CYBER GRID JOURNAL

特集
経営課題としてのサイバーセキュリティ

LAC

Vol.2 | 2016 WINTER

巻頭言

事業継続に活かせるセキュリティ情報を届けたい

川口 洋

サイバー・グリッド研究所 所長　チーフエバンジェリスト

サイバー・グリッド研究所ではサイバー空間におけるセキュリティ事件や脆弱性情報の収集、注意喚起を促す情報の発信をはじめとして、さまざまなセキュリティ対策技術の研究に取り組んでいます。

これらの活動の一環として、私は全国各地を飛び回り、企業や官公庁の方々に向けた講演や、組織でセキュリティ対策に携わる方々との意見交換を実施していますが、この時、質問を受けることも多々あります。その内容は組織の業態や担当者の地位・立場などによって異なりますが、多くの方が共通して口にされるのは次のような質問です。

「セキュリティを 100% にすることは難しいですよね」

背景にはどこまで対策をすればいいかわからないという気持ちや、普段の取り組みに自信が持てないということがあるようです。この手の質問をされるのは往々にして真面目なシステム部門担当の方が多いように感じています。日常のシステム運用の中で「動いていて当たり前」と100% の稼働率を維持しようと奮闘されている方だからこそ、セキュリティ対策に取り組んで 100% という評価が得られないことがもどかしいのかもしれません。この質問に対する私の回答はこうです。

「セキュリティ対策を減点方式で考えるのではなく、事業発展や事業継続のためにどのような対策をとればいいのかを考えてください。野球やサッカーで例えるならば完封勝利だけを目指して挑むのではなく、1 点取られても 2 点取って勝つ、このリーグ戦を突破するためには 3 点差で勝たなければならない、という発想がセキュリティ対策にも求められます。試合の中において限られたリソースを配分し、ある局面は守りに徹し、ある局面は捨てるという決断が求められます」

このようにサイバーセキュリティを考えるうえで大切なことは完全なセキュリティ対策を目指すことではなく、事業を発展・継続させるために何をすればよいのかという視点に立つことです。そのためには以下の事柄を明確にしておく必要があります。

・何を守りたいのか？
・どの組織と事業が重要なのか？
・事故が発生した場合、関係者への影響を最小限にするためには何が必要か？

どの組織もリソースは常に不足しています。限られた予算や人材でどこを守り、最悪の場合どこを切り捨てなければならないかを決めておかなくてはなりません。また、この決定はシステムやサービスなどの担当者ではなく、全体を俯瞰してリソースの配分を指示できる経営者が行うことが求められています。

経済産業省が策定した「サイバーセキュリティ経営ガイドライン」においても、「経営者のリーダーシップの下でサイバーセキュリティ対策が推進されることを期待する」と明記されています。

このような社会的要請も踏まえ、サイバー・グリッド・ジャパンおよびサイバー・グリッド研究所では今後も、CYBER GRID JOURNAL を通じて以下のような経営判断に資する情報を発信していきたいと考えています。

・経営や事業にダメージを与えた事件の解説
・ダメージを軽減するために効果的な方法
・ダメージが想定される脅威に関する情報

また、テクニカルな情報については、CYBER GRID VIEW をタイムリーに発行することで、サイバーセキュリティ対策を推進する技術者の方のお役に立ちたいと考えています。今後の両誌にご期待ください。

CYBER GRID JOURNAL Vol.2 WINTER

TABLE OF CONTENTS

特集
経営課題としてのサイバーセキュリティ

英 秀明
取締役 常務執行役員
IT プロフェッショナル統括本部長

西本 逸郎
取締役 専務執行役員 CTO 兼 CISO

三木 俊明
取締役 常務執行役員
サイバー・グリッド・ジャパン GM 兼
ナショナルセキュリティ研究所所長

標的型攻撃による大規模な個人情報漏えい事件やデータを「人質」に身代金を要求するランサムウェアの流行など、サイバー空間における脅威は深刻化の一途をたどっている。企業や組織にとってサイバーセキュリティのマネジメントは重要な経営課題の 1 つだと考えるべき時代となっている。そこで、今回の特集では「経営課題としてのサイバーセキュリティ」をテーマに、ラック自身のセキュリティを統括する担当役員（CISO）であり最高技術責任者（CTO）である西本逸郎と、セキュリティ・SI 両事業のサービス部門責任者である英秀明、研究開発部門の長である三木俊明が、それぞれの観点から幅広く意見を交わした。

司会＋記事構成：斉藤 健一（株式会社 HTP）
撮影：古瀬 友博

セキュリティは「投資」なのか「経費」なのか!?

司会：本日は「経営課題としてのサイバーセキュリティ」というタイトルで経営層に向けたお話を伺いたいと思います。ラックの経営陣である皆さんは、普段から他企業の経営層の方々と意見交換される機会も多いと思います。ラックがセキュリティ企業ということもあり、IT 関連でさまざまな相談を受けることもあると思うのですが、興味深いものがあれば教えていただけますか。

西本：最近では CSIRT（シーサート）[1] と PSOC（ピーソック）[2] の構築に取り組みたいという相談が増えました。われわれは 10 年ほど前から PSOC の意義についてお話ししてきましたし、CSIRT や PSOC のセキュリティを支援するサービスも提供しています。これまでは空振りすることも多かったのですが、ここに来て注目され、ようやく動き出してきたという印象を持っています。セキュリティ対策に関して政府がこれまで指導してきたのは、基本的に「ウイルス対策ソフトの導入」、「セキュリティパッチの適用」、「不審なメールは開かない・不審なサイトやアプリには近づかない」の 3 項目です。われわれは以前からこの 3 項目では防ぎきれない、逆に安心してしまい危なくなると主張してきましたが、このことがようやく一般にも知れ渡るようになってきた結果だと考えています。具体的にどのような対策を講じればよいかと、まじめに質問される経営者の方も増えています。これは大きな進歩だと思っています。

司会：昨年（2015 年）12 月、経済産業省などが「サイバーセキュリティ経営ガイドライン」[i] を発表しました。このガイドラインに関して経営層の方々から何か意見や質問などはありましたか。

西本：このガイドラインが発表された当初、経営層には読まれないのではないかという心配がありました。というのも、経営層向けに書かれているのは冒頭部分のみで、大半は主として実際にセキュリティを担当する方向けに具体的に記述したものだったからです。さらに、経営層の方々には IT のことは知らないし興味もないという人も多くいらっしゃいます。それが、経済産業省が発表したという「重み」のせいか、皆さん読まざるを得ないようでした（笑）。

司会：ガイドラインの中には「セキュリティを投資として考える」という内容が含まれています。「投資」というと、例えば設備投資のように、事業の生産性を高めるために工場に新たな機械を導入するといったものをイメージします。つまり、資産を投下したことによるリターンを期待するものという認識です。しかし、セキュリティではリターンは望めません。果たしてセキュリティは「投資」なのか「経費」なのか、この点についてどのようにお考えになりますか。

西本：投資と経費の違いは何かというと、「経費」は何かをやろうとすると必ず付いてくるもので、黙っていても発生してしまうものだと考えています。ですから、経費は抑制しなくてはなりませんし、放っておくと現場は際限なく使ってしまうものだと思います。一方、投資はしなくてもよいものです。ですので、放っておいてもよいものです。先の設備投資の例に当てはめるなら、設備投資を放っておくと自社の競争力が落ちてしまうから投資を行うのです。セキュリティの場合、放っておくとインシデントが発生し、事業継続ができなくなる恐れすらあります。このように本来やらなくてもよいものと考えると、経営者自身が「やる」と判断しない限り誰もやらないわけです。ですから、投資として考えるという内容になっているのだと思います。ただし、投資すると判断して動き出せば、今度は経費となるわけです。ですから、すでにセキュリティ対策を行っている企業では経費であり、対策を行っていない企業では投資ということになると思います。

英：企業の要職にある方々とお話しする機会がありますが、多くの方が IoT（Internet of

1 CSIRT（Computer Security Incident Response Team）
コンピューターやネットワークに関連するセキュリティ上の問題（インシデント）に対処するためのチーム。サイバー攻撃による被害の増加などに伴い、企業や組織内に設置するケースが増えている。

2 PSOC（Private Security Operation Center）
自組織内に設置した SOC（セキュリティオペレーションセンター）。SOC ではネットワーク機器・サーバー・セキュリティ機器などのログ（通信履歴）を監視・分析し、サイバー攻撃の検出・通知などを行う。

3 SoR（System of Record）
直訳すれば「記録のためのシステム」。後述する SoE と対の用語で、ビジネスで起こる事象を蓄積する従来の基幹業務システム全般を指すことが多い。

西本 逸郎 にしもと いつろう

株式会社ラック 取締役専務執行役員 CTO 兼 CISO。1958 年生まれ。1986 年、ラック入社。不正アクセス対策事業本部長、セキュアネットサービス事業本部長、サイバーリスク総合研究所所長などを歴任。2016 年 4 月より現職。

