CYBER GRID JOURNAL

サイバー・グリッド・ジャーナル

VOL.3

リアル！

特集

地方から発信する情報セキュリティ対策の現状と課題

LAC

CYBER GRID JOURNAL VOL.3

TABLE OF CONTENTS

巻頭言

『釜石の奇跡』に学ぶ情報セキュリティ・情報モラルの啓発

吉岡良平
サイバー・グリッド・ジャパン ICT利用環境啓発室 室長

「『釜石の奇跡』をご存じですか？」
「子どもの携帯電話利用に啓発・教育が必要だ」と熊本県内の学校でいち早く活動を開始され、2016年2月に惜しくも急逝された桑崎剛氏は、情報モラル講座の冒頭で必ずこの言葉を投げかけていました。2004年から8年にわたり津波からの避難訓練を積み重ねてきた岩手県釜石市内の小中学校では、東日本大震災の際、生存率99.8%という成果を上げました。その避難訓練では、「過去の経験から、大地震が起こったときにはこの地には大津波が来るので、家族のことすらも構わず、各自が一刻も早く高台に逃げて自分の身を守れ」、という考え方が徹底されていました。自らが住む地域の特性を十分に理解し、その特性に合った防災意識を地域にしっかりと根付かせていたことが実を結んだといえるでしょう。

サイバー・グリッド・ジャパンでは、インターネット利用者の情報セキュリティや情報モラルの向上を支援するため、全国各地で啓発活動を行っています。さまざまな地域で啓発を行い感じるのは、私が日頃生活している東京とは全く異なる生活環境や生活習慣があるということです。情報セキュリティや情報モラルの啓発は、情報という目に見えないものを扱う上での安全を訴えるものです。それだけに、日常にある分かりやすいものを例にとって説明することが多くなります。例えば「ログインパスワードは、玄関の鍵と同じ」「インターネットは公共の場所だから、公園や道路と同じように、ルールを守ろう」などという言い回しは常套句です。ところが地方には、玄関に鍵をかけない、道路には信号がほとんどない、など東京では常識だと思っていたことが通じない地域が少なからずあり、むしろその方が当たり前なのでは？　と考えてしまうことがしばしばあります。こうしたときに東京は特別な街なのだ、ということをしみじみ感じます。

2015年の国勢調査では、日本の人口は約1億2700万人。東京の人口は約1350万人で実に10.6%。さらに神奈川、千葉、埼玉を加えると日本の人口のおよそ4分の1が東京圏に暮らしています。東京には国会があり、国の行政機関があり、日本の主立った企業があり、多種多様な商品がある店で買い物ができ、活字や音楽にあふれた生活があります。しかし、その一方では政府により「地方創生」が提唱され、インターネットはそのけん引力として期待されています。インターネットは、距離や時間を超越したグローバルメディアとして普及し、ほとんどの年齢層がスマートフォンを持ち歩き、インターネットの利便性を享受するようになりました。インターネットを利用することで、情報だけでなく、これまで簡単には手に入らなかった商品を簡単に注文でき、早ければ翌日には商品が届くなど、地方にも大きな環境の変化が生じました。

確かに、インターネットによって地域差なくサービスを利用し、均一な情報や商品を入手できるようにはなりましたが、その足元には依然として、異なった生活習慣があることも忘れてはいけません。情報化社会が進む中で、インターネット環境の安心安全は、交通安全や防犯、防災と同じように希求されるものになりました。その実現に向けた政策や啓発は、インターネットがより生活に密着した基盤に成長したからこそ、大都市での利用だけでなく、地域の生活習慣や地域特性を考慮し、地域が主体となり、実践し続けるべきではないでしょうか。冒頭の桑崎氏の問いかけは、そんな思いを込めたものなのだと思います。

今回のサイバー・グリッド・ジャーナルでは、そんな日本の各地で情報セキュリティや情報モラルの向上に取り組む中で垣間見えてきた地方・地域の実情を取り上げ、今、何が地方・地域に必要かを考えてみたいと思います。

特集

リアル！ 地方から発信する情報セキュリティ対策の現状と課題

地方で活動するそれぞれの思い

川口: 今日は「リアル！ 地方から発信する情報セキュリティ対策の現状と課題」をテーマに、サイバー・グリッド・ジャパンのメンバーのうち東京以外に拠点を置いて活動をする3人に地方の現状とそれぞれの思いを語ってもらうため、座談会を企画しました。司会は、東京在住ながら月の半分は全国を飛び回っている私が担当します。

後藤: よろしくお願いします。

川口: あれ、七條さんがいない。今日の開催、アナウンスしていましたよね。もしかしてオンライン参加？

落合: 今、メッセージが届きました。溜池山王で道に迷っているみたいで少し遅れるそうです。

川口: 溜池山王？ まあ、永田町まで近いですから、何とかなりますかね。[i]

後藤: 「ためいけさんのう」だと「ためいき」出ちゃうね。

川口: え？ 後藤さん、それはダジャレ？[ii]

後藤: ははははは

落合: 後藤さん、今日もノリノリですね。

七條: 遅れてすみません!! 初めて降りた駅で盛大に迷いました。

川口: 慣れないと迷いますよね。でも、大丈夫です。後藤さんが場を温めてくれていました。さて、始めましょう。

川口: 全員そろったところで、改めてよろしくお願いします。前回のCYBER GRID JOURNAL Vol.2では、「経営課題としてのサイバーセキュリティ」というテーマで当社取締役３人による鼎談(ていだん)を実施しました。サイバーセキュリティが経営に及ぼす影響は年々大きくなっています。

経済産業省が2015年12月に「サイバーセキュリティ経営ガイドライン」を出すなど[iii]、経営者としてサイバーセキュリティへの積極的な関与が求められる時代になっています。一方、大企業や東京の企業とは環境が異なる地方や中小企業でも問題は起きており、セキュリティに関わる一人として見過ごせないことだと認識しています。そこで、今回のCYBER GRID JOURNAL Vol.3では、「地方と中小企業」をターゲットにセキュリティにまつわる話題について意見を交わします。まずは、それぞれの経歴や現在の活動内容について聞かせてください。

後藤: 私はもともと、愛知県にある自動車メーカーに定年まで勤めていました。在職中はIT部門に所属し、長年、社内のITインフラ整備を担当しました。「社員が働きやすいITインフラはどのように整備すればいいか」「安全にモバイルワークをしてもらうにはどうすればいいか」ということを考えてきました。セキュリティにはWindows95が登場した時代から関わっており、「必要なとき、必要な人に必要な情報を渡し、安心・安全に使ってもらう」ことを常に意識していました。

川口: ずいぶん昔からITとセキュリティに関わっているのですね。中でも「セキュリティ」は身近な問題だったのですね。

後藤: ネットワークやOA環境の整備などITインフラの構築を進める際は、情報管理に加えて、建物の入退室から物品持ち出しなどまで広くセキュリティのことを考える必要がありました。「情報を漏らさないこと（機密性）」だけでなく、「業務を滞りなく行うこと（可用性）」も非常に大事で、この点は昔から意識していました。もともと大きな組織でしたから、自前で持つインフラの規模も大きなものでした。しかし、サイバー攻撃のような外部からの攻撃や脅威に関するものは自社だけで何とかなるものでもなく、社会全体で連携して対応しなければ立ち向かえないという実感がありました。「東京のセキュリティの文化」と「地方のものづくりの文化」の懸け橋になれたらいいなという思いからラックに入社し、現在に至るまで活動しています。そして前職からは一般社団法人日本スマートフォンセキュリティ協会（JSSEC）の活動にも関わるようになりました。これはJSSECの西本逸郎事務局長（ラック取締役）から「スマホ利用者の目線を入れたいから」と誘われたことがきっかけです。

