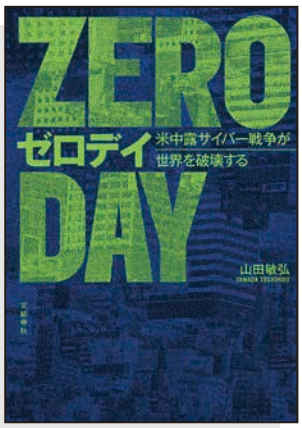
…→ 金井　遵



ゼロデイ
米中露サイバー戦争が世界を破壊する

山田敏弘 著，文藝春秋（2017），304p.，1,500 円＋税，ISBN：978-4-16-390521-1

2017 年 5 月に多数の被害を出した身代金要求型マルウェアの WannaCry など，サイバー攻撃（ネットワークを介したクラッキング行為）がニュースの話題に上がることが多くなっています．サイバー攻撃の報道では被害のみが強調され，「誰がやっているのか」はもちろん，場合によっては「何のためにやっているのか」も報道されないので全容が理解しがたく，気持ち悪さを感じている方は多いのではないでしょうか．

本書は若干過激なサブタイトルの通り，国家が関与したと言われるサイバー攻撃について，攻撃が行われた背景や利用された技術を分かりやすく解説しています．Web を検索すると特定の企業や組織により，個々のサイバー攻撃に利用された技術や攻撃者を解析もしくは推定して公表している情報も見つかりますが，情報の裏付けが不十分な場合も見受けられます．本書の最大の特徴は各国の政府関係者や軍関係者など，サイバー攻撃や防衛の当事者への取材を中心にまとめている点にあり，貴重な 1 冊です．

ゼロデイ

タイトルの「ゼロデイ」攻撃とは一般的に知られていない脆弱性を利用した攻撃のことです．攻撃されるまでに脆弱性修正パッチを当てる猶予が 1 日もないため，ゼロデイと呼ばれます．ゼロデイ攻撃は事前対策が困難であり，2000 年代中盤以降，世界はゼロデイ脆弱性の恐ろしさ，あるいは価値に気づき，脆弱性取引がビジネス化しています．

著者はゼロデイ攻撃の変曲点として，スタックスネットと米国大統領選でのメール漏洩事件を挙げています．スタックスネットとは 2009 年にイランで起きたサイバー攻撃に使われたマルウェアで，核兵器にも転用可能な濃縮ウランを製造する核燃料施設の遠心分離器を破壊しました．それまでのサイバー攻撃は軍事情報等の機密情報を盗むか，システムを停止させる攻撃が大半でしたが，スタックスネットはインフラを不可逆的に破壊する初めての攻撃です．一方，記憶に新しい米国大統領選でのメール漏洩事件においてもゼロデイ脆弱性が使われ，サイバー攻撃が一国の政治体制に影響を与え得ることを証明しました．これらのサイバー攻撃は規模や緻密性に加え，ゼロデイ脆弱性を多数利用した攻撃であることから，莫大な経済力と技術力を備える国家が攻撃に関与していると言われています．

こうなると，もはや一機関，一企業のみで完璧にサイバー攻撃を防ぐことは不可能です．本書の例を見てもエア・ギャップ（インターネットから重要なネットワークを物理的に切り離すこと）を設け，計算機室への入退室を厳しく管理しても完全ではありません．サイバー攻撃は起きるものと考え，攻撃された際の被害を事前に想定しておき，事故や被害（インシデント）の発生時に迅速かつ適切に対応できるよう準備することが重要です．

各国のサイバー攻撃戦略

本書では各国のサイバー攻撃戦略について，以下のように述べられています．

米国は情報量こそが重要との戦略の元，ネットワーク監視等での情報収集のほか，豊富な資金を利用して世界で最もゼロデイ脆弱性を収集していると言われます．元 NSA（米国家安全保障局）局員の Snowden 氏によれば，NSA は 2013 年の 1 年でゼロデイ脆弱性の購入に 2,510 万ドル（約 30 億円）を使ったそうです．一方，中国の人民解放軍の研究所である軍事科学院は著書において，サイバー攻撃や防衛は「国家を挙げて人海戦術により対応」することが重要と述べています．ロシアも自国の軍事インフラが GPS 等，他国のサービスに依存することを恐れ，民間から優秀な人材のリクルートに力を注ぎ，技術開発を行っていると言われています．このように各国は自国の人材，経済力，IT