Things）など先端技術の利活用に興味をお持ちです。ビジネスに関わるあらゆる事実をデータとして記録することを主目的とする従前のSoR（System of Record）[3] に加え、SoE（System of Engagement）[4] に注目しています。膨大な情報をもとに新たなニーズを捉え、いち早くビジネスを展開し進化していくことを目指していらっしゃるようです。イノベーションに新たな脅威は付き物で、セキュリティへの取り組みは重要かつ必然の要素とも捉えていらっしゃいます。

司会：よくわかります。企業が成長を続けるためにはイノベーションなどを通じて変化していく必要がありますからね。

英：そうですね。インターネットという概念やそれを支える技術がなければ、現在当たり前となっている利便性を得ることはできません。一方で、情報漏えいの被害はここまで甚大にはならなかったでしょうし、サイバー攻撃がテロリズムの手法として懸念されるようなこともなかったでしょう。このような「イノベーションから派生するリスク」が起こり得ることも視野に入れておくことが肝要です。

三木：企業に対するサイバー攻撃が激化・高度化している側面についても考える必要があると思います。インターネットそのものはご存じのとおり性善説に基づき発展しました。その中でビジネスをしようとすれば当然悪人も入ってきます。1990年代であれば、セキュリティ上の脅威も限られたものだったと思いますが、現在では一民間企業の担当者だけですべての脅威をキャッチアップすることは難しく、われわれのようなセキュリティ企業の手助けが必要になってきます。もちろんセキュリティ対策にかかる費用も単なる必要経費から、予算化しなければならない金額の費用へと変化しています。ただ、近年起こっている情報流出事件などを見ると、経営者の責任が追及されることも多いのが現状です。セキュリティは投資か経費かといわれれば、決断は投資ですし、継続は経費ということになると思います。

三木 俊明 みき としあき

株式会社ラック 取締役 常務執行役員 サイバー・グリッド・ジャパン GM 兼 ナショナルセキュリティ研究所所長。1958年生まれ。1983年、国際電信電話株式会社（現KDDI株式会社）入社。KDDI America,Inc. 技術担当副社長、Telehouse America 社長、KDDI Europe Limited 技術担当副社長などを歴任。2014年4月、ラック常務執行役員に就任。2016年5月より現職。

セキュリティ人材育成は企業のIT戦略立案にも役立つ！

司会：次に、経営者が組織のセキュリティを考える上ですべきことについて伺いたいと思います。

西本：サイバーセキュリティ経営ガイドラインに沿って考えるのがよいでしょう。まずはCISO（最高情報セキュリティ責任者）を立てることです。厳密な役職でなくても構わないと思っています。経営責任を負える人を決めて、ガイドラインを読むよう指示すればよいのです。すると、任命された人の顔が青ざめるはずです（笑）。私自身もラックのCISOに就任しましたが、自社のセキュリティについて改めて考える機会となりました。取締役という立場でCISOに就任するというのは重大な責任を負うことです。何かが起こった時に、知らなかったでは済まされませんから、おのずと意識は変わると思います。まずはここから始めるのがよいでしょう。本誌をご覧になっている多くの方は、何かしらのシステムと関連している企業の方だと思いますが、もし「うちの会社はシステムなどと無関係」などという会社があれば、実はそちらの方が危険です。なぜなら、そういった企業では従業員がルールを無視してシステムを自由に使うからです。昨今言われるセクハラ、パワハラ、過労などは、経営者として知ら

英 秀明 はなぶさ ひであき

株式会社ラック 取締役 常務執行役員 ITプロフェッショナル統括本部長。1964年生まれ。1988年、ラック入社。執行役員 SI事業本部長、エー・アンド・アイ システム株式会社 取締役などを歴任。2016年4月より現職。

4 SoE（System of Engagement）「絆のためのシステム」とも訳される。多種多様なデータソースの収集・分析によってビジネスパートナーや顧客に対して新たなコミュニケーションやコラボレーションの手段を提供するシステム。米国ボーイング社が航空機の主要部品にRFIDを取り付け、使用履歴やメンテナンス情報などを部品メーカー・整備会社・航空会社などと共有し、不要な在庫部品の削減や整備作業の効率化を図る取り組みなどはSoEの一例といえる。

なかったとは言えない課題であることが広く認識されています。これと同様に、セキュリティもトップが腹を決めて号令をかけないと動きませんし、継続できないのです。

司会：ある日突然、企業の CISO に任命されて、戦々恐々としている方などはいらっしゃいますか。

西本：当然いらっしゃいます。サイバーセキュリティ基本法が施行され、日本年金機構の情報流出事件などが発生し日本中が大騒ぎになる中、サイバーセキュリティ経営ガイドラインでは経営責任であることが明確化されました。例えば、CISO を置かずに現場の担当者の力で対応している組織も多いと聞いています。そういった企業では、そのこと自体がリスクなのです。ですので、ガイドラインによって CISO を任命せざるを得ないという状況になり困惑しているのが現状だと思います。

司会:関連する話題ではありますが、セキュリティ対策において、経営層と現場の技術者との間を取り持つ橋渡し的な役割を担う人材の育成が重要だともいわれています。この課題についてはどのように取り組んだらよいと思いますか。

西本：本来であれば、経営陣の中に IT システムについて理解している人物がいなくてはならないと思います。例えば、大手の銀行などではキャリアパスの中で、IT システムの部署を経験していないと頭取にはなれない仕組みになっているそうです。金融業は元々 IT システムそのものと言っても過言ではありませんから、早くからそういう認識を共有されていたのだと思います。ただ、一般的な企業の場合、IT システムは効率を上げる単なる道具であり、事業に付帯するものという認識だったはずです。そこへガイドラインが発表され、経営課題としてセキュリティが突き付けられた格好となりました。本来であれば、IT の重要性を理解せずに経営に携わること自体が問題だと思いますが、難しい課題ですね。

英：大企業であれば、経営層へのキャリアパスの一環として IT 部門を経験させることが可能だと思います。IT 部門といえば、ビジネスを下支えする役割との色が強かったと思います。しかし近年はクリエイティブな事業を企画推進し、ビジネスのエンジンを創出する役割を担うケースも増えました。ただし、中小企業の場合はどのようにするかという問題は依然残っていると考えます。

司会：わかりました。中小企業のセキュリティ対策については後ほどまとめてお話を伺いたいと思います。

西本：話はそれますが、先ほどの SoE は誰が企画しているのでしょうか。例えば SoE で事業競争力を高めたいと考えた場合、それを主導するのは、事業部側ですか、それともシステム部門側、どちらでしょうか。

英：ケースバイケースだと思います。事業企画側が主導することもありますし、システム側が主導することもあります。場合によっては共同して進めることもあります。

西本：IT のセンスがないとおそらく SoE は発想できないと思いますが、いかがでしょう。

英：技術的な知見がないと難しいですね。技術だけで言えば、外部の技術力に頼るケースもありますが、その実現性や可能性などさまざまな尺度によって判断するためには経営層を含め自ら技術への知見を深めることは必須です。経営力・IT・クリエイティブな知見などさまざまな能力をチーム化する、まさに英知を集結して推進することになります。

西本：現在のビッグデータや IoT といったキーワードを自社の事業に活かすとすれば、積極的に SoE などを展開する必要があると思います。こういった IT 戦略のプランニングを誰が企画・実施していくかという骨格を作っていかなければ、企業として生き残りは難しいのではないでしょうか。SoE などは、企業内に埋もれているデータ同士を結び付けると大きな化学反応が起きるようなものだと思います。企業戦略には IT やデータの活用による新たな価値の創造といったことも重要ですから、CISO に限らず、経営層の中にシステムについて理解している人材が必要ですね。

三木：個人的な意見ですが、リーダー層でも企業の IT 戦略のプランニングは可能だと思います。もちろん、全体を鳥瞰できて、かつ技術のことを理解しているというスキルセットを持っている

ことや部署間を横断的に統制できることが前提となります。組織内のどこかの部署に強みがあり、それを差別化の要素にして新たなビジネスを立ち上げていく場合、セキュリティの観点からもさまざまなことを考えなくてはならないと思いますが、実はそれ自体がビジネスチャンスにつながる可能性もあります。セキュリティ人材の育成は重要ですが、セキュリティに特化した人材ではなく、IT 全般を経営的な視点から捉えられる人材を戦略的に育てていかなくてはならないのではないでしょうか。

イノベーションに新たな脅威は付き物で、セキュリティへの取り組みは重要かつ必然の要素です

新たなテクノロジーの登場・普及が社会を一変させる!?