川口: そこでJSSECとつながりができたのですね。今でも頻繁にJSSECの会合や講演で飛び回っていますよね。

後藤: はい。定年後はもっと楽になるかと思ったのですが、あちこちに呼ばれちゃって。もっとテニスをしていたいんだけど(笑)。

落合: 私は生まれも育ちも新潟で、もともとIT系のエンジニアや営業として働いていました。その後、しばらく自分で会社を経営していたのですが、その時に新潟県内で毎年開催されているセキュリティイベント「情報セキュリティワークショップin越後湯沢」の事務局を請け負ったことでセキュリティに関係することになりました。昔は「ハイテク犯罪ワークショップ in 越後」という名称だったこのイベントも、かれこれ20年近く続いています。

川口: 20年も続いているのですか。「ハイテク犯罪」という言葉も懐かしいですね。それにしても東京ではなく新潟でセキュリティイベントが続いているのも珍しいですよね。

落合: 「ハイテク犯罪ワークショップ in

後藤悦夫

サイバー・グリッド・ジャパン サイバー・グリッド研究所 客員研究員／日本スマートフォンセキュリティ協会(JSSEC)[iv] 利用部会 部会長
2015年まで愛知県の自動車メーカーのIT部門にてインフラ系を担当。同社定年後の2015年にラック入社。愛知県を拠点に、趣味のテニスと仕事のワークライフバランスを実践中。

落合博幸

サイバー・グリッド・ジャパン ICT利用環境啓発支援室 リサーチャー／情報セキュリティワークショップin越後湯沢[v] 実行委員会 副委員長／新潟県サイバー脅威対策協議会 幹事
エンジニアや営業を経験した後に独立、起業。経営するIT企業でセキュリティイベントの事務局を請け負ったことがきっかけでセキュリティ業界へ。2016年ラック入社。新潟県を拠点にし、情報セキュリティ分野での産官学民の連携や情報モラルの啓発活動を行っている。

七條麻衣子

サイバー・グリッド・ジャパン ICT利用環境啓発支援室 客員研究員
IT初心者のサポート業務や大学での情報処理演習補助を経験。ネットトラブル全般の相談窓口業務を経て、消費生活相談員や警察官を対象とした研修を実施している。大分県を拠点にし、ITの一般利用者の底上げ活動のため、全国で情報モラル啓発の講演活動も行っている。

川口 洋（司会）

サイバー・グリッド・ジャパン サイバー・グリッド研究所 所長 兼 チーフエバンジェリスト
2002年ラック入社。ラックのセキュリティ監視センターJSOC（Japan Security Operation Center）や内閣官房内閣サイバーセキュリティセンターでの勤務を経験。現在は東京都を拠点にし、1年に40回以上、全国を飛び回り、講演活動を続けている。「Hardening Project」や「セキュリティ・キャンプ」など、ITシステム運用に関わる全ての人の能力向上のための活動も行っている。

i 関東圏以外の方のために補足すると、溜池山王駅と永田町駅は東京メトロ南北線で１駅。迷わず歩けば１５分程度の距離。

ii 座談会収録は終始、和やかに進んだ。

iii http://www.meti.go.jp/policy/netsecurity/mng_guide.html

iv https://www.jssec.org/

v http://anisec.jp/yuzawa/

越後」が立ち上がったのは、西川徹矢新潟県警本部長（当時）[vi]の号令によるところが大きいです。今でこそ全国各地でセキュリティのイベントが開催されていますが、そういうイベントはやはり東京に集中している傾向がありますよね。当時、サイバー空間の脅威について議論する場ができたことは新潟にとっても地方にとっても画期的なことだったと思います。

川口：あの日本三大温泉シンポジウム[vii]の一つがここで立ち上がったのですね。本誌が出る３月は、ちょうど愛媛県の「サイバーセキュリティシンポジウム道後2017」が開催された直後ですね。そういえば、毎年５月に和歌山県で開催される「サイバー犯罪に関する白浜シンポジウム」も西川さんが関係されているとか？

落合：そうですね。あちらも西川さんの号令により始まったと聞いています。こういう取り組みが地方で少しずつでも動いていることには意味があると思っています。大手企業や東京に本社がある企業の人にとっては当たり前のようなセキュリティの基礎知識も、地方ではまだまだ認知されていないことがたくさんあります。実は私も、事務局を始めた頃はセキュリティの「セ」の字も分からず冷や汗をかくこともありましたし、制作したワークショップの申し込み用ホームページを実行委員メンバーに見せたところ、すぐさま脆弱（ぜいじゃく）性を指摘されたこともありました。「そんなに簡単に脆弱性が見つかるんだ」と思ったものでしたが、今考えると恐ろしいホームページを作っていたなと思います。

川口：大きな問題になる前に身内に指摘されてよかったですね。ただ、地方の企業というとセキュリティは二の次になっているところも多いのでしょうね。

落合：二の次どころか頭にない人も少なくないですね。今では少しずつ意識されてきてはいますが、次々に登場するITやセキュリティ関連の用語に理解が追い付かないという悩みもあります。

後藤：地方だと家に鍵をかけずに暮らしている人も少なくありませんよね。そういうところにいきなりセキュリティの話題を持っていってもなかなか理解されません。

落合：そういう地方企業の感覚はよく分かります。会社を経営していた者としての実感では、地方の経済では普段の経営で精いっぱいです。その中で直接お金を生まないと思われているセキュリティの話題を持ち出してもなかなか聞いてもらえないのが現状です。地方では一社一社の体力が大都市圏の企業に比べて小さいこともあり、自社だけでの対応は限られたものになっています。私は現在、新潟県内の「サイバー空間の脅威に対する新潟県産学官民合同対策プロジェクト推進協議会」の運営のお手伝いをしています。県内の関係者が手を取り合ってセキュリティ対策を進めていければと思っています。

川口：東京に比べて活動の規模が小さくても、みんなで集まって何とかしようという取り組みが進められるというのは大事ですよね。

七條：私は社会人になりたての頃は、コンサートの企画運営をするような仕事をしていました。そのうちパソコンのサポート業務をしたり、大学の情報処理演習の助手をしたりするようになり、少しずつIT業界に足を踏み入れました。その後、大分県の事業として開設されたネットトラブルの相談窓口で、6年ほど相談員として従事しました。この相談窓口は当初、大分県民専用を想定していたのですが、全国的な法律相談機関と連携したこともあり、全国から相談の電話が多数入るようになってしまったのです。

川口：え？　もともと大分県を想定して窓口を作っていたのに全国区ですか？　めちゃくちゃ電話がかかってきたのではないですか？

七條：窓口は２人しかいないのに、多い年で年間1300件ほどの相談がありました。でも、大変な数の相談をこなしていくうちにだんだんと知識も付いてきました。問題発生のパターンが見えてきたこともあり、ネットを介したトラブルや被害がなくなるように啓発活動を続けています。具体的には子どもたちに対する講習や教育関係者、消費生活相談員や警察官に対する講習などで、幅広い層を対象に行っています。多くの場所で相談を受けていると「あの話題に関するものが気になってついクリックした」「続きが気になって入力してしまった」など、個人の自然な欲求に付け込む犯罪が多くある

vi　ラックの社外取締役でもある。

vii　和歌山県の白浜、新潟県の越後湯沢、愛媛県の道後と、温泉地で開催されるセキュリティシンポジウム。全国のセキュリティ関係者が集い、朝から晩まで熱い議論を交わす場として有名。

