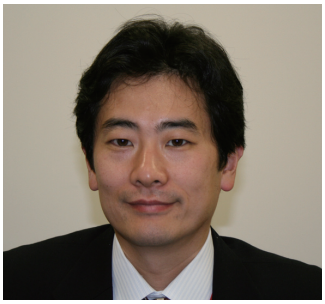
研究主幹に聞く

「サイバー攻撃の実態と防衛」プロジェクト

サイバー攻撃を止めることはできないのか



慶應義塾大学大学院 政策・メディア研究科教授
土屋大洋氏

2012年度の研究プロジェクト「サイバー攻撃の実態と防衛」の取りまとめをされている土屋大洋研究主幹に、サイバー攻撃の影響や対応の難しさについて聞きました（10月19日）。

――最近、公的機関や大学、特定の企業などに対するサイバー攻撃のニュースが報道されるようになりましたが、そもそもサイバー攻撃とは、どういうものですか。一般の企業や個人も攻撃の対象になるのでしょうか。

サイバー攻撃とは、コンピューターシステムやインターネットなどを利用して行う攻撃で、たとえば、①ウェブページの書き換え（ターゲットのパスワードを不正に入手してサーバーを操作し、ウェブページを書き換える）、②DDoS攻撃（多数のパソコンにコンピューターウィルスを感染させ、ターゲットのサーバーに対して大量のアクセスを集中させるように仕向けてダウンさせる）、③標的型電子メール攻撃（APT。ターゲットに電子メールで送って、ターゲット用にカスタマイズされたウィルス付きの添付ファイルを開かせたり、本文中に記載されたURL［ウェブサイトのアドレス］にアクセスさせたりして、ウィルスに感染させ、パソコンを乗っ取り、情報を盗んだり流出させたり、盗撮・盗聴したりする）、④ターゲットのコンピューターシステムにウィルスを感染させ（インターネットに繋がっていなくともUSBメモリなどを通じて感染する）、防空網やプラントなどを機能させなくする、などがあります（表１参照）。

イランの核施設（シーメンス社の遠心分離機制御プログラム）を使えなくしてしまった「スタックスネット」と呼ばれるウィルスは、その後、イランの技術者のパソコンからインターネット上に広まり、シーメンス社の制御プログラムを使っていた日本の水道施設も感染したと言われています。

マスコミなどでは報じられていませんが、こうした攻撃は、政府機関や特定の産業・個人に留まらず、既に、一般の企業や個人にも広がっています。その実態はなかなかつかめませんが、セキュリティサービス会社などに

表１　近年のサイバー攻撃の例

年月	事例
2000年１月	科学技術庁など政府機関サイトが改ざんされる。
2007年４月	エストニアの政府機関や金融機関などに対し大規模なDDoS攻撃。
2007年９月	イスラエルがシリア国内を爆撃の際、シリア防空網操作の疑い。
2008年	米国防総省の軍事機密を扱うネットワークがウイルスに感染し、他国のサーバーにデータが転送される。
2008年	リトアニアとグルジアでロシアからと見られる大規模DDoS攻撃。
2009年３月	カナダの研究者がGhostNetと呼ぶ秘密の情報収集ネットワークが発覚。
2009年７月	米韓に大規模なDDoS攻撃。
2009年	油田情報などを標的とした、中国のグループによる「ナイト・ドラゴン」作戦。
2009年12月	米グーグルなどのサービスを利用する中国や米国の人権活動家のメールが盗み見られるなど約30社が被害に遭う。
2010年６月	イランの原発で制御系のシステムに影響するウイルス「スタックスネット」が発見される。
2010年９月	尖閣諸島問題に絡み、中国から日本の政府機関などにDDoS攻撃。
2010年11月	経済産業省の職員にウイルス付きメールが送られ、省内のパソコン20台が感染。
2011年３月	米RSAのシステムが侵入され、使い捨てパスワードの設計情報を盗まれる。
３月	欧州連合（EU）の欧州委員会や欧州対外活動庁に攻撃。
４月	ソニーの複数のネットサービスから合計１億件の個人情報流出。
５月	米シティーグループのネットバンキングシステムから利用者の個人情報が盗まれる。
５月	米ロッキード・マーチンで外部から社内につなぐシステムを破られ侵入される。
６月	国際通貨基金（IMF）が数カ月にわたり大規模なサイバー攻撃を受けていた事実を公表。
６月	米グーグルの「Gメール」利用者数百人のメール内容が盗み見られる。
６月	米CIA（中央情報局）の公式サイトが攻撃され、利用不能に。
７月	韓国SKテレコムの子会社が運営するSNSなどから3500万人分の個人情報が流出。
８月	オランダのデジノター社の電子証明書発行システムに侵入され、500を越える偽証明書を発行。米グーグルの利用者などに被害。
2012年６月	「アノニマス」が日本のダウンロード違法化に抗議して政府サイトなどを攻撃。
７月	財務省のコンピュータ約120台が長期にわたりウイルスに感染し、情報が抜き取られていた可能性が発覚。

