CYBER GRID JOURNAL

サイバー・グリッド・ジャーナル

VOL. 5

特集

ラック社員の人材育成

形式にとらわれない自由な発想で、
技術とともに“人”を育てる

CYBER GRID JOURNAL VOL.5

TABLE OF CONTENTS

3 巻頭言
川口 洋

4 特集
ラック社員の人材育成
～形式にとらわれない自由な発想で、技術とともに“人”を育てる～
谷口 隼祐

8 ラックセキュリティアカデミー
「インシデントが起きたらこんな感じかもしれない」をつかむ
星 代介

10 「すごうで」のその後…
学生に対する支援活動の意義
株式会社Eyes,JAPAN 金子 正人氏
インタビュアー：川口 洋

14 ラックの顔　さまざまな場所で活躍する社員をご紹介
第5回 同性からのサポートが
セキュリティ業界で働く女性の未来を創る
鈴木 悠／青羽 真利

18 巻末あとがき
サイバー・グリッド・ジャパンのご紹介

巻頭言

サイバー・グリッド・ジャパンにおける人材育成活動

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

日本では、セキュリティ人材の不足が課題となっています。今回のサイバー・グリッド・ジャーナルではサイバー・グリッド・ジャパンが行っている人材育成の取り組みについて紹介します。

サイバー・グリッド・ジャパンでは、以下の3つの観点から人材育成に取り組んでいます。

1.ラック社員の育成
2.セキュリティ教育ビジネスへのコンテンツ提供
3.セキュリティ業界の健全な発展

サイバー・グリッド・ジャパンにおける人材育成の1つ目の取り組みは「ラック社員の育成」です。日々新しい技術が生まれ、変化するサイバー空間の脅威に対応するため、ラックではさまざまな取り組みを行っています。総務人事部主導の社員研修や各事業部の業務トレーニングに加え、社外で行われるカンファレンスや勉強会への参加も推奨しています。サイバー・グリッド・ジャパンでは、社員の技術的探究心を刺激するため、社内CTF大会「LACCON」を開催しています。また、コミュニティ活動であるHardening Project や SECCON などのスポンサーシップを通じ、社員の社外活動を支援しています。

2つ目の取り組みは「セキュリティ教育ビジネスへのコンテンツ提供」です。ラックは「ラックセキュリティアカデミー」というセキュリティ教育ビジネスを持っています。ラックセキュリティアカデミーはセキュリティ教育を、組織全体が取り組む活動と考え、セキュリティ対策の過剰や不足にならないようバランスを整えたセキュリティ強化を目標とした教育コンテンツを提供しています。サイバー・グリッド・ジャパンはLACCONやHardening Projectで得られた知見をもとに、競技形式の教育コンテンツをラックセキュリティアカデミーに提供しています。

3つ目の取り組みは「セキュリティ業界の健全な発展」です。サイバー・グリッド・ジャパンでは、セキュリティ業界が健全に発展していくためにはこの業界で働きたいという若者を発掘、支援することが重要だと考えています。サイバー・グリッド・ジャパンでは、突出した技術力を持つ若者を支援するプログラム「すごうで」を実施しています。誰もが安心・安全にネットを利用できる環境構築のために、情報セキュリティや情報モラルに関する地域啓発活動の普及・促進活動を行っています。[1]

大学院生時代に研究室のシステムが不正アクセス被害に遭ったとき、私は、多くのセキュリティ業界やIT業界の先輩方に指導や支援をしていただくことでシステムを復旧することができました。社会人になった今、「なんとか日本のセキュリティレベルを向上したい」「現在のセキュリティ問題を改善したい」「後輩たちの力になりたい」という想いを実現することで、その恩を返していきたいと思っています。

今回のサイバー・グリッド・ジャーナルではサイバー・グリッド・ジャパンが行っている人材育成活動を紹介します。読者の皆さまが少しでも人材育成に興味を持ってくださり、できるところから取り組んでいただけることを願っています。

[1] CYBER GRID JOURNAL Vol.3 https://www.lac.co.jp/lacwatch/report/20170316_001239.html