ことに気付きます。私のテーマは「セキュリティは欲望に勝てるか？」です。ネットトラブルの多くは、性欲や金銭に関係するところで起きています。何とかして欲望に勝てるような仕組みを作らなければ、被害を減らすことができないのではないかと思っています。そんな思いを胸に、一般利用者に対する啓発活動を行っています。

川口：セキュリティと欲望！　すごい名言が飛び出しましたね。それは深淵（しんえん）なるテーマですね。

東京と地方のギャップ

川口：この対談で「ITとセキュリティに関する東京と地方のギャップ」に焦点を当てた対策が考えられたらと考えていますが、どんなところで東京と地方のギャップを感じますか？

後藤：まず文化が違います。愛知県は自動車や飛行機に代表されるような企業が多くあり、ものづくりが盛んな地域です。前の会社では「○○のDNA」という言葉がよく使われており、その中に「ものづくりのDNA」というものもあります。この「ものづくりのDNA」には「創意と工夫」があり、他と違うものを創り出すことへの喜びみたいなものがあるような気がします。システム開発の際も市販の製品をそのまま使うのではなく、より便利でより使いやすいものを求めてカスタマイズする要求が強く出されます。セキュリティ対策でも同様で、自社に合う形でカスタマイズして使いたいという要求が出てきますが、それを運用できる人材を社内で確保できるケースはまれです。そうなると社外の人材に期待するところですが、これもまた難しいのが現状です。そもそも地方では転職による中途入社が少ない上に、景気によって新卒採用の人数が左右されるものですから、世代によっては極端に社員が少ないということがあります。年齢的に、層の薄い年代の人が中心となって活躍しなければならない時期を迎えており、彼らが企業の主力部門に重点配属されるため、セキュリティ人材の確保面でも苦労されていると思います。

落合：そして地方ならではですが、東京と比べて転職率が低く、人材の流動性が低いことが影響しています。外部から調達しようにも転職市場がないし、セキュリティ企業は東京に集中している。泣き言も言っていられないので、地元の企業それぞれが何とか奮闘しているというのが現状です。

七條：人が県外に出て行った後、なかなか戻ってこないことも問題です。大分県の場合、そもそも正社員の雇用がそれほど多くないことも、自社での対策が進まない理由の一つです。IT系人材の場合、会社を辞めた後そのままフリーランスになるケースも見聞きします。

川口：IT系やセキュリティ系の企業・団体はほぼ東京に集中しているため、上京したらなかなか戻ってこないというのはありますね。最近では「ITを学んだ地元の学生はほとんど県外に就職する。帰ってくるときは（給与などの理由から）IT以外の会社に就職したがる」という話も聞きました。さて、システム開発を海外の会社に委託する「オフショア開発」の類義語として、地理的に近い場所の会社に委託して開発する「ニアショア開発」という言葉もありますが、ニアショア開発の案件が増えているなどの傾向はどうでしょうか。

落合：新潟からだと東京まで2時間程度で行けるため、ニアショアというよりも必要があればその都度東京に行けばいいという感覚です。ただ、現在はセキュリティ上の理由で情報の持ち出しが制限されるケースも多く、東京の案件を新潟で担うというのは昔に比べて難しい場合が多くなっています。

後藤：自社のシステムを地元以外の企業に開発してもらう際には「ニワショワ」か「VDI[viii]」がセキュリティ面で有効だと思います。

川口：デスクトップを仮想化して遠隔から接続するVDIは分かりますが、「ニワショワ」とは何ですか？　もしかして……。

後藤：会社の近くに来てもらって「庭先」で作るから「庭（ニワ）ショワ」（笑）。

川口：そこもダジャレですか！

後藤：VDIもいいのですが、規模が大きく

viii　Virtual Desktop Infrastructure の略。デスクトップ環境を仮想化して用意し、ユーザーはリモートから接続して作業を行う。ファイルやシステムを転送するのではなく、デスクトップの画像情報を転送するため情報保護が行いやすい。当然、スクリーンショットやカメラ撮影などには無力である。

なるとサーバーやライセンスの費用が大きくなるのが難点でした。システム開発の規模が大きくなると、自社の近くのオフィスを借りてそこで外部のチームを集めて開発してもらった方が費用も安く済むんです。近くで開発してもらうから「庭」と私は呼んでいました。

川口: たくさんの人に働いてもらう環境があって、それを庭と言える規模の土地があるのもすごいですよね。情報システムという観点だと東京と地方での違いはどうでしょうか。

落合: 社内からインターネットへの通信を制御、記録するプロキシサーバーが設置されていない組織や、社内のWindowsシステムを統合管理するための仕組みであるActive Directoryが導入されておらず、個別に端末を管理している組織もまだまだ多くあります。標的型攻撃の対策で挙げられるような基本的な仕組みがそもそも導入されていないという現実はあります。また、予算はあってもどこから手を付けていいのか分からないという組織も多いようです。一方で、公共機関や病院は比較的セキュリティレベルが高いところが多いように感じます。

川口: 地方に行くと「サーバーはデータセンターに入れませんか！」という営業トークをまだよく耳にします。東京では「地震対策」や「集中管理によるコスト削減」などの理由でデータセンターにサーバーを配置するのは一般的になっていると思われるのですが、地方ではまだそんな状況なのかと驚くことがあります。データセンターにすら入っていないシステムにセキュリティ対策をと言っても、実施できないだろうなと思って。

落合: 公共系やインフラ系のシステムはデータセンターに入っていることが多いのですが、それ以外の企業のシステムはまだまだ自社内に配置されている事例も多く見かけます。昔、あるメーカーが業務システムとしてパソコンとファイル

サーバーと業務アプリケーションをセットで売っていたような時代がありましたが、そのまま業務システムのセットがオフィスにあることが当たり前のようになっている企業もあります。管理や運用の費用を考えるとクラウドサービスを使うという手もありなのですが、そこに移行するための費用がなく、技術者もいないというのがさらなる悩みです。

川口: 公共系のシステムといえば、マイナンバー制度の運用が始まり、セキュリティ対策に関するニーズが強くなっています。そこで自治体のインターネット接続ポイントを集約し、高度なセキュリティ監視を行う「自治体の情報セキュリティクラウド」の構築が推進されていますが、このシステムを担う人材の不足も懸念されるわけですね。

七條: 成功している他の自治体の事例を参考にしたいという声を聞きますが、そういうところは大きい都市であったり、たまたまセキュリティの素養のある人が担当であったりするなど、成功する理由があるようです。そのため、それ以外の自治体にとっては必ずしも参考とはならないようで、対応に苦労しているという話を耳にします。

後藤: 中小企業といっても、人様から預かった情報資産はきちんと管理しなければなりません。取引先が大企業であれば情報セキュリティに関する確認があることもあり、無関心ではいられないでしょう。ただ地方にはITやセキュリティの技術者が少ないため、技術者からボトムアップを期待することは難しいですね。こういう問題は社長からトップダウンで実行させるようにしないと進まないと思います。中小企業向けにセミナーを開催する場合には、「セキュリティセミナー」とするより「経営課題」と絡めて企画しないと集客も難しいのが現状です。

落合: 大企業と取引がある企業では、発注元である大企業からの要望もあり、セキュリティ意識が高いところも多いのですが、大企業と取引がない地方の中小企業はセキュリティに関して意識していないところも多いと感じます。「保護すべき情報が自社にはない」と思っているケースも多いのですが、例えばネットショップを運営している企業などは想像以上に情報資産が蓄積されているため、セキュリティに関する意識を高めてほしいと願います。

七條: 現実には人手が足りないし、社員が3人とか5人だったりするとセキュリティ担当どころかIT担当者すらいないのが現状です。ただ、そういう組織だと顔を合わせて意識統一をすればいいので、明文化されたセキュリティポリシーがなくても困らないかもしれません。企業のサイズに合わせて対策を進めるという意識があるだけで、かなり違うと思います。

