後5年間、その研究と教育のために17億ドルの予算を上乗せするというものである。

動きはじめたのは米国だけではない。欧州委員会は今年3月に、サイバー攻撃の予防、発見、緩和に関する標準的なアプローチをEU加盟国に推奨し、各国のサイバーセキュリティーへの取り組みの強化をめざす計画を提案した。

これらの動きの方向性はいずれも正しいが、それを実行に移すのは大仕事である。サイバー攻撃との戦いに「勝利」はない。サイバーセキュリティーは、新たな脅威が出現するたびにさらに高度な対応が必要とされる“軍拡競争”だからだ。

ゆえに、サイバーセキュリティーの研究が必要不可欠である。しかし、米国学術研究会議（NRC）をはじめとする米国のオブザーバーの多くは、国からの資金提供はあまりにも気まぐれで、提供される研究資金も少額すぎると結論づけている。米国エネルギー省や国土安全保障省と同様、NSFはこの分野にかなりの投資をしてきた。しかし、か

ISTOCKPHOTO

つて米国のサイバーセキュリティー研究を支えていた国防総省高等研究計画局（DARPA）は、ブッシュ政権時代に短期の軍事プロジェクトに集中するため、この分野からほぼ完全に手を引いてしまった。米国議会とオバマ政権が最終的にどのような機構を設立するにしても、国としてもっと一貫性をもち、協調して研究に取り組んでいかなければならない。

しかし、サイバーセキュリティーに関して問題になるのは技術面だけではない。目下の急務は、最新の効果的な対策やツールへの関心を高め、その導入を促すことである。この点では、コンピューターに精通し、電力供給網やその他の大規模な研究ネットワークに関与している研究者が、まさに最前線に立っている。一方で、大学のサイバーセキュリティーへの取り組みは遅れている。政府がサイバーセキュリティーの牽引役と先を見越した方策を必要としているというなら、すべての大学もまたそうなのである。現場の大学研究者のほとんどは、セキュリティーの専門家になるための時間も技術もないが、ただ、そうなる必要もない。サイバーセキュリティーの文化をはぐくむという困難な課題には、ネットワークに関係する民間の研究所や公的研究機関こそが取り組んでいくべきなのである。

多くの研究者は、インターネットそのものを再設計する必要があると考えるようになっている。インターネットが開発された当時には、セキュリティーのことなどまったく考えられていなかったからである。1つの可能性は、最初からアカウンタビリティーを組み込むこと、つまり、ハッカーが自分の居場所をごまかすのを困難にするような方法で、データパケットをコード化することである。この方法にはプライバシーに関する重大な懸念があるため、ネットワーク・コミュニティーでは大きな論争が起きている。けれどもこれにより、サイバーアタッカーから匿名性を奪うことができる。真剣に考えてみる価値はある。 ■