特別インタビュー 1
special interview

株式会社サイバーディフェンス研究所
専務理事
上級分析官
名和 利男 氏

企業が直面するサイバー攻撃の脅威 真の防御は「危うい現実」の直視から

セキュリティー対策を講じていても、サイバー攻撃によって防御網を突破され、個人情報・機密情報を窃取される――ここ数年、そんな事件・事故が後を絶ちません。なぜサイバー攻撃を防ぐことができないのでしょうか。また、今サイバー空間では何が起きているのでしょうか。

日本におけるサイバー・ディフェンス演習の第一人者で、サイバー防衛の「トップガン」と称される名和利男氏に、企業が直面するサイバー攻撃の脅威について話を伺いました。

境界防衛だけで情報資産を守り抜くことは不可能

―― ここ数年来、日本の企業や組織がサイバー攻撃によって情報漏洩などの実害を被るケースが増えています。セキュリティー対策を講じているにもかかわらず、情報を守れないのはなぜなのでしょうか。

名和氏（以下、敬称略） 大きな要因の一つは、企業のサイバー・セキュリティーの考え方が、一世代前の発想のままだからです。これまで企業は、「社内の情報資産を守る」という観点からセキュリティー対策を行ってきました。「社内の情報資産を守る」というのは、特定の物理的な設備・施設を保護するという考え方の延長線上にあるもので、例

えば、情報の機微性や重要性を格付けし、それに応じて「特定の場所にある特定の情報に対して、何かしらの保護策を講じる」といった発想が根幹にあります。また、その発想が、社内ネットワークと外部ネットワークの境界を守るという「境界防衛」の考え方につながり、大多数の企業がそのための施策に力を注いできたのです。しかし、「社内の情報資産を守る」という発想は、重要データが組織の中に閉じた基幹システムにしか存在しなかった時代の考え方で、今日では通用しなくなっています。

―― 通用しなくなった理由はどこにあるのでしょうか。

名和　理由はシンプルで、企業システムに、あらゆるモノ・人がつながり始めているからです。その背景には、モバイルやクラウド・コンピューティング、IoT（Internet of Things：モノのインターネット）などの潮流があります。このような「すべてがネットワークにつながる社会」では、守るべき情報が常に特定の場所にあるとは限らず、組織内外のネットワーク上を縦横に動き回ります。前述した境界防衛だけで情報資産を守り抜くことはもはや不可能なのです。

「内閣官房情報セキュリティセンター（現：内閣サイバーセキュリティセンター）」でも、2005年ごろから、「境界防衛だけではサイバー攻撃に対処できない」との注意喚起を行っています。しかし、企業の多くがいまだに境界防衛に力を注いでいるというのが現状です。

―― 今日のサイバー・ディフェンスを考える上で、必要とされる視点はどんなことだとお考えですか。

名和　一つは、守るべき情報がどう扱われるのかという「プロセス」を考慮することです。前述したように、今日のネットワーク社会では、企業が保護すべき情報が組織内外のネットワークをさまざまに動き回ります。他組織との協業の中で、自社の重要情報を社外とやり取りするケースも頻繁にあります。

情報の価値は、その情報を扱う企業・組織によって異なり、A社にとって極めて重要なデータであっても、B社にとってはそれほど重要ではないというケースもあります。そのような場合、A社とB社とではデータを扱うルールや規則が大きく異なってきます。そのため、企業は保護すべきデータについて、「誰（アクター）が、どう扱うのか（アクティビティー）」を常に念頭に置いておく必要があります。つまり、「自社のデータを受け取った相手（アクター）が、そのデータをどのように扱うか（アクティビティー）」というユースケースを考慮した上で、プロセスのリスク・アセスメントを行い、必要な対策を講じておくことが不可欠なのです。セキュリティー対策にプロセスを加味することの必要性は、世界中のセキュリティー専門家が以前から指摘しているポイントです。