川口: ランサムウエア[ix]の被害はどうでしょうか。ある調査によると「自社は被害に遭わないと思う」という回答が4割近いですし、被害者の6割が身代金を払った経験があるようです[x]。ランサムウエアにパソコンの中身が暗号化されてしまうと業務ができなくて大きな問題になると思うのですが。

落合: 私の周りではあまり被害に遭ったという話は聞かないのですが、たまたまかもしれません。ウイルス対策ソフトを入れているから大丈夫という程度の認識

ではないでしょうか。10年前、20年前と比べてウイルス対策ソフトも一般的になり、性能も向上してきたので、それで救われている部分はあると思います。

七條: 私もあまりウイルス感染の相談は受けていません。むしろ、「ウイルスって本当にあるの？」といまだに質問されることがあります。どちらかというと標的型攻撃や情報漏えいに関して話をしてほしいという依頼の方が多いです。特に情報漏えいなどは、記者会見が行われた様子を見て、経営者が謝罪することになるというイメージもあり、危機意識を持っている方もいます。全国の消費生活センターにおける相談では、ワンクリック請求[xi]の被害が最も多いようです。スマートフォンが若年層から高齢者まで幅広い年齢層に普及したことで、URLを注意して見たり、定期的にウイルスチェックをしたりするといった機会が減り、結果としてインターネット上の詐欺行為に対する知識や免疫のない人が増えています。ワンクリック請求の請求画面が出ても「５万円程度で面倒なことを避けられるなら」という思考が働き、払ってしまう人もいるようです。

川口: インターネットの世界に浸って長い私たちは、さまざまなパターンの詐欺を見てきているためつい軽視してしまいがちですが、もっと身近なところのセキュリティの話題も発信していかないといけないですね。

七條: 組織には毎年新しい人が入ってきます。そういう人には基本的な「情報モラル」を身に付けてもらい、組織のセキュリティレベルの向上を目指してほしいと思います。ぜひとも「自分事で取り組む情報モラル」ということでお願いしたいです！

各地方における セキュリティに関する取り組み

川口: これまで東京と地方のギャップについて幅広く話し合ってきました。課題は山積みになっているとはいえ、以前に比べればそれぞれの地域でさまざまな取り組みが進んでいるのではないでしょうか。

落合: 新潟では産官学民が連携した「サイバー空間の脅威に対する新潟県産学官民合同対策プロジェクト推進協議会」という取り組みを行っています。

川口: その「産官学民」というキーワードが気になりました。よく聞くのは「産官学」の三つの主体だと思いますが、「民」まで入れて四つの主体があるのですね。ここでいう「民」は何になるのでしょうか。

落合: 「民」はNPOなどの民間団体を示しています。公益社団法人や一般社団法人なども一緒になって活動しています。民間企業や行政機関、教育研究機関だけではケアし切れない範囲に情報を届けるために「民」としての団体にも協力をしてもらっています。

川口: 沖縄にも「沖縄サイバーセキュリティネットワーク」[xii]というのがありますね。内閣府沖縄総合事務局と総務省沖縄総合通信事務所、沖縄県警察本部が事務局になっていて、沖縄管内のサイバーセキュリティの維持、向上のためにさまざまな活動をしているようです。土地柄から、何か起きたときに隣の県に助けてもらうということが難しいため、沖縄管内で何とかしなければという意識の表れなのかもしれません。セキュリティ・ミニキャンプ[xiii]やHardening Project[xiv]のようなセキュリティ人材の育成プロジェクトとも連携して活動しているようです。

七條: その他の活動では、各都道府県警の「サイバーテロ対策協議会」が軸になって各地域の重要インフラのセキュ

リティ対策のケアが行われています。重要インフラに該当する企業のセキュリティに関しては、所管官庁だけでなく各地域の警察も注視しています。まだ大きな予算が付けられないかもしれませんが、行政がこういう取り組みを地道に続けてくれることが大事だと思っています。本来は民間企業の自助努力に期待するところですが、セキュリティに対する理解と余力がない地方では、行政が仕切った方

ix コンピューターウイルスの一種。感染したパソコンのファイルを暗号化し、ファイルを復元するための身代金を要求する。身代金を払ってもファイルが復元される保証はない。
x http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20160727064652.html

xi ウェブサイトのURLを「ワンクリック」することで、サービス使用料金や契約料金という名目で金銭を要求する画面を表示し、金銭を窃取する詐欺行為。
xii http://ogb.go.jp/keisan/2406/13243/index.html
xiii http://www.security-camp.org/minicamp/okinawa2016.html
xiv http://wasforum.jp/

がうまくいくように思います。

後藤: その「サイバーテロ対策協議会」というのは全国でやってるの？　愛知県内でもやっていたような気がするなあ。

七條: 全国の都道府県単位で設置されているようです。名前は少しずつ違うようですが、警察が年に数回、会合を開き、各地の重要インフラ企業を対象にセミナーやインシデント対応訓練などを行っています。私は大分県警などで毎年話をさせていただいていますが、川口さんは各地の警察でお話されていますよね。

川口: はい。全国から呼んでいただいて講演させてもらっています。ラックの受付には各地から頂いたマスコットキャラクターを並べていて、いつか全国制覇するのが目標です。

ラックの受付に並んだ各都道府県警のマスコットキャラクター

地方企業や中小企業がやるべきこと

川口: 地方企業や中小企業の限られたリソースの中で、「これだけはやってほしい」「これだけは気を付けてほしい」ということがあれば教えてください。

後藤: 人から預かったものをきっちり守ることは社会的責任と意識して、しっかり対策してもらいたいですね。リソースが少ないからといって、顧客情報を危険な状態で保管することが許されるはずはありません。ITやインターネット空間を使用する人の責任として、認識しておいてもらいたいと思います。

落合: 2016年11月に独立行政法人 情報処理推進機構（IPA）から公表された「中小企業の情報セキュリティ対策ガイドライン[xv]」を読み、対策をしっかり考えてもらいたいと思います。このガイドラインはもともと2009年に発行されたもので、昨年末に出されたものはその改訂版です。これがよくできていますので、ぜひとも読んでもらいたいですね。特に「情報セキュリティ５か条」として、まず手を付けてほしい五つのことが記載されています。

① OSやソフトウェアは常に最新の状態にしよう！
② ウイルス対策ソフトを導入しよう！
③ パスワードを強化しよう！
④ 共有設定を見直そう！
⑤ 脅威や攻撃の手口を知ろう！

いずれもさほどお金をかけずにすぐにできることばかりですね。特に個人事業主の場合は、最初の三つだけでも意識してもらえるといいのではないかと思っています。毎日のようにセキュリティに関する事件が話題になりますが、調査をしてみるとこれら五つの対策がきちんと実施されていないことが原因であったということがよくあります。

川口: 正直なところ、個人レベルでWindowsパソコンを使う人の場合はWindows10にアップデートしてパスワードを推測されにくいものにするだけで十分ではないかと思います。これだけの対策を心掛けるだけでウイルス感染やサイバー攻撃の被害に遭う確率を大幅に下げられると思います。

七條: お金をかけずにできるセキュリティ対策があるので、そこから実践していただきたいと思います。特に「情報資産の棚卸し」は重要です。「自社に重要な情報はない」と思っていても、以下のような情報を保持していることはあるでしょう。

- ○ 従業員の個人情報（マイナンバーを含む）
- ○ 顧客から預かった情報（マイナンバーを含む）
- ○ 取引に関する情報
- ○ 新商品や既存商品の設計図
- ○ 工場や製造ライン、制御ラインの操業に関する情報