司会：IoT、ビッグデータ、AI、フィンテックなど、現在さまざまなキーワードが話題となっていて、これまでのビジネスのやり方を一変させるような応用技術の登場を期待する声が上がっています。一方で、どの言葉も定義があいまいで、懐疑的な見方をする人たちもいます。過去のキーワードを見ると、クラウドコンピューティングなどは、言葉だけが先行してトレンドとしてもてはやされた時期もありましたが、いったんは沈静化しましたが、その間もクラウドコンピューティングの技術を応用したサービスが次々と登場し、現在のインターネットビジネスを考える上で不可欠な要素となっています。こういった流れからすると、現在のキーワードも流行語としてはいったん廃れますが、その後まったく新しいサービスなどが登場する可能性もあると考えられます。これらを踏まえて、経営者は新たなテクノロジーとどのように向き合っていけばよいとお考えですか。

西本：先ほど話題に出た SoE は、システム同士が連携し新たなビジネスや価値を生み出していきますので、現在の IoT やフィンテックなどにつながっていくものだと思います。おっしゃるとおり、新たなテクノロジーが出てくると過度の期待からブームとなりますが、当初は実体が伴わないことから幻滅期に入ります。しかし、背後では、その技術を応用した製品やサービスの開発は進んでいて、ある時、別のところから実体を表します。最近の例でいえば、フルハイビジョンテレビよりも高画質な 4K テレビの方が低価格という逆転現象が起こっているといいます。これは日本メーカーよりも中国などのメーカーがいち早く 4K に目を向けて製品開発に取り組んだ結果なのだと思います。「イノベーションのジレンマ」の一例とも言えます。企業が従来の技術にとらわれていると、その技術の衰退とともに企業も衰退していきます。ですから、新たなテクノロジーに対し世間の評判だけで判断するのではなく、その将来を見据えておく必要があると思います。これはわれわれ自身も肝に銘じておかなくてはなりません。

司会：4K テレビの例とは少し違いますが、自動車業界では、目下「自動運転」技術の開発に躍起になっています。自動車メーカーの競争はこれまで、より効率のよいエンジンの開発や、故障が少ない信頼性の高い製品の開発などでした。ところが、自動運転というテクノロジーの登場で、競争のルール自体が大きく変わりました。米国のテスラモーターズといった新興勢力や Google といった他業界からの参入も相次いでいます。

西本：ご存じだと思いますが、日本では自動運転車の公道での走行実験には法律による制限があります。ですから日本メーカーも海外で実験を行っていると聞きます。自動車業界に限らず、医薬品など他の分野でも法律の規制があり、日本国内での活動には制約があります。このままで

セキュリティに特化した人材ではなく、IT全般を経営的な視点から捉えられる人材を戦略的に育てていかなくてはならないのではないでしょうか

はあらゆる分野で日本の競争力が失われてしまうのではないかと心配です。しかし、こういった状況でも製品の品質や、セキュリティ・安全面はおろそかにできません。この点を外してしまうと日本製品が海外勢に駆逐されてしまうのではないかと思います。そういったことから、ラックの SI 事業においても品質に対する信頼の獲得は譲れない基本姿勢として貫いています。

英：新たなテクノロジーの登場による社会の変化にも注目すべきだと思います。先日、未来予想についての興味深いお話を伺いました。自動運転車の普及がさまざまな業界に及ぼす影響についてです。自動運転実用化の影響が及ぶ業界として自動車、エネルギー、流通、保険などは容易に想像できますが、思わぬところでは不動産業界などにも大きな変化が起こり得るとのことでした。自動運転による車の運行なら道路幅は今より狭くても通行可能で、その分敷地面積も広くなり、建物も変わっていく。ひいては地図も変わり、法規制や国土利用のあり方まで変化するという壮大な可能性があるとのことでした。

西本：どれくらい先になるかはわかりませんが、自動運転車が普及した時代では、カーシェアリングが中心になるでしょうから、建物の地下や 1 階は大部分が駐車場になるかもしれません。また、現在は人間が運転する自動車と自動運転車が混在することとなりますから、自動運転車側で事故を回避するための高度な技術が必要とされているわけです。仮にすべての自動車が自動運転車になれば、自動車同士がピア・ツー・ピア（1 対 1）で接続すればよいので、現在言われているような技術は不要になるはずです。東京などはこういった自動運転車しか走行できないようにすれば、もっと効率のよい都市になるはずです。小池百合子都知事にはぜひ頑張っていただきたいですね（笑）。

■ 企業が対峙する攻撃者の姿

司会：話題をセキュリティに戻したいと思います。最近ではセキュリティ分野における経営判断を支援する目的で「脅威インテリジェンス」を提供する企業が増えているように思います。ただ、この言葉も定義があいまいです。諜報機関のレポートのような響きがあって、部外者からすると内容が見えにくく、かつ本当に活用されているのか、疑問に思うのですが、いかがでしょうか。

西本：企業は事業を行う時に市場調査を実施します。市場規模、同業他社の強みや弱み、例えば流通業でしたら POS データによる実際の売れ筋や在庫管理などの実態把握をしないと生き残っていけません。セキュリティも同様です。脅威の動向を知らずして守るというのはあり得ません。「脅威インテリジェンス」なしにセキュリティ対策を進めようとするのは、風車に突撃したドン・キホーテとまさしく同じです。脅威インテリジェンスというと特殊なもののように感じるかもしれませんが、ごく自然なものです。これまではセキュリティ担当者間の寄り合いで情報共有していました。ラックでは JSOC が収集したデータを分析して、お客様に現在の動向や新たな脆弱性情報などをお知らせしていました。

司会：そうすると、これまでセキュリティに関わる人たちの中で共有されていた情報を企業が販売するために「脅威インテリジェンス」という名前を付けたということになるわけですね。ただ先ほども言ったとおり「脅威インテリジェンス」というと諜報機関のレポートのような印象を受けてしまいます。

三木：諜報機関というと大げさと感じるかもしれませんが、実はそうではありません。中国は

他国の機密情報を盗んでいると報道されることがあります。それは国防のためだけに限らず、自国の経済発展のためだとも言われています。CYBER GRID VIEW Vol.2[ii]でも紹介していますが、いくつかの事象から類推することによって攻撃者像が浮かび上がってきます。もし攻撃主体が国家、もしくは国家の支援を受けている者だった場合、一民間企業の努力だけでは太刀打ちできず、さまざまな企業や団体が協力して事に当っていく必要があるわけです。現在、「脅威インテリジェンス」の提供はビジネスとして行っていますが、今後は、別の形も考えられるでしょうね。

西本：昨年、米国のオバマ大統領と中国の習近平国家主席が会談し、「両国政府は知的財産に対するサイバー攻撃を実行、支援しない」ことで合意しました。要は「企業秘密などの知的財産を盗む行為はしない」ということです。少なくとも、米国は、中国は国家として米国の企業秘密を盗んでいたとみているということになります。企業はこういった国家レベルの攻撃者を相手にセキュリティ対策をしていかなくてはならないのです。そこに経産省から「サイバーセキュリティ経営ガイドライン」が公表され、企業の責任が明確になったわけです。つまり外からは国家レベルの敵に相対し、何かあるとお上からお叱りを受ける構造が出来上がっているわけで、先に言ったように、任命されたCISOの顔が青ざめるというのもわかっていただけると思います。この点を自覚しなくてはならないのです。

三木：日本は法整備が遅れているという側面もあると思います。米国の場合は、スパイ防止法[5]の他に経済スパイ防止法[6]というものがあります。日本でも不正競争防止法がありますが、不十分だと言わざるを得ないと思います。以前から言われていることですが日本は「スパイ天国」なのです。

西本：日本では、戦前の軍国主義時代のトラウマからか、スパイ防止法への取り組みについては消極的だったと思います。しかし、経済を含めてサイバー空間での活動がより活発になっていく中で、これらの情報の窃取に対しては何らかの対策を早急に考えるべきだと思います。

セキュリティインシデントが発生したとき企業はどのように対応すべきか？

司会：次の話題です。情報漏えい事故が発生した場合についてです。対応のポイントなどがあれば教えてください。

西本：事故対応の考え方は大きく3つあると考えています。1つ目は「被害者の保護」です。被害者というのは取引先や顧客などの関係者ですから、被害を封じ込めた上で被害拡大の防止策を図る必要があります。まずここに全力を尽くさなくてはなりません。また、被害拡大を防ぐためには情報を共有する必要があります。しかし、多くの組織では事故そのものを隠ぺいしたり、被害拡大防止に手を打とうとする関係者（関係する被害者）に必要な情報を提供しなかったりします。この点でいえば、被害拡大の防止策ができていないということになります。2つ目は漏えい事故の原因が社のルールに違反するもので、それが常習的に行われていた（割れ窓現象）場合、それは経営責任になるという点です。3つ目はルールや対策が適切であったかどうかです。ただし、これは、何を再発させないかの観点が極めて重要ですがいわゆる再発防止策で事故対応後に見直せばよい問題です。事故対応で経営者が認識しておかなくてはならないのは、例えば情報漏えい事故が起きた場合、次にどんなことが起きるのか、という点です。元々、そういう事態を招かないようにするための対策だと考えてしまうと、そこで思考が停止してしまいます。思考停止することがないように理解して納得しておく必要があると思います。