出所：土屋大洋著「サイバー・テロ　日米 vs. 中国」（文春新書）

は、かなりの相談があると聞きます。

――サイバー攻撃は、通常の攻撃や犯罪とどのように違うのでしょうか。それは、誰がどのような目的で攻撃するのでしょうか。

サイバー攻撃の第一の特徴は、攻撃者の特定が非常に難しいということです。サイバー攻撃の目的には、遊び・いたずら、金儲け、政治的攻撃などさまざまですが、攻撃される側から見ればどれも同じに見えます。しかも、攻撃者が、国内外のいろいろなルートを迂回して攻撃してきて、ウィルス感染の痕跡も消してしまう。たとえば、DDoS攻撃では、ウィルスに感染したたくさんの一般のパソコンが攻撃に使われます。また、中国などからの攻撃が多いと言われていますが、政府の指示によって統一的に行われているわけでは必ずしもありません。各部局がばらばらに攻撃したり、個人（民間人）や金銭でサイバー攻撃を請け負う「傭兵」が攻撃したりするなど、攻撃主体は多様であると言われています。さらに、他国が中国のパソコンを利用しているケースもあると言われています。

攻撃者の特定は非常に難しく、特定できなければ、反撃を加えることも、犯人を捕まえることも非常に困難になります。

第二の特徴は、攻撃されている側が、攻撃されていることに気づきにくいということです。特に標的型電子メール攻撃では、関係者からの正常な電子メールを装って送られて来ますので、添付ファイルを開いたり、URLにアクセスしたりしてウィルスに感染したことに気づかず、知らない間にサーバーやパソコンに蓄積された知的財産や情報が盗まれてしまうケースがあります。標的型ではありませんが、遠隔操作ウィルスに感染して、知らない間に脅迫メールの送信者に仕立て上げられた４人が、誤認逮捕されたケースも発生しています。

――それでは、わが国のサイバー攻撃への対応は、どうなっているのでしょうか。

日本政府は、サイバー攻撃に対して比較的早い段階から対策を取り始めていて、1999年８月の不正アクセス禁止法の公布を皮切りに、内閣官房情報セキュリティセンター（略称NISC。センター長は内閣官房安全保障・危機管理担当副長官補）と情報セキュリティ政策会議（議長は内閣官房長官）が中心となって、2010年５月に策定した「国民を守る情報セキュリティ戦略」に基づき、年度計画を立てて取り組んでいます。なお、これらの対応は、主に政府の重要施設や国の重要インフラを守ることを念頭に置いたもので、直接個々の企業や個人のシステムを守るものではありません。

また、警察庁の定点観測システム（全国の警察施設のインターネット接続点にセンサーを設置）がサイバー攻撃を24時間体制で監視しています。

自衛隊にもサイバー部隊「システム防護隊」がありますが、これはあくまでも自衛隊のシステムを守るためのものです。

国際的には、非政府組織ベースでは、JPCERT（Japan Computer Emergency Response Team）コーディネーションセンターが、各国のCERTとの間で連絡調整の窓口機能を果たしています。政府ベースでは、「サイバー犯罪に関する条約」が2001年に採択され、日本でもようやく関連の国内法を改正して、今年11月１日に発効しました。また、国際サイバー会議や国連でもサイバーセキュリティの問題が取り扱われはじめ、12月の国際電気通信連合（ITU）ではインターネットがITUの管轄に入るか否かが議論される見通しです。

いずれにせよ、抑止の対象となる攻撃者が誰だか分かりにくいので、完全に抑止することは難しい。

――企業や個人は、サイバー攻撃を回避することはできるでしょうか。攻撃を受けてしまったらどうすればいいのでしょうか。

企業や個人が、サイバー攻撃から完全に逃れることはできませんが、最低限自助努力で、ウィルスソフトの導入やOSのアップデート、メールの添付ファイルを安易に開かない、不要なアクセスはしない、などによってある程度は防げると思います。さらに、自分のパソコンでどのようなプログラムが動いているか、不正な動きをしていないか、モニタリングすることが重要です。自分でできなければ、プロバイダーやセキュリティサービス会社に依頼することになります。

特に企業の場合、弁護士や会計士を雇うのと同じ感覚で、情報セキュリティを確保するための専門家を雇う必要があると思います。国は、米国や韓国の先進事例を参考に、そうした人材の養成を急ぐ必要があります。

攻撃を受けてしまったら、セキュリティサービス会社などに相談して被害をできるだけ最小限に止めるしかありませんが、独立行政法人情報処理推進機構（IPA）などを通じて広く攻撃情報を共有し、日本社会全体のセキュリティレベルをあげることも非常に重要です。

インタビューを終えて

IT化の進展に伴い、サイバーセキュリティの確保は、非常に重要な課題になっています。当プロジェクトでは、一般の企業・個人にとって参考になるような報告書を取りまとめ、シンポジウムを開催したいと考えています。（主席研究員　篠原俊光）