特に最近ではマイナンバーの取り扱い業務が増えており、ほぼ全ての企業に関係する話です。それぞれの組織で、保有している情報資産の棚卸しを実施してほしいですね。

後藤: 従業員の教育も大事ですね。ある調査によると、重視するセキュリティ対策として「従業員のセキュリティ教育」と回答する企業が多くなっています[xvi]。人材の流動性が低い地方だからこそ、教育をした従業員が長く勤めてくれれば、企業としてその教育効果を長期間享受することができます。システム的な対策が費用面で難しい企業にとっては、経営層自らが従業員教育を担当することが最も効果が大きいと思います。

七條: 私も従業員教育は非常に重要だと思います。先ほども説明しましたが、前から勤めていて教育もなされている従業員と、毎年新たに組織に入ってくる人との間には、「情報の取り扱い」に関してギャップがあります。個人間や世代間のギャップをなくし、意識を共有するためにも、従業員教育、情報モラルの教育は実施すべきだと思います。

参考になるホームページや書籍

川口: 最後に、セキュリティ対策を実施する上で参考になるホームページや書籍があれば教えてください。

後藤: JSSECの利用部会 部会長としては「スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン」[xvii]を参考に、安全にスマートフォンやタブレットを使っていただきたいですね。このガイドラインでは、企業が従業員に貸与する端末や従業員の私物を業務で利用する場合に考慮するべきポイントを取り上げています。「メールを利用する」「スケジュールを利用する」など、スマートフォンやタブレットが登場する具体的なシーンを想定し、そこに潜む脅威や対策方法を解説しています。

川口: このセキュリティガイドラインは企業内のシステム担当者にぜひ読んでほしいですね。特にリモートワークを推進している企業の方も多いと思うので、このガイドラインを読んで進めてもらいたいですね。

後藤: ぜひ！　モバイルワーク、リモートワークにスマートフォンやタブレットの活用は欠かせませんからね。付録には、チェックシートや誓約書への記載項目の例などもありますので、参考になることが多いと思っています。

落合: 私はサイバー・グリッド・ジャパンのメンバーが書いた「漫画で学ぶ サイバー犯罪から身を守る30の知恵」[xviii]を推します。身近なサイバー犯罪の事件・事故を取り上げ、漫画で分かりやすく解説しています。「難しいことは分からない」と思う人にも気軽に読んでもらえると思います。

川口: 漫画といえば、IPAが出している「サイバーセキュリティのひみつ」[xix]もいいですよね。対象は小学4年生～6年生となっていますが、大人が読む入門書としてもいいと思います。

七條: 私はIPAの「対策のしおりシリーズ」[xx]をお薦めします。「ウイルス対策のしおり」「不正アクセス対策のしおり」「初めての情報セキュリティ対策のしおり」など話題になることが多いテーマを、しおりという形にしたPDFが公開されています。これがよくまとまっていて、とても参考になります。

川口: 展示会やセミナーで配っている小冊子ですね。IPAのホームページには啓発に使えるコンテンツがたくさんありますので、「お金をかけられない」という人こそ、IPAが出しているコンテンツを活用してもらいたいですね。

七條: 特に「情報漏えい対策のしおり（第7版）」[xxi]と「情報漏えい発生時の対応ポイント集」[xxii]を読んでいただきたいです。情報漏えい事故を起こさないための七つのポイントや、万が一、事故が起きてしまった場合の対応方法を紹介しています。

①企業（組織）の情報資産を、許可なく、持ち出さない
②企業（組織）の情報資産を、未対策のまま目の届かない所に放置しない
③企業（組織）の情報資産を、未対策のまま廃棄しない
④私物（私用）の機器類（パソコンや電子媒体）やプログラム等のデータを、許可なく、企業（組織）に持ち込まない
⑤個人に割り当てられた権限を、許可なく、他の人に貸与または譲渡しない
⑥業務上知り得た情報を、許可なく、公言しない
⑦情報漏えいを起こしたら、自分で判断せずに、まず報告

川口: これらは新しい技術やサービスが登場した場合にも応用できることですので、基礎知識として身に付けておきたいですね。本日は、地方に根差して活動するメンバーならではの深い話がたくさん聞けました。ありがとうございました。

xv https://www.ipa.go.jp/security/keihatsu/sme/guideline/
xvi https://www.nri-secure.co.jp/security/report/2015/analysis.html
xvii https://www.jssec.org/report/20140417.html
xviii https://www.amazon.co.jp/dp/4890633332
xix https://www.ipa.go.jp/security/keihatsu/security-himitsu/
xx https://www.ipa.go.jp/security/antivirus/shiori.html
xxi https://www.ipa.go.jp/security/antivirus/documents/05_roei.pdf
xxii https://www.ipa.go.jp/security/awareness/johorouei/index.html

フツーの企業が気にするべき たった1つのこと

とにかくネットバンキングの不正送金対策!!

普通の企業がITを利活用して事業を推進するために気にするべきことは何でしょうか？

私はいつも「とにかくネットバンキングの不正送金対策!!」と言っています。巧妙に作られたコンピューターウイルスや偽物のネットバンキングの画面から不正に入手したIDとパスワードを使用して、ネットバンキングの口座から不正に送金を行う事件について一度は耳にしたことがあるのではないでしょうか。私が警鐘を鳴らすのは以下の二つの理由からです。

① お金がなくなれば事業が継続できない
② 法人口座は個人口座と違い、被害が補償される保証はない

一つ目の理由はどなたにでも理解していただけるでしょう。会社の口座からお金が無くなってしまえば、事業を続けることができません。極端な話、どんなにウイルスに感染しても、ホームページが改ざんされたとしても、お金があれば立て直すことも、新たな対策を行うこともできます。しかし、お金が無くなってしまえば、IT投資やセキュリティ対策はおろか従業員の給料を払うこともできず、事業運営は止まります。「情報セキュリティはもうからないから」と思う人がいるのは仕方がないことですが、事業資金を守るためにやるべきことがあるという理解は絶対に必要です。特にここ数年は法人口座を狙った不正送金事件の被害が増加しており、法人口座の残高は個人口座より多いこともあって1件当たりの被害金額も大きくなっています。犯罪者も、対策をしていない企業があることを分かった上で法人口座に狙いを定めているのでしょう。

二つ目の理由も非常に重要です。実は個人口座は不正送金の被害に遭っても100%近い割合で補償[1]されています。法人口座の場合は統計データは公開されていないため、正確なところは不明ですが、個人よりも口座残高の大きい法人口座の被害をすべて補償するのは難しいのではないかと推測します。現在は被害が増加していることもあり、全く救済（補償）されないということはないと思いますが、いずれにしても一時的に事業資金が不足することは間違いありません。事業運営を続けるためにも、ネットバンキングの不正送金の被害にだけは遭わないように気を付けていただきたいと切に願います。

インターネット・バンキングによる預金等の不正払戻しにかかる補償件数等について【個人顧客】

時 期	対応方針決定済件数 1	うち補償件数 2	補償率 2 ÷ 1
平成26年度	**1,048**	**988**	**94.3%**
平成26年 4月～ 6月	*422*	*389*	*92.2%*
平成26年 7月～ 9月	*256*	*248*	*96.9%*
平成26年10月～12月	*200*	*192*	*96.0%*
平成27年 1月～ 3月	*170*	*159*	*93.5%*
平成27年度	**1,091**	**1,073**	**98.4%**
平成27年 4月～ 6月	*277*	*267*	*96.4%*
平成27年 7月～ 9月	*253*	*249*	*98.4%*
平成27年10月～12月	*160*	*160*	*100.0%*
平成28年 1月～ 3月	*401*	*397*	*99.0%*
平成28年度	**149**	**146**	**98.0%**
平成28年 4月～ 6月	***149***	***146***	***98.0%***
平成28年 7月～ 9月			
平成28年10月～12月			
平成29年 1月～ 3月			