三木：少しテクニカルに話をすると、この問題はシステム系の問題とヒューマンエラー系の問題に分けることができると思います。システム系は元々、人間の負荷を減らす目的で導入され、なおかつ継続的に利便性を確保しながら運用するのが前提です。仮にここに問題があるのであれば、当然正さなくてはなりません。一方、どんなに注意をしていても人間が介在する限りミスはつきものですから、システム側で人間がミスをし

5 スパイ防止法（Espionage Act of 1917）
米国が第一次世界大戦に参戦して間もない1917年に制定。その後数回の改正を経て、現在では合衆国法典第18編第37章「諜報活動と検閲」内に記載。米国に損害を与える意図を持った者による国防情報の取得・受領・漏えいなどの行為を規制している。

6 経済スパイ防止法（Economic Espionage Act of 1996）
1996年に連邦法として制定。米国企業を保護することを目的としており、企業の知的財産・営業秘密を従業員・競合他社・外国政府が不正に取得する行為などを規制している。

たとしてもある程度事故を防げるような仕組み作りも必要かもしれません。

司会：セキュリティインシデントと関連して「サイバー保険」についても伺いたいと思います。ラックも代理店業務を行っていますが、サイバー保険については、現状あまり売れていないと聞いています。それでもなお扱うのには何か意図があるのでしょうか。

西本：世界的に見てもサイバー保険は大きな市場にはなっていないと思います。ラックも過去に何度もチャレンジしてきました。企業がセキュリティ対策など、やるべきことをやっていて、それでも被害を受けてしまった場合に有限責任にならないというのは健全な社会とはいえないと思います。例えば個人情報漏えい事件が起きた時など、企業は過度な責任を負わされていると思います。だからこそ保険が機能する社会にしなくてはなりません。ただし、その有り様はまだまだ模索中です。自動車の場合、保険に入っているからといってどんな運転をしてもよい、ということにはなりません。同様に、サイバー保険についても、組織のセキュリティの堅牢性・掛け金・補償内容などのバランスを取っていく必要があります。ラックとしては今後のセキュリティ業界を考える上で、積極的にチャレンジしたいと考えているわけです。

英：保険業界では取り扱う保険の種類別に３つのジャンルに区分されるそうです。終身保険や養老保険などの「生命保険」は第一分野、自動車保険や火災保険などの「損害保険」は第二分野、医療保険や疾病保険などは第三分野です。セキュリティインシデントの被害拡散スピードの速さや脅威の進化によるビジネスの復旧や信用失墜といった新たなリスクへの対応は急務となっており、社会性の高い保険業界にも「情報」を扱うこの巨大な分野が注目されていることは間違いないと思います。

司会：今年１月、カレーチェーンの CoCo 壱番屋で廃棄を依頼した冷凍カツが業者により不正に転売されたという事件が発生しました。この時 CoCo 壱番屋の対応が迅速だったと評価されています。事件発覚の発端は、パート従業員がスーパーで買い物中に自社の冷凍カツを発見し、本部に連絡したことだそうです。このように迅速にトップに情報が上がるための仕組み作りで必要なこととは何でしょうか。また、情報の伝達にかかる時間を早くするためにはどのような組織作りが必要だと思いますか。

西本：今年９月、人事院が「懲戒処分の指針について」の規定を一部改正して、国家公務員の秘密漏えいについて、その原因が情報セキュリティ対策を怠ったことによるものだった場合は停職や減給の処分を課す、という発表を行いました[iii]。しかし、こういったアプローチを取るのなら、運用をきちんとしないと、現場は隠ぺいしようとする動きが強くなるのではないかと危惧しています。逆に、普段から報告することは良いことだという組織の風潮を作っていかなくてはなりません。これは経営層の仕事です。しかし、経営者は往々にして「オレに悪い話は聞かせてくれるなよ～」といった態度を取ってしまいます。これでは、いざというときに情報が上がってくることはありません。また、普段から報告が遅れがちな組織についても同様だと思います。これは自戒の意味も込めてということになりますが（笑）。

英：他にも、個人が何とかしようと頑張ったがゆえに報告が遅れるケースもありますね。頑張ること自体は褒めるべきですが、それ以前に黙って頑張ることは組織的に「アウト」だということを周知させなくてはなりません。なかなか難しい問題です。

西本：日本の組織では失敗した時に責任を取らされるという意識が強いからなのだと思います。こうした責任についても企業文化として見つめ直してみるとよいのではないでしょうか。

三木：組織内での社員の評価が減点方式だとなかなかうまくいかないのではないでしょうか。もちろん、こういった評価をすべき部署や従業員も存在するとは思います。ただし、組織内すべてにこの基準を当てはめる必要もないはずです。一方で「何でもかんでも報告しろ」というのも現実的には難しいですし、管理できません。組織内で最低限報告すべき情報をきちんと整理し、「報告・連絡・相談」手順を策定するところか

ら始めてはどうでしょうか。

西本：情報の伝達に関連して 1 つ紹介したい事例があります。今年 9 月、会計検査院が政府の情報システムに関して報告書を発表したのですが、この報告書の中で政府情報システムのセキュリティ対策についても言及しており、約 7 割のシステムでセキュリティリスクの評価が実施されていないと明記しています[iv]。会計検査院がセキュリティ対策に踏み込んで言及するのには違和感を覚えますよね。一見すると、会計検査院の指摘によってセキュリティ対策費用が余計にかかるのではないかとも受け取れます。しかし会計検査院としては、セキュリティリスクを抱えたままのシステムを使い続ける方がそれ以上に費用がかかる可能性があると判断したのだと思います。これは重要なメッセージです。ですから企業内のシステムにおいても、今後監査の観点で経営者が責任を果たしているのかといった視点も重要になるでしょう。

中小企業の情報セキュリティ対策

司会：続いて中小企業のセキュリティ対策について伺います。現在、独立行政法人 情報処理推進機構（IPA）が「中小企業の情報セキュリティ対策ガイドライン」の改訂[v]を進めています。ただ、現時点（10 月 6 日）では公開前ということもあり、取り上げないこととします（編注：11 月 18 日に公開）。前置きが長くなりましたが、予算も人材も不足している中小企業ではセキュリティ対策にどのように取り組んでいけばよいでしょうか。

西本：企業にお金がないからといって、車検が切れた自動車で営業してもよいということにはなりません。セキュリティ対策もこれと同じだと思います。業務でインターネットを使うのであれば、セキュリティに関する最低限の知識は持っていただきたいと考えます。セキュリティ対策は「安全」対策と理解している方も多いでしょう。先ほどの自動車の例で考えると、自動車の整備までは自社では行いません。従業員には道路交通法の遵守や事故を起こさないための「用心」が重要です。セキュリティにおいても同様に従業員の「用心」が重要な要素になります。中小企業は大企業と比較して従業員が少ないので、この「用心」の向上は、安価にセキュリティのレベルを高めることができ、企業競争力も高められる方策といえます。また、サイバーセキュリティ経営ガイドラインでは、サプライチェーンも含めた形でセキュリティ対策に取り組むよう明記されています。大企業に依存している中小企業も多いと思われますので、その意味からもセキュリティ対策強化に努めるべきだと思います。

司会：では具体的にどのような対策を講じていけばよいでしょうか。

西本：中小企業という言葉は、資本金や従業員数の規模によって定義されていますが、製造業やサービス業といった業種によっても異なっています。また、中小企業という言葉から連想する組織のイメージも人によってまちまちです。例えば、従業員 10 人程度の町工場で CSIRT の設立というのはあまり現実的とはいえません。そもそも中小企業では、情報システム部門を持たない方が多いはずですから、大企業のやり方とは違う形で考えた方がよいでしょう。1 つ参考になるのは地方自治体のセキュリティではないでしょうか。総務省では「地方公共団体における情報セキュリティポリシーに関するガイドライン」を公表しています[vi]。ちなみに、日本でいちばん人口の少ない地方自治体は伊豆諸島南部に位置する「青ヶ島村」で、人口 168 人（2016 年 6 月現在）なのだそうですが、このガイドラインではこういった自治体のセキュリティについても指針を示しています。例えば、インターネットのサーバーなどは自前で構築せずクラウドサービスを利用すること、マイナンバーなどの重要データを扱うコンピューターはネットワークから切り離すことなどが含まれています。自治体の例を参考にした極端な例かもしれませんが、業務は従業員のスマートフォンやタブレットで行う。重要な顧客情報などはネットワークから切り離した場所で管理するなども考えられると思います。

司会：ありがとうございます。ここで話題を現実的な方向に移します。現在、ランサムウェアが

猛威を振るっています。ランサムウェアとは、ハードディスクやファイルサーバーのデータを暗号化してしまうコンピューターウイルスの一種です。攻撃者はデータを人質に取り、元に戻してほしければ身代金を払えと脅迫してきます。2015 年あたりから急激に被害が増大しているという話ですが、ランサムウェアを防ぐ方法はありますか。

西本：ウイルス対策ソフトの検知をすり抜けるものも多いですから、完全に防ぐことは難しい状況です。防衛策としては社内ネットワークから切り離された場所にデータのバックアップを用意するしかないと思います。

