情報セキュリティ研究者
武田圭史・慶應義塾大教授に聞く

サイバーセキュリティ*に臨め

＊目的によって呼び方が整理されている。防衛省はサイバー攻撃、経済産業省は情報セキュリティ対策、総務省は情報通信セキュリティ対策、警察庁はサイバー犯罪あるいはサイバーテロ

人事院や内閣府が運営するホームページや、三菱重工、IHI、川崎重工の防衛産業をターゲットとしたサイバー攻撃が9月18日を中心に発生した。今年4月に発生したソニーのプレイステーション・ストアや米ロッキード・マーチン、米シティグループ、韓国SKテレコムなど、世界でサイバー攻撃の被害が明らかにされ、サイバー攻撃が最近増えてきたという印象を受ける。今後、サイバー攻撃をどう考え、どういう対策を考えるべきなのか。人材の育成から担当者のポジショニングも含めて、情報セキュリティの第一人者である慶應義塾大学の武田圭史教授に話を聞いた。

（聞き手：吉井 勇・本誌編集長、構成・写真：古山智恵・本誌編集部）

セキュアな設計が前提

―― 三菱重工業株式会社（以下、三菱重工）の潜水艦や原子力発電プラント、ミサイルなどの研究・製造拠点において、社内のサーバおよびPC計83台がサイバー攻撃を受け、ウイルス感染し、情報漏洩の危険性が判明しました（9月19日発表）。4月のソニーをはじめ、企業を狙った「サイバーテロ」が世界的に増えているように思います。

武田 まず、サイバーテロという表現ですが、ソニーのプレイステーション・ストアが世界的ネット集団アノニマスに攻撃されましたが、これは情報の自由に対する抗議活動であり、サイバーテロと言えるものです。ですが、三菱重工や米シティグループの問題はソニーの場合とは目的が違います。軍事目的の三菱重工は「サイバーエスピオナージュ（サイバー上でのスパイ活動）」あるいは「サイバーインテリジェンス（サイバー諜報活動）」、営利目的のシティバンクは「サイバー攻撃」と言えるでしょう。テロとは、恐怖を与えることで政治的メッセージを伝えるものですから、サイバーテロというと、日本の政府官公庁のWebサイトを反体制メッセージで書き換えるとか、従来のテロをサイバー手段でもって行うということになります。

サイバー攻撃が増えているように感じるということですが、三菱重工のような事件に関して言えば、情報セキュリティに関わる人たちの間では、2006年ごろから政府機関や関連する団体などがサイバー攻撃を受けていることが知られていました。政府は2006年ごろから特定のターゲットを狙う標的型攻撃が来ていることを告知しており、2008年にはJPCERT（Japan Computer Emergency Response Team）コーディネーションセンターから「標的型攻撃について」という調査報告書が公開されています。今回、三菱重工は防衛技術を取り扱っており、被害状況が大きかったために公表せざるを得なかったのだと思われます。

―― 三菱重工へのサイバー攻撃は標的型攻撃？

武田 そうだと思われます。一般に特定の個人や組織を対象とした攻撃を標的型攻撃と呼び、攻撃プログラムを仕込んだ添付ファイルを送り付けるのは、その典型的な手口と言えます。

送られてきた標的型の添付ファイルを開き、ルートキット（rootkit）がインストールされてしまうと、作動中のプロセスやファイル、システムデータを隠蔽するので、ウイルスに感染したことを察知するのは困難です。ルートキット被害に遭った場合、ゼロからOSを再インストールした方が早いといわれています。

―― この状況を世の中はどうとらえているのでしょう。

武田 サイバー上のセキュリティ対策を講じていると思われていた組織が攻撃を受けたわけですから、これまでの対策の仕方では不十分だから、セキュリティ対策を見直さなければいけないという認識を持ったと思います。

―― 三菱重工に自覚はあったのですか。

武田 攻撃を受けている確認が公式に取れた最初のケースが、今回の三菱重工です。難しいのは、たとえ異変に気が付いても、実際に感染して情報が漏洩したかどうかまでは確証が取れないということです。バックドアは開いているが、盗まれているかどうかわからないという「被害が見えない」ことです。だから私たちは、情報は漏洩する、あるいはそういうリスクは存在するという前提で、業務フローや情報の提供・扱い方を考えていくよう提案しています。そのためには、これまでのようにシステムを作り上げた後でセキュリティ対策を足していくのではなく、業務フローやデータ設計の段階でセキュリティを考えて進める。セキュアな設計を前提とすることが最も重要なのです。

―― 米国などITセキュリティ問題の超先進国では、どんな議論がされているのですか。

武田 5～6年前から、設計段階でのセキュリティ確保という意味の「セキュア バイ デザイン」が提唱されています。実際の現場まではなかなか浸透していないようですが。

日本では、安全なプログラムの書き方を教えている大学は少ないのです。本を購入すれば最低限動かすためのプログラムを書くことができるので、本をまねて脆弱なプログラムを作る、それをまた誰かがまねる。だ