全国銀行協会の統計データ

1 全国銀行協会 「インターネット・バンキングによる預金等の不正払戻し」等に関するアンケート結果
http://www.zenginkyo.or.jp/fileadmin/res/news/news280831_2.pdf

川口 洋

サイバー・グリッド・ジャパン
サイバー・グリッド研究所
所長 兼 チーフエバンジェリスト

具体的にどうするか？

ネットバンキングの不正送金の被害に遭わないためには、「取引銀行の注意をよく読む」ことが重要です。どこの銀行でもインターネットバンキングを紹介するホームページには「不正送金対策」や「セキュリティ対策」に関する注意書きが掲載されているはずです。各銀行が推奨する対策を実施しておくことは必須です。理由は「不正送金被害に遭わないため」と「不正送金被害に遭ったときに補償してもらえる確率を上げるため」です。それぞれの銀行が推奨する対策に共通するポイントは以下の３点です。

① パスワードや暗証番号はしっかり管理する
② OSやソフトウエアは最新版にアップデートして使用する
③ ウイルス対策ソフトを最新版にして使用する

いずれの対策も、特集の座談会で紹介した独立行政法人情報処理推進機構（IPA）の「中小企業の情報セキュリティ対策ガイドライン」の「情報セキュリティ５か条」に含まれているものです。このガイドラインを見ておくことが事業資金を直接守ることにつながります。ぜひともこれらの対策についてガイドラインを参照してください。

そして、ネットバンキングならではの対策もあります。これらの対策は個人には必ずしも勧められるものではありませんが、法人は重要な事業資金を守るためにも実施しておきたい対策です。

④ 銀行が提供する専用のセキュリティ対策ソフトの導入
⑤ ワンタイムパスワードや乱数表の使用
⑥ 電子証明書の適切な利用

④の専用のセキュリティ対策ソフトはネットバンキングの不正送金を行うウイルスに特化したもので、多くが無料で提供されています。無料で利用できるものはありがたく有効活用しましょう。また、このセキュリティ対策ソフトは銀行によっては「ウイルス対策ソフト」として紹介されている場合がありますが、通常使用しているウイルス対策ソフトと併用が可能です。ネットバンキングを使用するパソコンでは、一般のウイルス対策ソフトとこの専用のセキュリティ対策ソフトを両方インストールしておきましょう。

すでに⑤のワンタイムパスワードや乱数表を利用している方はいるかもしれません。ネットバンキングのログインや送金時に使用します。頭の中で記憶しておくだけのIDとパスワードと違い、「パスワードになる何か」を「トークン（ワンタイムパスワードを提示する機械）」や「カード」の形で持ち歩く必要があります。持ち歩くのが面倒という理由で使用されないケースもありますが、ネットバンキングを利用する以上は併用するべきです。

最後の⑥の電子証明書は、なじみがない方が多いかもしれません。法人口座の契約ユーザーに提供された電子証明書をパソコンにインストールすることで正当なアクセス権を持つパソコンとして扱われます。たとえ犯罪者がIDとパスワードを盗んだとしても、電子証明書がない限りは口座にアクセスすることができません。ここで注意が必要なのは「適切な利用」という点です。電子証明書による認証は銀行が推奨する手順で扱わなければ、コンピューターウイルス等を経由して犯罪者に電子証明書自体を盗まれてしまいます。電子証明書の発行とともに案内される手順をよく参照して実行してください。

体力のない中小企業は大手企業のような対策は実施できないかもしれません。しかし、大手企業のような体力がないからこそ、貴重な事業資金を守るためにネットバンキングの対策だけは真剣に考えてもらいたいと思っています。これらの対策は慣れてしまえば苦もなくできますが、それでも難しくてできない場合は、ネットバンキングの機能を使用しないか、振込限度額を大幅に引き下げるなどの対策を実施するべきです。

ネットバンキングの不正送金を狙う犯罪者の目的はお金です。セキュリティ対策を行わない企業があると分かった上で、あの手この手を駆使して口座にあるお金を狙ってきます。しかし、お金が目的である以上、犯罪行為で得られる金額以上のコストをかけてまでは実行しません。幾つかの対策を導入することで犯罪にかかるコストを引き上げ、犯罪者のターゲットにならないようにすることも重要です。いつか犯罪者が「ネットバンキング口座を狙うのは割に合わない」と思うような日が来ることを願って、これからも私は全国で情報発信を続けます。

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3回

家庭菜園から考えるセキュリティ投資

谷口隼祐　サイバー・グリッド・ジャパン
サイバー・グリッド研究所　チーフリサーチャー

標的型攻撃、不正アクセス、情報漏えい……。
これらの言葉を誰でも一度は耳にしたことがあると思います。
それでもなお「セキュリティ対策は必要なのか？」
「不必要に対策をあおっているだけではないか？」と思っている方向けに、
必要最低限のセキュリティ投資の考え方について、
家庭菜園を例にお話しします。

家庭菜園とセキュリティの関係性

私は一時期、自宅でイチゴを育てていました。最初は数株だったイチゴの苗も順調に増え、1シーズンで50個以上、収穫できるようになりました。次のシーズンもおいしいイチゴをと期待していたのですが、ここで事件が起こりました。何者かにイチゴを食べられてしまったのです。結論から言うと、“犯人”は鳥とナメクジでした。鳥についてはすぐに見当が付いたので鳥よけネットで対策をしましたが、ナメクジについてはなかなか気付けずに、大事なイチゴを幾つも食べられてしまいました。食べ跡やプランター周りの痕跡を調べてようやく別の“犯人”の正体を突き止め、ナメクジ退治用の薬をプランターの周りにまいたところ、被害を減らすことができました。

さて、ここまではセキュリティと一切関係のない話のように思われるでしょうが、実はこの中に必要最低限行うべきセキュリティ投資のヒントが隠れています。

- 守るべき対象をはっきりさせる（今回はイチゴの実）
- 脅威や攻撃の手口を知らなければ有効な対策ができない
- 本格的に対策すると、それなりにお金がかかる

当たり前のことばかりですが、いずれも非常に重要なポイントです。
情報セキュリティにおいては、その「当たり前のこと」ができていない企業が少なからずあります。なぜでしょうか？　原因の一つは、インターネットに代表されるサイバー空間の特徴が十分に理解されていないからだと思われます。

サイバー空間の特徴

現実の空間に対して、サイバー空間の特徴は「その中でのやりとりが見えにくい」「物理的な距離の制約がない」という点にあります。こうした特徴ゆえに、そもそも攻撃されていることに気付かなかったり、自社は攻撃されないと思い込んだりしがちです。イチゴは食べられればなくなりますが、情報は盗まれても（コピーされても）なくなりません。また、現実世界で「ご近所さん」というと物理的に住まいが近い、限られた人を指しますが、サイバー空間におけるご近所さんは全世界の人や組織です。ご近所さんとの関係が良好ならば攻撃される可能性は小さいかもしれませんが、全世界のご近所さんと良好な関係を築き、攻撃されない状況を作り出すことは可能でしょうか？
さらに厄介なことに、皆さんの所属する企業がサイバー攻撃の対象として狙われたとしても、攻撃者の本当のターゲットは別の企業であることもあります。攻撃者は皆さんの企業のパソコンやサーバーを勝手に使い、全く別の人や企業、場合によっては取引先に対して悪事を働く可能性があります。最近では、ルーターやネットワークカメラなどのIoT機器や情報家電と呼ばれる機器が悪用される事例も相次いでいます。