司会：わかりました。では現実にランサムウェアに感染してしまった場合、どのように解決したらよいでしょうか。ネットを見ていると、米連邦捜査局（FBI）が言うように身代金を支払い、データを復号してもらうのがよいという意見もあれば、一方で身代金を支払うことは反社会勢力に利益を供与することだとして、支払うべきではないと主張する人たちもいます。このあたりはどのような考えをお持ちでしょうか。

西本：法令の遵守は別として、企業で重要なのは顧客を守ることです。ですから、暗号化されたデータを元に戻せなければ、顧客を守ることができないという状況であれば、身代金を支払うのもやむを得ないと思います。しかし、身代金を支払うことはある面犯罪者への利益供与とみられ経営責任が問われることになっても不思議ではありません。ですから、身代金を支払うなら経営者の退陣もやむなしくらいの覚悟は持ってほしいと思います。ランサムウェアの脅威は一般のニュースで報じられるほど知れ渡っています。セキュリティ対策としてはもちろんのこと、経営問題に発展させないためにもオフラインのバックアップ作成をお勧めします。

セキュリティ業界の今後の展望

司会：次にセキュリティ企業との付き合い方について伺います。セキュリティ企業は顧客の不安をあおって商売につなげている側面があると思います。一方、顧客の方は、どういった基準でセキュリティ企業を選んだらよいか判断できないことも多いと思います。例えば、住宅建設や中古車販売といった分野では、業界の専門家が「業者選びのポイント」などを指南する雑誌企画などがあります。セキュリティ業界でこういった業者選びのポイントは何かありますか。

西本：「これさえ導入すれば万全です」「完璧です」というセールストークは疑った方がいい（笑）。セキュリティ企業の役割には「安全・安心を提供する」の他に「怠ってはならない用心を喚起させる」という側面があると思います。顧客の不安をあおるという表現を使われると、ラックとしても多少耳が痛い部分がありますが、われわれはわれわれのやり方で「用心」を喚起していきたいと思います。

三木：組織がそれぞれ違うようにセキュリティ対策も組織ごとに異なるはずです。ですから、セキュリティ企業側が組織に寄り添って、実現可能な対策から優先順位を付けた提案をしてくれるようなところに相談するのがよいのではないでしょうか。

英：製品や自社サービスを売り込むだけのセキュリティ企業よりも、恒久的な事後対策や運用も含めた提案ができる企業の方が信頼できると思います。医療の現場に例えると、ただ薬を処方するだけの医師と、患者の話にきちんと耳を傾けてくれる医師とを比べて、どちらがよいかということと似ていると思います。甚大なインシデントに見舞われたお客様は相当な不安の中で事態に対処し、収束していく必要があります。そのため、さまざまな観点から共に対応を考えるという点が最も価値を置くべきところではないでしょうか。

司会：さて、最後の質問です。日本の IT 業界発展のために業界全体として取り組まなければならないことは何でしょうか。また、日本の強みや環境を活かした施策はあると思いますか。このあたりについて考えを伺いたいと思います。

西本：これは提言というよりも反省も込めた意見です。「日本では IT 業者はいるけれど、IT 業界はない」と言われることがあります。IT ゼネコンという言葉もありますが、これは発注者から一括で仕事を受注した企業の下にいくつもの下請け

企業が連なる構造が建設業界と似ていることに由来しています。この構造下では、下請けや孫請けの企業は、元請けから指示されたシステムを適切に構築することが重要で、そのシステムが顧客や社会へ貢献しているという実感までは持てない技術者も多いのではないでしょうか。これはこれで重要なことですが、一方、変化の激しい時代においてそれぞれのプロの見立てや意見も重要になってきていると思います。つまり、請け負っている仕事をこなすだけでなく専門分野を背景にもう一歩踏み込むことで、社員の一人ひとりが社会を支えているという実感を持てるような組織を目指したいと思います。さらに、今後の企業のあり方を考えるとITの事業が企業の事業そのものになっていくはずです。ですから、以前のようにシステムを開発して納品すれば終了という仕事だけでなく、企業を取り巻く環境変化に合わせてシステムの改良を進めるなど、運用にも携わっていくべきだとも考えています。

英：ITの爆発的な普及や社会インフラの急速な技術進化への期待は明らかです。先端技術を利用できるよう、社会を変えていく必要があると感じています。法改正のほか、地域を限定して規制緩和などの特例を設ける「特区」の一層の推進など、イノベーションを育む環境を作っていかなければグローバルな競争の中で日本の存在感は出しにくいと思います。ITに限らずさまざまな知恵を持った人たちはたくさんいるはずですが、日本国内では形にしにくいという状況もあると思います。やはり社会全体で取り組んでいかなくてはならないでしょう。

三木：先日、高校生のICTカンファレンス「ネットの安心・安全を自ら考える」に参加して、彼らと意見交換をする機会がありました。彼らは幼い時から身の回りにIT機器があって、われわれ大人とはモノの見方も使い方も違っています。こういった若い世代が考えるセキュリティというのもまた新鮮に感じました。彼らがITの世界を牽引していくことになるのはもう少し先のことですが、いち早く彼らの意見を取り込んでいくことも重要だと感じています。この観点では、ラックは「ITスーパーエンジニア・サポートプログラム“すごうで”」を2013年から毎年実施し、若手エンジニアの活動を支援しています。

司会：本日はどうもありがとうございました。

セキュリティ企業の役割には「安全・安心を提供する」の他に「怠ってはならない用心を喚起させる」という側面があると思います

出典

i　サイバーセキュリティ経営ガイドライン
http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf

ii　CYBER GRID VIEW Vol.2「日本の重要インフラ事業者を狙った攻撃者」
http://www.lac.co.jp/security/report/2016/08/02_cgview_01.html

iii「懲戒処分の指針について」の一部改正について
http://www.jinji.go.jp/kisya/1609/choukai280930.htm

iv　会計検査院法第30条の2の規定に基づく報告書
「政府の情報システムを統合・集約等するための政府共通プラットフォームの整備及び運用の状況について」
http://www.jbaudit.go.jp/pr/kensa/result/28/pdf/zenbun_h280929_01.pdf

v　中小企業の情報セキュリティ対策ガイドライン
http://www.ipa.go.jp/security/keihatsu/sme/guideline/

vi　総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」
http://www.soumu.go.jp/main_content/000348656.pdf

リサーチャーの眼

《研究・開発の最前線からお届けする技術情報》

第2回

セキュリティ対策の新たな常識「セキュア・ウェブ・ゲートウェイ」について

文＝内田 高行（サイバー・グリッド・ジャパン　次世代技術開発センター担当部長）

サイバー攻撃による被害が数多く確認される時代となり、多くの企業や地方自治体（以下組織）ではセキュリティ対策への関心がこれまでになく高まっています。しかし、一言でセキュリティ対策といっても何から手を付ければよいのかわからない、セキュリティ対策の重要性は理解できるがコストは抑えたい、という話もよく聞きます。そこで今回の「リサーチャーの眼」では、最低限のセキュリティ対策では不十分といわれる中、新たな常識となりつつある「セキュア・ウェブ・ゲートウェイ（以下 SWG）」について概要を説明します。

組織の一般的なセキュリティ対策環境

多くの組織では、外部からの攻撃は「ファイアウォール（FW）」で防御し、内部に入り込んだコンピューターウイルスを検知・除去するために「ウイルス対策製品（AV）」を導入していることと思われます。セキュリティ対策としてはこれが最低限の組み合わせです。これに加えて、国内中規模以上の組織の約 5 割が「URL フィルタリング製品（UF）」を導入しているとされます（MM 総研調べ）。URL フィルタリングは、アダルトサイトや SNS サイトなど業務に必要のないサイトに社員がアクセスしないよう、労務管理の一環として導入されていますが、実はセキュリティ対策においても重要な役割を果たしています。コンピューターウイルスに感染させたり不正広告を埋め込んだりする悪質な Web サイトへのアクセスを制限する機能です。つまり「触らぬ神に祟りなし」を実現するのです。ファイアウォール、ウイルス対策製品、URL フィルタリングの組み合わせを表したのが**図 1** です。

セキュリティ対策の新たな常識となる SWG

ファイアウォール、ウイルス対策製品、URL フィルタリングの組み合わせによるセキュリティ対策からもう一段の強化が叫ばれていますが、運用の手間、コストなどの面から大規模なセキュリティ対策を採用することにちゅうちょしている組織が多いのも事実です。そこで、次のステップとしてふさわしいセキュリティ対策を容易に実現するのが、SWG です。

SWG は複数の機能からなるセキュリティ対策機器です。その機能の多くは「外に出て行く通信」を制御することを目的としており、それによって Web アクセスに関連するさまざまな脅威を大きく減少させます。標的型攻撃メールに代表されるようなサイバー攻撃は依然として組織にとって最大の脅威といえますが、Web サイトにウイルスを仕込み、サイト訪問者へ攻撃を仕掛ける手法も昨今、頻繁に確認されています。また、ウイルスを仕込まれたコンピューターが情報を盗み出す脅威にも、Web アクセスの経路

