NPO ISEF
Not-for-Profit Organization of Information Security Forum

特定非営利活動法人
NPO情報セキュリティフォーラム

NPO-ISEF 情報セキュリティレポート：2011-No.01

サイバー攻撃の現状と対策

株式会社ラック
取締役 最高技術責任者　西本 逸郎（Nishimoto Itsuro）

【著者経歴】
通信系ソフトウェアやミドルウェアの開発に従事。１９９３年ドイツのシーメンスニックスドルフ社と提携し、オープンPOS（WindowsPOS）を世界に先駆け開発・実践投入。２０００年よりセキュリティ事業に身を転じ、日本最大級のセキュリティセンターＪＳＯＣの構築と立ち上げを行う。さらなるＩＴ利活用を図る上での新たな脅威への研究や対策に邁進中。情報セキュリティ対策をテーマに官庁、大学、その他公益法人、企業、各種ＩＴイベント、セミナーなどでの講演、新聞・雑誌などへの寄稿等多数。一般社団法人 日本スマートフォンセキュリティ協会 理事 事務局長。NPO 日本ネットワークセキュリティ協会 理事。
著書：「国・企業・メディアが決して語らないサイバー戦争の真実」中経出版。

IT 革命で何が起きているのか

P.F.ドラッカーは、産業革命と IT 革命を対比し、2000 年頃までの IT 革命は蒸気機関が発明され大量生産が行われた産業革命前期と同様であると記していた。その後、人を運ぶ鉄道の発明により、私たちの生活様式を変化させたことが産業革命の本質であるとのことであった。それは、ものが移動し人が受動的に受け入れていた時代から、能動的に人が移動し住む場所やものを選択することで、従来の生活様式や社会基盤を根本から覆したのだろう。そういう面では、皮肉にもドラッカーが他界した2005年以降急速に発展した検索エンジンやソーシャルメディアがもたらしつつある情報への能動的な目を持つに至らせる動きは、スマートフォンにより一気に世界中の各層へ急速に広がり新しい社会基盤や秩序を産みだそうとしている。東京電機大学の安田浩 未来科学学部長は、この状況を生物の全てが目を持ち現在の形へと一気に進化した「生命ビッグバン」が発生した 500 万年に及ぶカンブリア紀に例え、1980年頃から2030年頃までの50年がすべての人類が情報への目を持つという「情報ビッグバン」であり私たちにとってのカンブリア紀であると説いている。恐らくは、この数年で単なる合理化の道具だった IT は、能動的に情報を発信し活用する社会基盤へと変化したのだろう。

第五の戦場誕生

こういう状況の中で、昨年米国がサイバー空間を「第五の戦場」として定義したことは衝撃的であった。極めて当たり前のことではあるが、ここに到るには伏線もあった。まず米国は、サイバー空間を「国家の重要な資産」であるとの意思決定をし、2009 年５月にはサイバー空間におけるセキュリティは「経済繁栄と安全保障の基盤」であるとの認識を示したのだ。故に、実社会と同様にサイバー空間においても米国は同盟国と協調し主導権を握り、重要資産であるサイバー空間への攻撃は米国へ

の攻撃ともみなし報復をも辞さない。つまりは、戦場でもあるとの定義に到ったのであろう。

※　市川類@JETRO「米国連邦政府のサイバーセキュリティ政策を巡る動向」が参考となる。
http://www.ipa.go.jp/about/NYreport/201003.pdf

わが国においては、IT を重要な成長分野と定義はしているものの、重要な国家資産であるというほどの意思表示はない。これも、私たちが現状を理解することに楽観的である原因かもしれない。

サイバー攻撃の現状

サイバー空間で経済などあらゆる活動が行われ、その活動や成果が記録され蓄積されている。こういう中、サイバー攻撃が激化していることは誰も否定できないだろう。まずは、誰がどんな目的で行っているかを考えることは重要なことである。一般的に言われているが、それは愉快犯から金銭目的やストーカ的な犯行へと拡大。自分たちの主義主張のための侵入や情報窃取と暴露、さらに国家関係機関からの諜報活動や破壊活動と際限がない。

そういったことから、私たちは何をどうすればよいのかも分からなくなってきている。そもそも、悪いのは犯罪者であり、私たちが気にすべきことではないのではないかとも考える。実際に、平成 23 年 11 月 1 日の参議院本会議における答弁で野田総理大臣は「また、これらのサイバー攻撃事案については、警察においても鋭意捜査や情報収集等を行っており、違法行為があれば厳正に対処していくものと承知をしております。さらに、サイバー攻撃の発信元が海外であると判明した場合には、海外の捜査機関等に対し捜査協力要請を実施するなど、国際的な連携を推進しているものと承知をしています。」と答弁している。
※ http://kokkai.ndl.go.jp/SENTAKU/sangiin/179/0001/17911010001004a.html

私たちが合理的に対応を行うためには前述の「誰がどんな目的で」が重要であり、その相手によって対抗できることが変わってくる。例えば、相手が愉快犯やこそ泥ならば、犯罪捜査の観点が重要である。ビシッとやって頂きたい。相手が国家機関などの場合は犯罪捜査の観点だけでは十分ではない。しかし、万一被害が出た場合は、自分たちが守るべき顧客の保護や社会的使命を全うしつつ、相手の狙いを阻止して行かなければならない。ここが重要な点である。相手が誰であれ、私たちは私たちの顧客と事業などを守るという使命を全うしていかなければならない。それに対して、相手が国家機関レベルであっても、個々の組織が個々の責任でのみ対応していかなければならないという現実もここにはある。