基本的な対策のススメ

いわゆるサイバー攻撃は、セキュリティの弱い組織を片っ端から攻撃するタイプと、特定の組織に狙いを定めて攻撃し続けるタイプに大別できますが、前者はソフトウエアを更新したりパスワードを推測が難しいものに変更したりといった基本的な対策で防げる場合がほとんどです。手っ取り早くセキュリティを向上させる手段の一つに、対策そのものを外部に委託する方法がありますが、委託する範囲が広ければ広いほど費用がかかります。そのため、まずは自分たちでできる基本的な対策を実施することをお勧めします。何から手を付ければよいか分からない場合は、特集でも紹介している独立行政法人 情報処理推進機構（IPA）の「中小企業の情報セキュリティ対策ガイドライン」を参考にするとよいでしょう。ガイドラインではセキュリティ対策の充実したクラウドサービスへの移行にも触れています。その他、OSのアップグレードもセキュリティを向上させる場合があります。システムを入れ替えるタイミングでご検討ください。

必要最低限の対策は人に迷惑をかけないようにすること

「中小企業の情報セキュリティ対策ガイドライン」が参考になると述べましたが、これだけでは必要最低限の対策には至らないと私は考えています。なぜなら、企業ごとに保有する資産は異なるため、それぞれで必要最低限の基準が異なるからです。仮に守るものが一切ないという場合であっても、攻撃者にパソコンやサーバーを悪用される恐れがあります。そのため、経営上のさまざまな事情によりセキュリティ投資が後回しになる状況であっても、少なくとも「人に迷惑をかけない」レベルの対策は必要です。そして、必要最低限のセキュリティ対策を実施した上で、企業として成長するための投資として、もう一歩進んだセキュリティ対策を検討していただきたいと思います。
本稿の最後は、10年前に同僚が発した「名言」で締めましょう。
「アップデートもウイルス対策ソフト導入もせずにネットサーフィンすることは、雪山に裸で登るようなものなんですよ！」

ラックの顔

第3回

どんな仕事でも楽しむ姿勢の持ち主

今回紹介する佐藤豊彦は社歴30年を超えるベテランだ。プログラマーとして入社後、システム開発のプロジェクトマネジャーやセキュリティの営業職、さらにサイバー救急センター長など豊富な経験を持つ。2016年4月からは、活躍の場を鹿児島大学へと移し、学術情報基盤センターサイバーセキュリティ戦略室 室長を務める傍ら、特任教授として教壇に立っている。

佐藤豊彦
sato toyohiko

鹿児島大学が市民との交流拠点として設けている
インフォメーションセンター

プロジェクトを円滑に進めるには？

「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、佐藤の人物評を見ると「アットホームな雰囲気作りがうまい」「上司であると同時に父親的な存在」といった声が寄せられている。インタビューの席でも、佐藤は終始和やかな表情で比較的ゆっくりとした口調で話し、筆者自身も温厚な人物という印象を受けた。

一方で職務経歴を見ると、システム開発が難航する案件のプロジェクトマネジャー（以下PM）やセキュリティインシデントの初動対応を行うサイバー救急センターなど、常に時間に追われ、緊張感が漂うシビアな職場を取りまとめてきた。

「周りからは温厚そうに見えるかもしれませんが、実際は短気です。PMを務めていたとき、メンバーからの報告で過大な申告やウソがあれば、ちゅうちょなく叱ってきました。プロジェクト管理の鉄則は“火（トラブル）”が起こりそうであれば事前に対処し、“火災”が起きたならばすぐに消して影響を最小限にとどめることです。このときに必要なのは周囲の協力です。普段からメンバーと信頼関係を築いていれば、いざというときに協力してくれます」

「アットホームな雰囲気」と「職場での厳しい姿勢」。相いれない要素にも思えるが、実はこれがプロジェクトを円滑に進めるこつなのだそうだ。

ユーザーの口コミで広がったセキュリティ事業

ラックがセキュリティ事業に乗り出して3年後の1998年、佐藤も営業部の初期メンバーとして参画する。その当時、顧客のセキュリティに対する意識はまだ薄く、事業がなかなか売り上げにつながらなかったため、社内からは「金食い虫」とやゆされることもあったという。

こういった事態を打開するため、営業部ではセキュリティ意識啓発のための無償セミナーを週に1回ほどのペースで開催した。佐藤は当時を振り返って「お客さまにセキュリティの費用対効果を説明することが難しかったのですが、実際にトライアルで診断を行ったり、監視装置を一定期間試用していただいたりしました」と語ってくれた。

このような地道な活動を続けたところ、口コミで業界内でのラックの認知度も高まり、売り上げも徐々に伸びていったそうだ。

同時期の2000年には中央官庁のWebページが相次いで改ざんされる事件が発生した。まさに、セキュリティに対する意識が大きく変わる転換点でもあったといえるだろう。

3年間で約1500件もの緊急連絡に対応したサイバー救急センター

インタビューでは佐藤の経歴について、さまざまな質問をしているが、その中でも筆者が過酷だと感じたのが、サイバー救急センター長時代の経験だ。3年間で約1500件もの緊急連絡に対応し、実際に出動した回数も約1000回に上るという。

ラックのホームページにはサイバー救急センターの電話番号が掲載されている。現在ではフリーダイヤルで法人からの問い合わせと個人からの問い合わせを振り分けているが、当時はこの振り分けがなく、すべての連絡が深夜・休日を問わず携帯に転送されていたそうで、佐藤はBluetoothのヘッドセットを常に装着していたという。

大きなストレスがかかる仕事のように思えるが、佐藤は「最初こそ大変でしたが、次第に慣れてきました。もともと、人と話をすることが嫌いではないという性格が幸いしたのかもしれません。逆にセンター長の職を離れて携帯電話が鳴らなくなった日常の方に戸惑いを感じてしまいます」と笑みを交えながら話す。

緊急連絡には、Webの改ざん・情報流出・ウイルス感染・P2Pファイル共有ソフトによる情報拡散など、さまざまな事案が含まれているが、佐藤はこうした事案の一つひとつが自身の知識や経験につながると考えていた。時には電話対応がうまくいかずに相手を怒らせてしまったこともあるそうだが、その場合でも今後の応対の糧にしようと考えていたそうだ。

こういった前向きな性格の持ち主だからこそ、膨大な緊急連絡に対応できたに違いない。

ヤシの並木が南国のイメージを醸す
郡元キャンパスの北辰通り

佐藤豊彦（55）
1984年入社。製造系大型汎用機のSEから官公庁・金融・流通系システムの開発マネジャーなどを担当。1998年からはセキュリティ営業部の立ち上げメンバーとして参画。その後、サイバー救急センターのセンター長などを歴任。2016年4月より鹿児島大学学術情報基盤センターに新設されたサイバーセキュリティ戦略室において、室長・特任教授に就任。

どんな仕事でも楽しみ、そして感謝する

佐藤の前向きな姿勢を表すエピソードはいろいろとあるが、鹿児島大学への赴任の経緯もその一つだといえる。鹿児島大学からラックに人材派遣の要請があり、佐藤は社内でその候補者を探す立場だったという。しかし、自らが名乗りを上げることにしたそうだ。

「私はプログラマーとして入社し、PM・営業職・サイバー救急センター・執行役員などを経験してきましたが、これに大学教授というキャリアが加わるのも面白いと思ったのです。また、私がこの職に就くことにより、後進にも同様のキャリアパスを歩んでもらえるかもしれないと考えました」