特集

ラック社員の人材育成

～形式にとらわれない自由な発想で、技術とともに“人”を育てる～

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　谷口 隼祐

ラックは、1986年に設立した旧ラックと1987年に設立したエー・アンド・アイシステムが経営統合し、その後、事業買収や子会社の吸収合併などを経て現在に至ります。サイバーセキュリティの分野においては、旧ラックが1995年からいち早くサービスを提供してきましたが、国内の市場はまだ小さく、10年後の2005年までセキュリティ事業は赤字が続くような状況でした。「それでもセキュリティの必要性を信じ日本を守る」という思いに共感し、私は2006年に入社しました。入社当時は、標的型攻撃の話題もありましたが、SQLインジェクションの脆弱性やファイル交換ソフトによる情報漏えいの方が注目されていました。

その後、社会のITに対する依存度は年々高まり、それに呼応するように脅威も大きくなっていきました。今では「情報セキュリティ」よりも「サイバーセキュリティ」、「ウイルス」よりも「マルウエア」といった、より広い範囲を示す用語が使われ始めていますし、また、システムの企画・設計段階からセキュリティを意識するようにもなってきています。セキュリティが社会全体に広がっているのを実感しています。

このような変化の激しいセキュリティ情勢の中、道なき道を行き、ラックが成長し続けてきた原動力を、生意気な言い方ですが、私は「人材」だと考えています。前置きが長くなりましたが、ラック社員の人材育成の一部を紹介します。

ラックの成長と共に醸成された企業文化

現場で目にする実際の脅威をもとに、セキュリティソリューションサービスを提供してきたわけですから、ラックのセキュリティに関する新規サービスは、使命感が先行しているものが多いように思います。技術好きがまず試し、後に正式なサービスになる――。こうして、セキュリティ診断に始まり、JSOCの監視、セキュリティアカデミーでの教育やトレーニング、サイバー救急センターなどのサービスが展開されました。“「やりたい」と声を上げるとやれる文化”がラックをつくってきたとも言えるでしょう。この辺りの話は、下記のサイトでの対談に詳しく載っています。[1]

1 セキュリティ診断サービス「ほぼ」20周年特別企画「行く診断」
https://www.lac.co.jp/lacwatch/service/20170116_001173.html

興味先行で始まったコンテンツが人材育成に発展

一方、興味が先行してスタートし、現在では社員の人材育成にも活用されているコンテンツとして、Hardening Project（以下、Hardening）とLACCON（ラッコン）があります。ここまでの流れで勘の良い方はお気付きかと思いますが、「あったらいいな、楽しそう!」をひとまず形にしたものが、結果的に社内の人材育成に活用されています。

Hardening

Hardeningでは、「衛（まも）る技術」の価値を最大化することを目指して活動しています。具体的には、チーム対抗で、事務局側が事前準備したセキュリティがおろそかになっているECサイトを競技期間中に仕掛けられるさまざまな脅威から守りつつ売上を競うイベントを開催しています。Hardeningは、非営利団体のWASForumが企画・運営していますが、このプロジェクトの発起人の一人がサイバー・グリッド研究所の所長でもある川口です。現在はプロジェクト委員にラック社員が3名、技術協力として他に数名が関わっています。

Hardeningイベント開催一覧

2012年	4月	Hardening Zero	（東　京）
	10月	Hardening One	（東　京）
2013年	7月	Hardening One Remix	（東　京）
2014年	6月	Hardening 10 APAC	（沖　縄）
	11月	Hardening 10 Evolutions	（沖　縄）
2015年	6月	Hardening 10 MarketPlace	（沖　縄）
	11月	Hardening 10 ValueChain	（沖　縄）
2016年	6月	Hardening 100 Value × Value	（沖　縄）
	11月	Hardening 100 Weakest Link	（沖　縄）
2017年	6月	Hardening 1010 Cash Flow	（沖　縄）
	11月	Hardening 2017 Fes	（淡路島）

2017年11月に行われたHardening 2017 Fesの競技風景

各チームの売上や人気度を表示したスコアグラフ

Hardeningイベントに参加することで、息つく暇もなく発生するインシデントに対処する経験が得られるだけでなく、他の組織の方との交流を深められるというメリットもあります。そのため、ラックでは社員の参加を推奨しています。サイバー・グリッド研究所では、参加者の旅費の支援やHardening参加報告を兼ねた勉強会を開催しています。また、本家Hardeningの企画・運営に携わるメンバーの知見とJSOCやC119のインシデント対応の知見を活用して、2012年以降、社内版Hardeningイベントとして「ラックサバイバルチャレンジ」[2]を実施し、現在も継続しています。

社内版Hardening
「ラックサバイバルチャレンジ」の競技風景

2 サイバー攻撃パニックシミュレーション「ラックサバイバルチャレンジ」
https://www.lac.co.jp/corporate/citizenship/lac_survival_challenge.html