現状のセキュリティ対策の落とし穴

一方、私たちが取り組んでいるセキュリティ対策にも落とし穴が潜んでいる。

現状のセキュリティ対策の根幹は予防・防御策である。つまりは、被害にあわないことが目的となっている。私たちのセキュリティ対策三カ条は「OS などを最新にしておく」「ウイルス対策ソフトを

入れよ」「不審なメールやホームページは開くな」などというものである。その結果、被害が発生した場合、悪いのは「OS を最新にしていないこと」、「ウイルス対策ソフトが古い」、「不審なメールに騙された」こととなる。よって、再発防止策は、その線の深堀となり、いたちごっこに陥る羽目となる。

例えば、ウイルスに感染した時は「ネットワークから切り離し、ウイルス対策ソフトを最新にして駆除を行う。」となっているだろう。これは正しいことだろうか。ウイルスに感染する前や感染直後であれば「駆除」で大丈夫である。しかし、活動中を発見した場合「駆除」で対策完了とはならない。どこから侵入したのか、仲間はいないのか、そもそも守るべき情報や機能は大丈夫なのかなどを調べるのは当たり前のことである。

また、制御系システムや高セキュリティが要求される組織やシステムでは「他のネットワークから隔離する」が根幹となっていることも多い。しかも「OS を最新にしてウイルス対策を行う」ところも多いときく。この「隔離セキュリティ」の場合、「隔離」することが極めて重要な要件であることを理解しなければならない。つまり、徹底的に隔離しなければならないのだ。しかし外界との接点はプログラムや機器の保守で否応無しに持つ必要もある。以前は保守会社側も隔離されていたが現在ではあらゆるものがつながっていることが前提で調査や開発や保守が行われている。非常に辛い時代になっていることを改めて見直さなければならない。つまりは、市販の製品や開発環境を使用しているならば「隔離」するより、上手くつなげて管理し安全に制御できるように考える時代であろう。

こういったことは小学生でも分かることだと思うが、そうなってしまうには何か原因があるに違いない。

一つとしては「管理責任」の要求があると推測される。個人情報保護法の運用ガイドラインに代表する管理責任の要求は、多くの組織にとって「アリバイ作り」的な対策に終始させてしまい、本来の対策への思考能力を低下させてしまっているのかもしれない。そんなこと言っても現実に被害が発生しているのである。私たちは、忘れることもあれば騙されることもある。それでも、被害は防いでいかなければならない。

二つ目は、前提条件＝「現在は、被害にあっていない」というのが既に間違っているのではないか。そう言えば、文章でも、間違いはないと思ってチェックをすると間違いには気が付かないものだ。必ずあると思ってチェックすると不思議と見つかるものだ。組織内の異変も同様である。既に何か起きていることを前提に、対策を講じることが重要である。

三つ目は、「IT システムやセキュリティはシステム部」以上のように、IT システムが経営責任になっていないことである。売上やコストなどと同じように、管理や制御が出来ることとそうでないこと（リスク）を十分にかつ明確に経営に伝えておくことがまずは第一歩なのだろう。

どうすべきなのか？

多くの方々がセキュリティ対策だと思っている予防策は、積み上げればあげるほど費用対効果が悪くなるだけではなく、事件は起きないという慢心や、大半の脅威から守られているため警戒心も薄れ、結果的に組織力、社員力までもが低下してしまうという危険性もある。わざわざお金や時間をかけて対策をしているのに、そんなことになってしまうのは何故だろうか。逆説的だが「アリバイ対策」を一所懸命行ってしまうからだではないか。「アリバイ対策」は、そこそこで良いのだ。法律などで要求されている管理責任は果たさなければならないが、命までかけてまで果たすことはない。

一方、IT は子会社や業者に委託しているので、セキュリティも業者の責任だと考えるかもしれない。その場合、自分の軸足を預けていることを忘れてはならない。単なる合理化で IT を使用していても、合理化である以上単一障害点になっている可能性は極めて高い。日々変わる環境変化を適切に捉え、万一のビジネスインパクトの把握は怠れない。

サイバー戦争時代。一般企業でさえ、国家関係機関からの脅威を考慮しなければならなくなった時代であるが、「戦争」とは物騒な言葉でもあり誤解の懸念もある。私たちの理解から言えば、相手を制御できないならば「災害」と理解した方が早いのかもしれない。私たちは、現状の脅威をサイバー上の「災害」として認識し対策を講じた方が現実的なのだろう。

一方、「広域災害」のような「有事」をどのように認定し、誰にどのような「救助活動」が必要なのかを取り決めていくことも国のサービスとして必要なことであろう。多くの人々の生活や経済活動に差しさわりが出る、資産や財産が失われる事態などである。重要インフラの保護や捜査力の向上は当然のことであるが、万一の時には復旧措置をどうするか、そろそろ考えておいて良いと思う。

2012 年3月２８日発行

特定非営利活動法人　NPO 情報セキュリティフォーラム
〒221-0835
神奈川県横浜市神奈川区鶴屋町 2-17　相鉄岩崎学園ビル
TEL(045)311-8777　　FAX(045)311-8747
E-Mail: isef@isef.or.jp　　URL: http://www.isef.or.jp