佐藤は赴任の動機をこのように語る。現在は鹿児島大学 学術情報基盤センターでサイバーセキュリティ戦略室 室長・特任教授として活躍し、ラックと情報共有しながら大学のインシデント事案の対応や大学全体のセキュリティ対策の企画・実施、経営層・教職員・事務職員・他大学の教職員を対象に講習会などを行っている。併せて大学のネットワーク環境でインシデントの研究も実施するという。また、特任教授として講義も受け持っているという。

「情報セキュリティの入門編という位置付けで全学部・全学年を対象とした共通教育科目を担当しています。今年度は250人ほどの学生が履修しています。初回の授業で最前列に座った学生が堂々と居眠りをしているのを見て落ち込みましたが、周りの先生からは『そういうものです』とアドバイスしていただきました（笑）。これまでセミナーなどで話をしてきた経験はありますが、90分の授業を15回という連続した講義は初めての経験です。本来は学生に教える立場なのですが、自分自身にとっても新たな勉強をさせてもらえる機会だと思い、常に『行いて教え、教えて学ぶ』を肝に銘じています。今回赴任を許可してくれた会社、機会を与えてくれた鹿児島大学にとても感謝しています」

また、鹿児島県警の「サイバー犯罪テクニカルアドバイザー」に委嘱され、警察職員に対して犯罪手口の最新技術について情報を提供したり、捜査員の技能向上のための講演会を行ったりもするという。2016年12月にはラック、鹿児島大学、鹿児島県警の三者による産学官連携協定が締結された。「この協定は二者間の協定書の集合の連携協定ではなく、三者が同じ内容の協定書を締結した、日本でも数少ないケースだと思います。それぞれの特徴、強みを生かして情報共有し、鹿児島県内の安心、安全に寄与していくという取り組みです。これを書面上だけでなく、成功事例として鹿児島県から発信していくことが私の使命だと考えています」

この他、地元のNPOである鹿児島インファーメーション（特定非営利活動法人鹿児島インファーメーション）に加盟し、ITを活用する全ての現場や分野において調査・研究・教育・指導・啓発を行うなど、鹿児島県に暮らす人たちの生活向上等に貢献する活動も実施しているという。

最後に、仕事に対するモチベーションの源泉について聞いてみた。

「どんな仕事でも楽しみながらやらなくては仕事ではないと思っています。そして新しいことにチャレンジできることへの感謝が原動力となっています。社会人になって30年以上たっていますが、常にこの気持ちを持ち続けています」

記事で紹介したそれぞれのエピソードを改めて「楽しむ」というキーワードで見直してみると、全てが一本につながると合点がいくはずだ。そして、佐藤は今後も同じスタンスを保ちながら仕事を続けていくに違いない。

インタビュー＝斉藤健一（株式会社HTP）

第3回 地方から盛り上げる情報セキュリティ勉強会

文=八尾 崇　サイバー・グリッド・ジャパン ICT利用環境啓発支援室　チーフリサーチャー

▶セキュリティ勉強会って？

近年、全国各地で年間40回を超える情報セキュリティの勉強会が開催されています。この「セキュリティ勉強会」、皆さんはどのようなものを想像するでしょうか？

- ○ 悪い下心を持った人たちがセキュリティの研究・発表をする場？
- ○ 営業が講演と称して商品説明をする場？
- ○ 飛び交うのは専門用語や横文字ばかりで日本語では話していない？
- ○ いつも同じ顔触れで新規には加わりづらい？
- ○ 変な商品を売り付けられる？

ご安心ください。このようなことが当てはまる勉強会は一つもありません。勉強会は、参加者が直面しているセキュリティの問題について、セキュリティ業界関係者から話を聞いたり、参加者同士で意見交換をしたりと、真面目にセキュリティの勉強をする場です。勉強会には、どのような人が参加しているのでしょうか。私は長年、各地のセキュリティ勉強会で企画・運営のサポートを行っています。その経験からお話しすると、参加者の多くは30代から40代で、技術者もいれば、業務でパソコンを利用する一般ユーザーまで、実にさまざまな職種の人が一堂に会します。

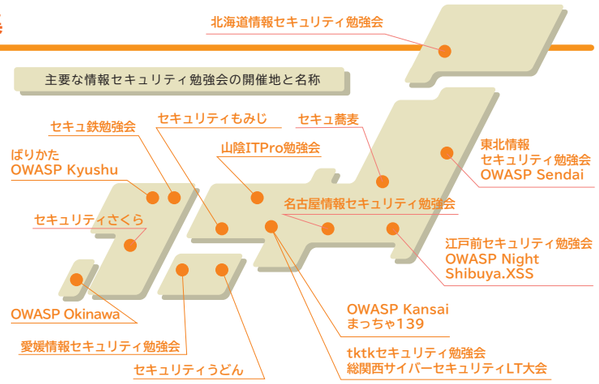
勉強会のような集まりに参加すること自体が初めてだという人がたいてい半数程度を占めます。学生の参加も、多いところでは20%程度、少ないときでも5%程度は見られます。

皆、何かしらの問題意識を持って足を運んでいるため、勉強会中も、終了後に講師を囲む質問タイムも真剣そのものです。日頃、セキュリティ対策で苦労している人が多いんだなと思う瞬間です。

▶参加者の目的は社外からの情報収集

これも私の経験則によりますが、参加者の目的は社外から情報を得ることにあるようです。しかし、参加者が所属する組織に目を向けると、勉強会に参加する人の割合は組織全体の１%程度にすぎません。人口の多い首都圏であれば１%でも相当な数になりますが、地方ではまだまだ参加者の数そのものが少ないのが現状です。図は、各地で開催されている勉強会のうち、有名なものや私がサポートしているものを一覧にしたものです。

全国さまざまな場所で情報セキュリティの勉強会が開催され、セキュリティに関する情報交換や勉強をしています。



▶不足するセキュリティ人材と地方の現状

国内では現在、セキュリティ技術者が大幅に不足しています。独立行政法人情報処理推進機構(IPA)が平成26年に実施した調査によると、国内のユーザー企業で情報セキュリティに従事する技術者は約26.5万人ですが、それでもまだ８万人が不足しているとされています。

ただ、不足していると言っても、首都圏と地方では求められる人材が異なります。首都圏では現在、サイバー攻撃などから企業を守るセキュリティスペシャリストのニーズが高まっていますが、地方では、セキュリティベンダーや各種ベンダーの人材の他、自組織のメンバーを動かしたり、社外とやりとりしたりするセキュリティディレクターが必要とされています。

地方でこうした人材が求められる背景には、情報システム関連の業務を一人のスタッフが全て担う「一人情報システム担当」体制となっていたり、さらには、システム開発からインフラ運用までをも一人で担っていたりする組織が多く見受けられる現状があります。

勉強会では、このような一人で奮闘している人にこそ、セキュリティの現状についての認識を深めてもらい、身近な問題と捉えた上で対策を進めるきっかけとしてもらいたいと考えています。

最後に

読者の皆さんも、少しでも興味を持った勉強会にぜひ遊びに行ってみてください。
業務での自分の守備範囲よりも少し広めの分野の情報収集を目的として参加すると、さまざまな発見があるかもしれません。
身近な場所で開催される勉強会だけでなく、離れた場所で開催される会にも
「おいしいものを食べに行くついで」程度の気軽な気持ちで足を運んでみてはいかがでしょうか？

CYBER GRID JOURNAL VOL.3

サイバー・グリッド・ジャパンは株式会社ラックの研究開発部門です。
サイバー攻撃や各国のセキュリティ事情、セキュリティ防御技術などに関する最先端の研究のほか、
複数のセキュリティ企業との連携や新たな製品・サービスの開発、各種啓発活動などにより
日本のセキュリティレベルと情報モラルの向上に貢献しています。

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　https://www.lac.co.jp/

株式会社ラック
サイバー・グリッド・ジャパン