インフラに与えられる影響力の大きさなどから，自国のサイバー攻撃戦略を決定しています．

イランや北朝鮮の動きも無視できないと言います．インフラの IT 化が進んでいない国では，サイバー攻撃によって他国に与えられる被害と自国のインフラが攻撃された際に被る被害の大きさに「非対称性」が存在します．この非対称性がこれらの国がサイバー攻撃に力を入れる背景になっています．

スタックスネット以降，さらにサイバー攻撃は高度化し，今日までインフラへのサイバー攻撃はとどまることを知りません．冒頭には日本のインフラを狙ったフィクションのサイバー攻撃が登場しますが，似た攻撃は十分起き得ます．また考えたくもありませんが，仮に国家間のサイバー攻撃の応酬が激化した場合には著者の主張の通り世界を破壊する状態になってもおかしくないと感じました．

では我が国は？

インフラのネットワーク接続や IoT 化が急激に進みつつある日本でも，サイバー攻撃対策が重要なことは言うまでもありません．ところが日本が採る対策は米国に頼る部分が多く，中にはメールを米国のサーバにいったん送って検査するものまであり，逆に自ら情報漏洩リスクを高めていることに警鐘を鳴らしています．著者は米国に頼る方針を見直すべきと主張していますが，理由として憲法第 9 条による日本独特の事情も挙げています．たとえば海外からサイバー攻撃を受けた際の犯人を特定するための情報収集において，日本では何がどこまで許されるかがきわめて曖昧であり，インシデントへの対処さえも制約を受ける可能性があると言います．

本書を読み終えて，インシデント発生時に打てる対策が限られる可能性がある日本は他国以上に防衛を固める必要があり，高度なセキュリティ技術が必要であると感じました．外部の技術に無批判に頼るのではなく，現状のリスクを考慮した上で技術開発戦略を決定，実行することが重要です．そのためには政府機関はもちろん，個々の研究者，技術者が果たすべき役割も大きいはずです．

『適切に語らなければ伝わらない』

あとがきで引用されたテレビ番組の Snowden 氏へのインタビューが印象的だったので最後に紹介します．米政府が行っていた諜報活動の深刻さを伝えようと「（米政府は）子供のための基金であるユニセフですら，スパイしているのです」と言った Snowden 氏に対し，インタビュアーは「で？」と興味がなさそうにし，「あなたが実施した行為は適切に語らなければ伝わらない．あなたは以前言っている．NSA では（監視中に入手した）人の裸の写真をみんなで見ている，と．この事実こそが人々を恐怖に陥れる」と返します．

一方，セキュリティ技術者であれば「セキュリティ対策（もしくは技術開発）が必要です」と主張したとき，相手は必要性自体は認めてくれつつも，実際には「コストとの兼ね合いで採用は難しい」と言われた経験をお持ちではないでしょうか．

両者の話の根本は同じで，サイバー攻撃は一般の人にとってまだ遠い世界のことであり，実感がないのかもしれません．しかしインシデントはたまたま今のところ身の回りに起きていないだけで，危険と隣り合わせです．我々研究者，技術者は大きな問題意識から，大上段に構えて対策の必要性や課題を語ってしまいがちです（場合によってはそれも重要ですが）．リスクも効果も目に見えにくいセキュリティは特に「適切に語る」のが難しいとは思いますが，これはどの研究でも多かれ少なかれ存在する課題でしょう．無駄に不安を煽るのもよくありませんが，相手の身近な問題としてリスクや技術の必要性を伝えなければ真剣には考えてもらえません．その伝え方も専門家としての腕の見せどころであると感じました．

本書で語られる内容は，攻撃の規模や技術，影響の大きさもサイバー攻撃の古典的名著『カッコウはコンピュータに卵を産む』（1991 年）の時代とは隔世の感があります．セキュリティ関係者にとっては，セキュリティ対策やインシデントレスポンスの重要性，さらには技術開発の在り方を考えさせられる内容ですし，専門外の方でも専門知識なしで読むことができ，今世界で何が起きているのかが理解できる内容になっています．ぜひとも一度手に取ってみてはいかがでしょうか．

（2017 年 7 月 31 日受付）

金井　遵（正会員）　jun4.kanai@toshiba.co.jp
2008 年日本学術振興会特別研究員（DC2），2009 年東京農工大学工学府電子情報工学専攻博士後期課程修了．同年，（株）東芝 研究開発センター入社．現在，同社 電力・社会システム技術開発センター．セキュリティおよびシステムソフトウェアの研究開発に従事．博士（工学）．