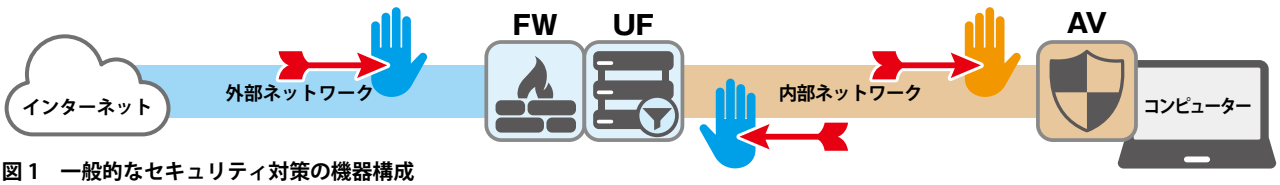

図 1　一般的なセキュリティ対策の機器構成

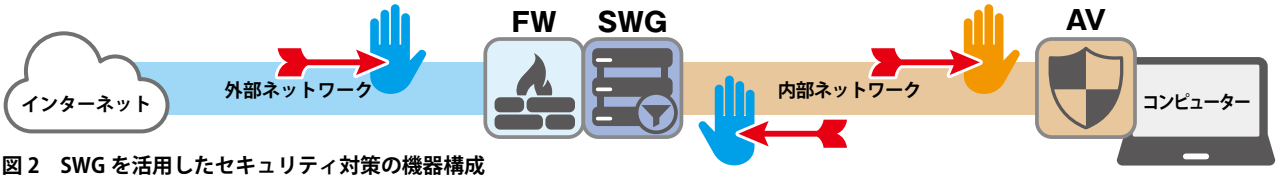

図 2　SWG を活用したセキュリティ対策の機器構成

機能	概要
出口対策	危険なサイトや危険の可能性があるサイトへの通信を遮断する
URLフィルタリング	アクセスが不適格な Web サイトなどを分類し、通信を制限する
Web アプリケーション制御	SNS への投稿を制限するなど、Web サービスの利用を制限する
アクセスログ収集・保存	情報漏えいなどの事実確認のため、アクセスした Web サイトへのアクセス履歴を保存する
入口対策	パソコンに導入されているウイルス対策製品と連動し、Web 通信時の悪意のあるプログラムを検知する。
Webプロキシ	認証やキャッシュ機能をもった Web アクセスの中継機能で、Web ブラウザーからのアクセス要求を代理で処理することで、効率性と安全性を実現する

表 1　SWG が提供するセキュリティ対策機能とその概要

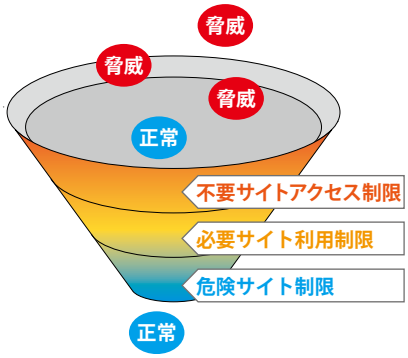

図 3　脅威を減少させる概念図

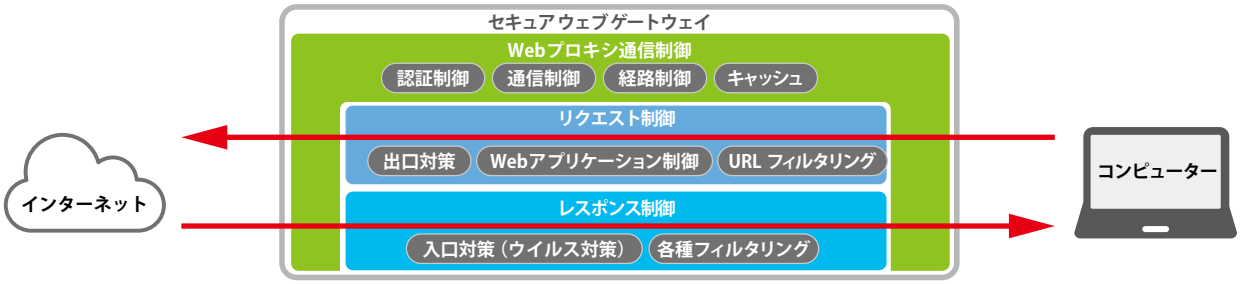

図 4　SWG の機能構成と通信の流れ

を使われることが多くなっています。つまり SWG とは、Web の安全性を高めることで企業全体のセキュリティ対策に有効な手段となるわけです（**図 2**）。

SWG が提供する機能を一覧にまとめました（**表 1**）。SWG の機能で最も重要と考えられているものが「出口対策」です。たとえウイルスに感染しても、データやファイルを流出させずに被害を封じ込めてしまうのです。

近年、攻撃者は開発したウイルスを攻撃に使用する前に、各種ウイルス対策製品で検知されるかどうかをあらかじめ調査しています。そうなるとコンピューターに導入している従来型のウイルス対策製品は用を成さなくなります。代わって注目されているのが「出口対策」です。万が一、組織内にウイルスが入り込んだとしても情報窃取といった被害につながらないよう、ウイルスが Web アクセスを悪用して情報を配信する行為を検知し、遮断してしまう技術です。

そして、SWG のもう 1 つの特徴的な機能が「Web アプリケーション制御」です。SWG の導入を検討している組織の多くがこの機能に注目しています。

Web アプリケーション制御は、従来の URL フィルタリングと同様に不要な危険を排除することを目的としていますが、両者には大きな違いがあります。Web アプリケーション制御の場合、例えば SNS の閲覧は許可するが投稿は禁止するなど、URL フィルタリングでは制御できない高度なアクセス制限まで行うことができ、Web サイトの利用を許可しながら深刻な脅威に利用者が遭遇する機会を減らすことができるのです（**図 3**）。

一般的には多機能な SWG ですが、機能を Web アクセスのセキュリティ対策に絞ることで、既存のファイアウォールやウイルス対策製品によって構成されているセキュリティ対策環境との親和性が高くなります。それだけでなく、ファイアウォールの内側にプロキシサーバーとして設置しても機能させることが可能です。そのため導入の手間も少なく、対策を行う技術分野が Web アクセスのみに限られているため、専門スキルを持つネットワークエンジニアがいなくても比較的簡単かつ効率的に運用することができます。**図 4** に、SWG の機能構成と通信の流れを示します。

SWG のこれからと、ラックの取り組みについて

ここまで一般的なセキュリティ対策の構成と SWG の特徴について述べてきました。これまでは最低限のセキュリティ対策しか行わなかった組織が今後の対応を検討するとき、SWG は有効な選択肢となるでしょう。

ラックの次世代技術開発センターでは、既存の SWG では実装されていないいくつかの機能を備えた新しい SWG の可能性について研究を進めており、これまでに蓄積してきた脅威に関する情報を有効活用する手段や、防御の新たな仕組み作りを行っています。

研究の結果は何らかの形で IT を活用する組織のセキュリティ対策支援に役立てたいと考えています。

ラックの顔　様々な場所で活躍する社員をご紹介

“システム開発やセキュリティ分野の専門家と経営をつなぐゼネラリスト”

第2回 大野祐一　トヨタメディアサービス

日本を代表する企業の 1 つであるトヨタ自動車。そのグループ内で公式サイトの運営やテレマティクス（移動体通信システムを利用した自動車への情報サービス）を提供しているのがトヨタメディアサービスだ。

今回ご紹介する大野祐一は、この組織のチーフ・セキュリティ・ストラテジストを務め、目下 CSIRT 設置に向けて準備を進めているという。

インタビュー＝斉藤健一（株式会社 HTP）

自らが率先して行動するリーダー

大野祐一がラックに入社したのは 1994 年。日本大学生産工学部数理工学科に在学中から、「ソフトウェアを作ることはコンピューターを使いこなすこと」と考え、独立系のソフトウェア開発会社を志望していた。当時は、ラックがセキュリティ事業に乗り出す前で、SI（システム・インテグレーション）が事業の柱であり、大野も入社後 10 年間にわたり、システム開発事業に従事した。

「ラックの顔」ではインタビューに先立ち、毎回その人物を知る周囲の社員から人柄を表すエピソードやコメントを集めているが、大野の人物評を見ると「システム開発案件で日程が厳しい時などに頼りになる先輩」といった声が数多く寄せられている。このことを本人に尋ねてみると、当時を振り返りこう語ってくれた。

「今でこそセキュリティ業界でのラックの知名度はありますが、当時の SI 事業ではそれほどでもありませんでした。お客様の方が強い買い手市場ということで、さまざまな仕様変更にも応じざるを得ないことが多く、プロジェクト・マネージメントが不十分だったこともあり、納期間際になると徹夜が続き、メンバーに迷惑をかけたこともあります。ただ、当時は自分の背中を後輩に見せられていたと思います。自分自身でプログラミングも行っていましたし、オフィスでは私が最後まで残って仕事をしていました。『逃げずにやりきる』この姿勢が大切だと思っています」