―― 自社の重要情報に対して、「誰に、どのように扱わせるか」という規則やルールが徹底されていないということですね。

名和　そうですね。情報管理責任の所在が曖昧なまま、社外の人に重要な情報を扱わせてしまえば、そこをサイバー犯罪者に突かれることにつながります。言い換えれば、企業の「セキュリティー対策が甘い」のではなく、「情報を取り扱う前提条件である規則が、現状に即していない」ということなのです。

サイバー・セキュリティーを取り巻く世界の情勢やIT環境は劇的に変化しています。にもかかわらず、情報を扱う側が一世代前の考え方から変わっ

PROFILE

名和 利男 ［なわ としお］

株式会社サイバーディフェンス研究所 専務理事 上級分析官。航空自衛隊において、信務暗号・通信業務／在日米空軍との連絡調整業務／防空指揮システムなどのセキュリティー担当（プログラム幹部）業務に従事。2003年に退官した後は、国内ベンチャー企業のセキュリティー担当兼教育本部マネージャ、JPCERT/CC早期警戒グループのリーダーなどを経て現職に就く。2006年からサイバー・ディフェンス演習を展開し、日本のサイバー・セキュリティーを担う人材の発掘にも力を注ぐ。

ていないことが、今日の企業におけるセキュリティー対策の大きな問題と言えるのです。

―― サイバー・セキュリティーを確保する上で、ほかに留意すべきポイントがあれば教えてください。

名和　それは、ITシステムに対するセキュリティー・コントロールが難しくなっている点です。1990年代まで、日本企業の基幹システムの多くは、独自性の高いハードウェアと自作のソフトウェアで構成されており、セキュリティー・コントロールを徹底させることが可能でした。しかし2000年以降、軍事システムにおける「COTS（Commercial off the shelf：民生品利用）」が進んだのと同様に、民間企業の間でもソフトウェアの生産性向上やコスト削減を目的として標準コンポーネントを用いることが主流となり、開発・保守・運用も外部にアウトソースするのが一般化しました。これは、自社のITシステムのセキュリティーを完全なかたちで自らコントロールできなくなったことを意味します。標準コンポーネントは、セキュリティーをコントロールすることが難しく、脆弱性を突かれやすいというネックもあります。また、アウトソース先の企業に対して社内と同レベルの統制をかけることは、たとえ契約条項があったとしても不可能に近いからです。

攻撃者は組織やシステムの脆弱な部分を最初に攻撃するため、外部に委託した領域や標準コンポーネントが真っ先に狙われてしまいます。実際、セキュリティー・コントロールの効いた「企業システムの本丸」から情報がサイバー攻撃によって盗まれるケースは少ないのです。

拡大する攻撃者の裾野

―― 日本でサイバー攻撃の脅威が広く認識されるようになったのは、ここ数年の話のように感じます。その背景要因として、サイバー攻撃による被害の拡大がありますが、サイバー攻撃自体は変化しているのでしょうか。

名和　まず、「サイバー攻撃が高度化しているから、被害が広がり、サイバー・リスクが取り沙汰されるようなった」と見るのは正確ではありません。むしろ、日本の企業・組織を狙ったサイバー攻撃には一部で質の低下が見られ、それによってサイバー攻撃の存在が広く認識され始めたとも言えるのです。

少し前までのサイバー攻撃は、専門知識を持ったプロの犯行が目立っていました。ところが、日本の企業や組織に対する「攻撃の成功率の高さ」に味をしめたプロたちが、事業を拡大したり、スピンオフをしたりして攻撃者の裾野を押し広げた結果、攻撃が模倣されたり横展開され始めたのです。今日のサイバー犯罪の末端にいるのはプロではなく、ほとんどが素人で、10代の少年達も多く含まれています。実際、私は「6歳児のクラッカー」と対峙したことがあります。最近の攻撃者コミュニティーでは、攻撃マニュアルだけでなくハウツー動画が紹介されているため、専門知識がなく攻撃マニュアルが読めなくても、その動画と同じように操作をすれば、6歳児でも攻撃ができてしまいます。