後輩から頼りにされる背景には、自らが率先して行動するリーダーの姿があったようだ。

システム開発とセキュリティ、その両面に精通するゼネラリスト

2004 年、大野はデータベースセキュリティ研究所所長に就任する。この研究所はラックがセキュリティ事業の将来を見据えて取り組んだ新たな試みの 1 つ。組織の重要な情報資産は当時もデータベースに格納されていたが、データベース自体を守るための技術やサービスが確立されていなかった時代だ。研究所という名は冠しているが、基礎研究などは行わず、既存の技術を活かしたサービス作りに専心していたという。

データベースセキュリティというと、SQL インジェクションなど外部からのサイバー攻撃に対応する WAF（Web アプリケーション・ファイアウォール）などの製品を連想するが、当時はデータベース管理者が情報を窃取する内部犯行を想定し、設定や運用状態の診断サービスや、アクセスログの取得・不正アクセスの検知やブロックを行うデータベース・ファイアウォール製品の導入や運用支援サービスを行っていたそうだ。現在であれば大企業や国防関連で導入されているものだが、当時としては製品・サービスともに高価であり、一方で導入する組織側の意識が追い付いていなかったことから売り上げにはつながらず、今にして思えば時代が早すぎたと振り返る。

また、データベースセキュリティ研究所時代で、最も記憶に残っている事柄を聞いてみたところ、兼務していた緊急対応サービス「サイバー 119」のことを挙げた。

「サイバー 119」は、セキュリティインシデントが発生した顧客の元へラックのエキスパートが駆け付け、初動対応から復旧支援・恒久対策、さらにアフターフォローまでを行うサービスだ。

「実際、いくつもの現場に入りました。私自身は一流のセキュリティエンジニアではありませんから、ハッカーと同じようなことはできません。しかし、システムをゼロから構築した経験がありますから、インシデントの全体像が見えるので

大野祐一（45）：茨城県土浦市出身。日本大学生産工学部数理工学科卒業後、1994年ラックに入社。10年間にわたりシステム開発事業に従事し、2004年からデータベースセキュリティ研究所所長に就任。2009年からはセキュリティ事業の事業部長や海外子会社の取締役を経て、2014年からトヨタメディアサービス株式会社に出向し、セキュリティ強化の戦略立案、実行支援に邁進中。自他共に認める愛妻家。

す。ですから、ある事象が起きた時にどこを調べたらよいのかわかります。緊急対応ではお客様の元へ向かい、現場で応対するのが私の役割でした。医療の現場に例えるなら『主治医』のようなもので、患者と接してコミュニケーションを取りながら治療方針など全般に責任を持つ存在です。そして『執刀医』や『麻酔医』など他のスペシャリストと連携して対応を進めるのです」。こういった経験が大野のキャリアの糧になっている。「システムとセキュリティ、その両面に精通するゼネラリスト」、これが大野の強みだ。

顧客の役に立ちたいという真摯な想い

こういった経験を経て、大野は2014年からトヨタメディアサービスに出向することとなる。トヨタメディアサービスはトヨタ自動車の子会社で、トヨタ自動車の公式サイトの運用をはじめ、「テレマティクス」と呼ばれるカーナビやGPS、移動体通信システムを利用し、渋滞回避ルートの案内や緊急通報、さらには盗難車の追跡などを行うサービスを提供している。余談だが、2011年の東日本大震災の時に注目された「通れた道マップ」は、実際の自動車の通行実績データを元に、通行可能ルートを地図上に示すものだが、このサービスでもトヨタメディアサービスが保有していた情報がうまく活用されている。

近年では、ネットワークに常時接続する「コネクティッドカー」のセンター側システムの開発・運用も行っており、トヨタ自動車が企画したものをカタチにする役割を担っている。

トヨタメディアサービスにおいて、大野はチーフ・セキュリティ・ストラテジストとして活躍している。トヨタメディアサービスのセキュリティに加え、委託先やトヨタメディアサービスが運用に当たっているトヨタ自動車公式サイトのセキュリティなど幅広く関わっている。

「仮に、トヨタメディアサービスから情報漏えいなどの事故や事件が起これば、それはトヨタの問題へと発展してしまいますから、大役を任されていると思います」

このように語る大野は、現在トヨタメディアサービスのCSIRT（Computer Security Incident Response Team：シーサート）設置に向けて準備を進めているそうだ。そして、ここでもラックで培ってきた経験が役立っているのだという。

「出向する前はセキュリティ事業の副本部長を務めていました。ラックのセキュリティサービス事業の内容はすべて把握していますし、緊急対応の経験もあります。インシデント発生後の初動対応や、インシデントを未然に防ぐ策についても熟知しています。仮にこれらの知見がなかったとしたら、CSIRT設置の提案後はすべてコンサルタントに頼ることになっていたと思います」

ビッグピクチャー（大局）を把握しているからこそできる仕事であろう。大野の言葉を借りれば「自分の仕事は塗り絵の枠線を描くこと。あとはそれぞれのスペシャリストに色を塗ってもらえばよい」ということとなる。

大野自身は、CSIRTの設置まではトヨタメディアサービスでの仕事を続けたいと考えている。現在は名古屋に単身赴任中で、週末ごとに東京に戻り家族（妻・子2人）と過ごす生活を続けている。身体への負担やストレスはないかと質問したところ「確かに名古屋・東京間の移動は多少の負担はありますが、東京にいた頃は終電間際まで仕事をしていたこともあり、家族と過ごす時間はそれほど変わっていないのです。また、名古屋での通勤時間が10分ほどなのでその点は楽をしています。それに名古屋の食事も気に入っています」と快活に答えてくれた。

子供から仕事について尋ねられた時には「皆がコンピューターを安全に使えるようにする仕事」と答えているそうだが、仕事のモチベーションの源泉について聞いてみると「SIの業務ではお客様の業務効率化の役に立ちたいという想い、現在はトヨタ自動車やトヨタメディアサービスのセキュリティ対策に寄与したいという想いです」と答える。さらに今後帰任したときはラックのセキュリティ事業拡大に貢献したいと語ってくれた。

Cheer Up! ラックの対外活動

社会人と情報モラル

文＝ ICT 利用環境啓発支援室　客員研究員　七條麻衣子

情報モラル教育を取り巻く状況

昨今、子どもたちの間でネットトラブルが起きると「情報モラル教育の推進を」という声が聞かれます。では、この「情報モラル教育」とはどのようなものでしょうか。

文部科学省が定める現行の学習指導要領では「情報社会で適正な活動を行うための基になる考え方と態度」と定義されています。具体的には、他者への影響を考え、人権・知的財産権など自他の権利を尊重し、情報社会での行動に責任を持つことや、危険回避など情報を正しく安全に利用できること、コンピューターなどの情報機器の使用による健康とのかかわりを理解すること、とされています。これらの内容は**図 1** のように 5 つに分類され、小中学校ならびに高校のすべての教員が指導することとなっています。

しかし、現状ではカリキュラムの都合などにより、1 年に一度、専門家を招へいして講演会を実施するということにとどまっている学校も少なくありません。確かに、上記の内容を網羅するには教員も新しい知識を習得し続ける必要がありますし、子どもたちの発達段階に応じた丁寧な指導が求められるため、時間もかかります。保護者や IT・情報セキュリティの専門家、法律家の協力が不可欠であり、学校だけで対応するのは非常に難しいのです。

図 1　情報モラル教育における 5 つの領域

ネットトラブルに巻き込まれるのは子どもだけではない

筆者は 2009 年から 6 年間、大分県が開設したネットトラブル専門の相談窓口で、住民からの相談対応に従事していました。そこでわかったのは、子どもより大人の方が圧倒的にネットトラブルに巻き込まれている、といった実態でした。「子どもが被害に遭ったがどう対応してよいかわからない」という保護者の相談も非常に多いものでした。特に「無料だと思って動画サイトにアクセスしたが、いきなり料金を請求された」というワンクリック請求や、「ネット上に中傷を書き込まれた」という内容は毎日のように寄せられました。

今年 8 月に発表された、国民生活センターによる 2015 年度の消費生活相談の統計を見ても、相談件数の上位を占めるのは、上述のワンクリック請求などのインターネットに関するものとなっています（**表 1**）。

また、警察庁の統計によると、2015 年は約 13 万件のサイバー犯罪などに関する相談が寄せられています。最も多い内容は、ネット上の詐欺や悪質商法に関するものであり、迷惑メール、名誉棄損・誹謗中傷等に関するものと続きます（**図 2**）。

このように、非常に多くの人がネットトラブルに巻き込ま

2015年度		件数
全体		925,681
順位	商品・役務等	
1	アダルト情報サイト	95,364
2	デジタルコンテンツその他	78,035
3	インターネット接続回線	43,797
4	商品一般	42,810
5	賃貸アパート・マンション	33,625
6	フリーローン・サラ金	32,046
7	移動通信サービス	25,492
8	健康食品	21,878
9	相談その他	17,529
10	四輪自動車	13,477
11	他の役務サービス	13,366
12	放送サービス	12,930
13	修理サービス	11,544
14	出会い系サイト	11,098
15	新聞	10,907