とはいえ、専門知識もなくマニュアルも読めない素人たちは、しばしば攻撃に失敗します。その失敗によって攻撃の存在が気付かれ、騒ぎになっているというのが今の状況です。

日本企業の中にも、他の先進国の企業と同等、もしくはそれ以上の対策を講じているところもあります。ところが、自分たちが今どのようなサイバー・リスクにさらされているのか、自社が守るべき情報が、誰に、どのように扱われているかを適切に把握できておらず、サイバー・セキュリティー対策がなおざりになっている企業も少なくありません。

日本には約385万社の企業があり、うち99.7%が中小企業・小規模事業者[※1]ですが、それらの多くが、ITに投資する財務的なゆとりがなく、専任のIT担当者やセキュリティー担当者を配置できないのが現状でしょう。これでは、今日のサイバー攻撃に太刀打ちできません。とはいえ、企業規模が小さいからといって機密情報を扱っていないわけではなく、取引先や顧客の重要データを数多く扱っている場合も少なからずあります。そうした組織がサイバー攻撃に対して無防備であることは、日本の産業全体にとって憂慮すべきことだと思うのです。

サイバー攻撃はさらに拡散する

―― サイバー攻撃は、今後どうなっていくのでしょうか。

名和　サイバー攻撃は、「手段」であって「目的」ではありません。攻撃を仕掛ける側には、経済・軍事・科学技術における競争に勝ち、経済的な利益や紛争での優位を確保するという大目的があります。そうした視点で世界情勢を観察すれば、日本を取り巻くサイバー・リスクが今後さらに深刻さを増すことは容易に想像できるはずです。

例えば、サイバー犯罪のブラックマーケットは年々巨大化していますが、背後には、富を得るためには手段を選ばない一部の悪辣な裕福層と、そうした人間の元で働く「下請け」のサイバー犯罪者の一群がいます。その下請けのサイバー犯罪者らの多くが、生活の糧を得るために犯罪に加担しています。言い換えれば、経済的な弱者が増えれば増えるほど、下請けのサイバー犯罪者の“供給”は潤沢となり、攻撃側の戦力が強化されるということです。

そして現在、世界の多くの地域で経済危機が発生し、格差が広がり、テロリズムとの紛争も絶えず、経済的に極限状態に追い込まれる人が増えています。そう考えると、サイバー犯罪者の裾野がこれからも拡大し続けるのは確実で、攻撃はさらに激しさを増すことになるでしょう。にもかかわらず、企業がサイバー・ディフェンスの能力を高めようとしないなら、その存続に関わるような痛手を被る恐れが高いと言えるのです。

さらにもう一つ、日本の場合、サイバー攻撃から身を守るための科学技術面の対策が進んでいないのも問題です。

―― それは具体的に、どのような問題なのですか。

名和　例えば、中国政府は2015年に、同国の衛星測位システム「北斗衛星導航系統」に搭載するチップセットを独自開発すると宣言しました。目的は、「ロジックボム」[※2]と呼ばれるハードウェアに仕掛けられるサイバー攻撃への備えです。ハードウェア・レベルで仕掛けられる攻撃に対しては、中国だけでなく米国も危機感を持って対応しており、何百億円もの巨費を投じてハードウェアに組み込まれたトロイの木馬型ウイルスを検出する技術「Hardware Trojan Detection Technology」を開発しました。

ところが日本の政府も民間も、そうしたディフェンス技術の自国開発の必要性を適切に認識していません。今日、日本の製造企業は、海外ベンダーからチップセットを調達しなければならない状況にありますが、そのチップセットにトロイの木馬型ウイルスが仕込まれていても、それを検出する技術が日本にはないのです。ゆえに、日本は、「ロジックボムが仕掛けやすい国」の筆頭に挙げられています。私は2006年から、そのリスクの深刻さを訴えてきましたが、日本の企業・組織の危機感にさしたる大きな変化は見られていないようです。

「すべてがネットワークにつながる社会では、守るべき情報が常に特定の場所にあるとは限らず、組織内外のネットワーク上を縦横に動き回ります。一世代前の対策では情報資産を守り抜くことはもはや不可能です」と、名和氏は警鐘をならす。

現実を知ることが、現状打開の第一歩

―― こうした現状を打開する上での課題とは何なのでしょうか。

名和　まず言えることは、IT部門の力だけでは現状を打開することはできないということです。IT部門の限られた予算の中で、鳥瞰的なセキュリ

2006年からサイバー・ディフェンス演習に取り組み、日本のサイバー・セキュリティー対策を担う人材の育成（抽出）に力を注ぐ名和氏。「私が発掘したいのは、自らサイバー演習を立案し、行動できる人材です。こうした人材が増えれば、危機管理の訓練に参加する人も増え、日本のサイバー・ディフェンス力も強化されます。発掘・育成には、5〜10年の歳月が必要かもしれませんが、やるしかありません」と話す。

ティー対策を遂行するのはほぼ不可能でしょう。

また、実際にサイバー攻撃を受けているのは、情報資産や営業情報を扱っているビジネス部門ですが、そこにITやセキュリティーに精通した人材がいることは稀で、ほとんどを外部の委託者に委ねています。さらに、会社によってはIT部門を別会社にしており、この場合も重要情報を社外の人に管理させていることになります。このような中で、サイバー・セキュリティーを強化するのは困難と言わざるを得ません。

―― では、何から着手すべきなのですか。

名和　何よりも重要なのは、経営陣を含めた会社全体が「現実を知る」ことです。情報を自ら集め、「世界で何が起きているのか」「自分たちがどのような状況に置かれているか」を肌身で理解することが、現状打開の第一歩です。

いったん現実を「認知」すれば、現場で働く人たちは優秀ですから、一挙に事が前進するはずです。つまり、管理職者が具体的な方法論や作業手順を示さなくても、現場が自ら学習し、ボトムアップのかたちでさまざまな改善策が出てくるでしょう。また、現実を認知したのちには、演習を通じてリスクに備えるといった「行動」を取ることが肝心です。危険回避のプロセスは、「認知」、「判断」、「行動」の3要素から成りますが、訓練などの行動を重ねることで人の認知力・判断力は格段に向上し、何かが起きたときに自然に身体が動き、適切な対応が取れるようになります。ですから、多くの情報から現状を正しく認知し、それに即した行動を取るようにすれば、サイバー・ディフェンスの能力を高めていくことができるのです。

実際、米国では、FEMA（Federal Emergency Management Agency：連邦緊急事態管理庁）の「HSEEP（Homeland Security Exercise and Evaluation Program：国土安全演習・評価プログラム）」のマニュアルを用いながら、州政府が、大企業経営層を対象にしたサイバー演習を四半期に1回の頻度で行っています。この取り組みは、セキュリティー・インシデントに対する経営層の対応力を高めるのと同時に、サイバー・リスクに対する彼らの意識向上にもつながっています。危機感を持っている国は、このような行動をすでに起こしているのです。

産業全体のサイバー・セキュリティー・レベルを上げるには

―― とはいえ、企業の中にはサイバー・リスクの現状を正しく捉えること自体、難しいところもあるのではないでしょうか。とりわけ、IT専任の担当者が少ない、あるいは専任者がいないような中小の企業の場合、サイバー・リスクの現状を正確につかみ実際の行動に移すのは、かなり困難なように感じます。

名和　確かに、中小の企業のサイバー・セキュリティー・レベルをどう底上げするかは、難しい問題です。日本政府は、「日本再興戦略 改訂2015」[※3]の中で、2015年度中にサイバー・セキュリティー対策

の経営ガイドラインを策定すると明記していますが、ガイドラインのベースとなっているのは、国際標準の「情報セキュリティマネジメントシステム認証制度（ISMS認証）」です。現在、経済産業省が同ガイドラインを策定していて、2016年度よりISMS認証の審査に同ガイドラインに沿った審査項目が追加されます。ただし、このガイドラインは基本的にセキュリティー対策に一定のリソースが割ける大手企業を対象にしたもので、中堅・中小企業向けには、評価項目を減らした簡易な認証制度の新設が検討されているようですが、網羅性や完全性が欠けることになります。