表 1　国民生活センターに寄せられた「商品・役務」に関する相談上位 15 位
出典：「2015 年度の PIO-NET にみる消費生活相談の概要」
http://www.kokusen.go.jp/pdf/n-20160818_2.pdf

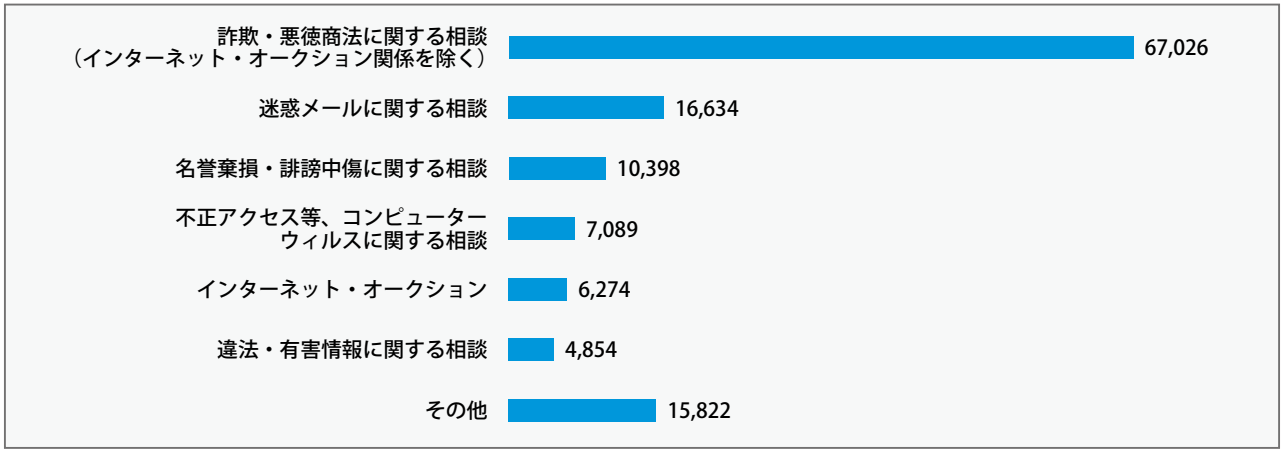

図 2　各都道府県警察における相談件数
出典：警察庁「平成 27 年におけるサイバー空間をめぐる脅威の情勢について」https://www.npa.go.jp/kanbou/cybersecurity/H27_jousei.pdf

れている現状があります。

「自分は被害に遭わない」という自信がある方も多いと思いますが、「ネットトラブル」を「情報にまつわるトラブル」と置き換えて考えてみます。

例えば、情報漏えい事故。残念ながら 2014 年の 1 年間だけで 1591 件の事故が発生し、約 5000 万人の情報が漏えいしています[1]。ただし、これはあくまで報道された件数であり、水面下では多くの事故が起きていることが想像されます。事故原因の多くは、管理ミスや誤操作、紛失など人的ミスによるものですが、その「うっかり」によって被害者が発生し、組織や個人は加害者になってしまいます。

また、善意の情報発信が逆効果になってしまうこともあります。筆者の住まいである大分県は、本年 4 月に大きな震災に見舞われました。Twitter や Facebook には、身内の安否確認や支援情報など、本当にさまざまな情報が拡散されていました。ただ、時間が経つにつれて誰かの投稿を「コピペ」して拡散しているものも増え、中には元の発信者が不明であったり、内容が誤っているものも相当数ありました。

【拡散希望】

一部の人にしか情報が行き渡っていない状態で、来る人が少ないのが現状です。
熊本の熊本港、八代港、三角港に巡視船が停泊し、給水、お風呂、おにぎり、携帯充電の用意をしております。
時間は朝 8 時から夜 8 時までです。

この投稿では拡散している方々に悪意はなく、少しでも誰かを助けたいという思いが感じられましたが、支援状況が変わっても同じ内容が拡散され続けたため、逆に住民を混乱させる結果となりました。「情報の真偽」「情報の鮮度」「情報の取捨選択」について考える訓練を、日頃から行っておく必要性を痛感した出来事です。

情報モラルは賢く安心して生きていくための知恵

私たちはこの情報社会において、さまざまなサービスを利用し、自分自身も容易に情報発信ができるようになりました。

自分は大丈夫と思っていても、無意識のうちに詐欺に遭ったり、誰かを傷つける行為をしたりしているかもしれません。私たちの周りには、DV やストーカー被害などにより、居場所を知られないように生活している方々もいます。その方々は「私は隠れています」と声にすることはありません。情報の取り扱いを誤ると、誰かの命に関わる事件につながる可能性もあります。

自分が利用しているサービスは本当に安全なのか、利用規約はどうなっているのかといった消費者としての視点、どうすれば情報を安全に管理できるのかといった安全への意識に加え、自分の投稿が他者を傷つけたり、情報漏えいにつながったりする可能性はないかという人権への配慮も必要です。つまり、『情報モラル』とは、私たちが「賢く安心して生きていくための知恵」です。これからの子どもたちに当然必要な教育ですが、私たち大人が、いま一度自分自身の生活を見つめ直し、子どもたちと共に考えていくことが急務ではないでしょうか。

[1] 日本ネットワークセキュリティ協会「2014 年 情報セキュリティインシデントに関する調査報告書」http://www.jnsa.org/result/incident/2014.html

若者がITで描く夢の実現を支援する すごうで2017

スゴウデ SUGOUDE IT Super Engineer Support Program Supported by LAC

支援対象者募集中2017年1月10日(火)まで

株式会社ラックは、IT に関する突出した技術力やアイデアを持った若者を支援する「IT スーパーエンジニア・サポートプログラム " すごうで "」について、2017 年度支援対象者を募集しています。

応募は 2017 年 1 月10日（火）（当日消印有効）まで受け付け、選考により最も優れた個人またはグループには、当社専門家による技術的な助言、活動費用の支援など、目標を実現するための各種支援を実施します。

2013 年度にスタートした " すごうで " は、IT を活用して実現させたい夢がある「エンジニアの卵」を発掘し、そのチャレンジを技術と資金の両面から支援することで、多様化・高度化する IT 社会において次世代を担う人材に成長してもらうことを狙いとしています。

これまでに、米ラスベガスで開かれた国際的な情報セキュリティ競技大会に挑戦する若者や、米国の教育現場での IT 利用状況や最先端の IT 企業の現状を学び、新しい金融のありかたを考えアプリケーションの制作を目指す若者を支援するなど、若い才能を飛躍させる取り組みを続けています。

" すごうで " で支援する「夢」は、IT に関するものであれば特に内容は問わず、ソフトウェア開発からハードウェア開発、イベント企画など、どんなものでも対象とします。支援対象者には、当社専門家による技術的サポート、活動費用の提供のほか、夢の実現に向けたあらゆる支援を行います。

若い皆さんの自由な発想で、当社審査員が思わずワクワクしてしまうような夢のご応募をお待ちしています。

すごうで2017の募集概要

■応募資格

1. 次のア又はイに該当すること

ア：IT に関する技術力や IT を活用したアイデアを有する 20 歳未満（誕生日が 1997 年 4 月 2 日以降）の方

イ：アに該当する方が過半数を占めるグループ

2. 保護者（グループの場合は、上記 (1) アに該当する方の保護者）の同意が得られること 等

■支援内容

応募の中からアイデア・発想が最も優れた 1 件を選定し、提出された活動計画に沿って、2017 年度中、目標を実現するための各種支援を行います。主な支援内容は次のとおりです。

- セキュリティの観点からの試作ソフトウェアの検証、プログラミングのアドバイスなどの当社専門家による技術的な助言
- ハードウェア、ソフトウェア、書籍などの購入費用の提供
- 国内外で行われる勉強会や競技会参加のための必要経費の提供
- プログラミング技術など IT のトレーニング、各種講習の受講費用の提供
- 目標の実現に協力できる人や企業・団体の紹介 等

活動費用の支援総額は上限100万円です。ただし、生活のための費用や、目標の実現のための活動に関連のない費用に関しては、支援対象とはなりません。

■ 応募方法

所定の応募申込書および活動計画書に必要事項を記入し、2017 年 1 月10日（火）（当日消印有効）までに、株式会社ラック すごうで事務局あてに郵送してください。応募要項等は下記 URL から特設サイトでご確認ください。

http://www.lac.co.jp/lp/sugoude2017.html

株式会社ラック
〒102-0093 東京都千代田区平河町 2-16-1 平河町森タワー
TEL : 03-6757-0113（営業） E-MAIL : sales@lac.co.jp　http://www.lac.co.jp/

株式会社ラック
サイバー・グリッド・ジャパン