そのため、それを補完する手段を講じなければなりません。その際の参考例として挙げられるのは、韓国の「DDoS避難所」です。これは、政府がDDoS攻撃に耐えられる堅牢なネットワーク環境を用意し、DDoS攻撃を受けているサイトを同ネットワーク下に避難させて運用の継続を支援するというものです。日本では、大手のISP／データセンター事業者が同様のサービスを提供しようとしていますが、私はこうした対策は国が取り組むべきことではないかと感じています。

―― 日本の行政は、韓国の「DDoS避難所」のような取り組みを推進していないのですか。

名和　総務省自治行政局の配下で進められている「総合行政ネットワーク（LGWAN）」※4の取り組みが、それに相当すると思います。LGWANという閉域ネットワーク上で提供される共有アプリケーション・サービス（LGWAN-ASP）を使えば、中小の企業も一定のセキュリティーが担保できるはずです。

とはいえ、LGWANのような共用インフラ自体のセキュリティーを確保するには、当然、技術者が必要とされ、適正人数の技術者で、日本全国・各地域の企業・組織のサイバー・セキュリティー・レベルを底上げしようとするならば、技術者の担当エリアを少し広く取る必要があります。このような運用管理の体制・仕組みを機能させるには、一部で議論されている「道州制」を利用することが考えられます。

ここで言う「道州制」とは、現在の都道府県を9から13程度の州に分割して「ローカル・ガバメント」を作り、地方自治の役割や経済規模を欧州の小国程度にして行政の効率化を目指す枠組みです。この枠組みを導入すれば、共用ネットワークのセキュリティー対策をローカル・ガバメント単位の大きな予算で遂行できるようになります。また、各地域の課題に包括的に対応できるようにもなるはずです。ところが、今日のように、行政区域が47に分かれている状態では、共用ネットワークを効率的に運用し、強化していくことは難しく、結果として、各地域の企業・組織のセキュリティー・レベルを全体的に底上げすることも困難と言えるのです。縦割り行政の中で道州制を実現するのは至難かもしれませんが、私は、日本の産業を支える数百万の中小の企業をサイバー攻撃から守るためには、このような大胆な施策を利用するしか方法はないと考えています。

もう一つ、サイバー・セキュリティーの啓発活動も大切です。私はかねてから、メディアでの発言や講演、さらに人材育成などを通じてサイバー・リスクの現状を伝えてきましたが、ここにきて、官民学連携による地方での啓発活動も活発化しつつあります。これは地道な活動ですが、こうしたアクションを通じて理解を深めてもらうことが、日本企業全体のサイバー・セキュリティー・レベルを高める現実解ではないでしょうか。

※1 経済産業省「中小企業・小規模事業者の数（2012年2月時点）の集計結果を公表します」
http://www.meti.go.jp/press/2013/12/20131226006/20131226006.html

※2 ロジックボム：サイバー攻撃用のマルウェアの一種。攻撃対象のコンピューターの内部に潜伏し、あらかじめ設定された条件が満たされる（指定の日時になるなど）と起動し、破壊活動などを行う。
http://e-words.jp/w/%E8%AB%96%E7%90%86%E7%88%86%E5%BC%BE.html

※3 日本再興戦略 改訂2015
「第二 3つのアクションプラン　一. 日本産業再興プラン」より
http://www.kantei.go.jp/jp/tyoukanpress/201506/30_p.html
http://www.soumu.go.jp/main_content/000375794.pdf

※4 総合行政ネットワーク（LGWAN）
地方公共団体の組織内ネットワーク（庁内LAN）を相互に接続する行政ネットワーク。安全確実な電子文書交換、電子メール、情報共有および多様な業務支援システムの共同利用を可能とする
http://www.soumu.go.jp/denshijiti/pdf/061212_02.pdf