LACCON（ラッコン）

LACCONは、ラックおよびグループ会社を対象としたCTF（Capture The Flag）形式のセキュリティ競技です。技術が好きな若手社員が集まり、「CTF未経験者でも学びを得られる問題を作る」をコンセプトに2015年度から開催しています。サイバー・グリッド研究所が企画・運営を支援しています。

LACCON開催一覧

2016年	3月	新入社員対象CTF
2017年	2月	第1回社内CTF「LACCON」
	4月	即！西本面接
	12月	第2回社内CTF「LACCON」

第1回社内CTF「LACCON」表彰式

当初は、作問者も参加者も新入社員という形でスタートしましたが、翌年には、任意参加の社員研修という位置付けになり、対象もラックのみならずグループ会社にまで拡大して実施しました。この時にLACCON（ラッコン）という名称がつきました。第1回大会は、現社長（当時は専務取締役）の西本から、活躍した個人にオリジナル腕時計のプレゼントもあり、大いに盛り上がりました。結果は、グループ会社のネットエージェントから参戦したチームが優勝し、2位はサイバーセキュリティ関連部門！　ではなく、システムインテグレーションサービス部門から参戦したチームでした。そして3位は研修中のJSOCアナリストチームでした。

LACCONには、作問者、参加者それぞれに面白い社員がいることを経営層に気付かせる副次的効果があり、2カ月後にはLACCONのシステムを利用した新卒採用「即！西本面接」[3]が実施されました。2018年4月には、「即！西本面接」で好成績を残した3名が入社する予定です。私も最終面接に同席いたしましたが、3名とも個性的で優秀な方々でした。彼らの活躍を楽しみにしています。実は、CTFスキルは業務スキルに直結しないことが多いため、「即！西本面接」実施に当たり社内でも議論があったのですが、会社として真面目に取り組むと約束もあり、最終的に実施に至っています。本記事では紙面の都合上、詳細は割愛させていただきますが、ご興味のある方は当社サイトをご覧ください[4]（いろいろと大変でした）。

本記事執筆時点において、第2回ラックグループCTF「LACCON」の開催準備をしています。今期はサイバーセキュリティ関係部門のチームは活躍できるのでしょうか。また、無事に開催できるのか。期待と不安で胸がいっぱいです。

第2回社内CTF
「LACCON」スコアサーバー

3 『即！西本面接』CTFによる新卒採用キャンペーン！才能ある「あなた」をお待たせしません。
https://www.lac.co.jp/lacwatch/announce/20170418_001271.html

4 『即！西本面接』を支える社員たち（裏方のベテラン達）
https://www.lac.co.jp/lacwatch/announce/20170421_001275.html

アジャイル開発の基礎を学ぶ、SCRUM BOOT CAMP

現ラックに対してセキュリティ会社というイメージを持たれる方は多いと思いますが、当社は独立系ITベンダーの顔も持っています。事実、社員の約2/3はシステムインテグレーションサービス系の業務に従事しています。ラックでは、アジャイルソフトウエア開発手法の一つであるスクラムでシステム開発を行っているエンジニアや、これからスクラムを導入してシステム開発を行うことを検討しているエンジニアを対象にした研修を実施しています。

研修では、

- スプリント内の割り込みが、どれだけ効率を落とすかを実感できた
- 普段やっているプラクティスの目的を再確認することができた
- スクラムの手法というより、自分の働き方を考え直す良いきっかけになった
- “カイゼン”ではなく、普段いかに残業でカバーしているだけかを気付かされた
- いかに普段のマルチタスクが業務効率を下げているかを理解できた

といった、ソフトウエア開発に限定されない「仕事の進め方」を学んだという声も多く聞こえています。主にシステム開発で導入されているスクラムですが、アジャイル開発で必要とされる考え方や自己組織化の手法はシステム開発以外の業務でも有効です。ラックではセキュリティ診断サービスにおいてもスクラムに基づく管理手法を取り入れており、研修にはセキュリティ系の業務に従事するエンジニアも参加しています。

その他のラックの人材育成の取り組み

トップガン講座

現場の最前線で活躍しているエンジニアによる社内研修
「Webアプリ診断」「マルウエア解析」「フォレンジック」の3コース

アカデミーオープンコース受講

ラックで社外向けに提供しているセキュリティ教育サービスを受講できる
https://www.lac.co.jp/service/education/

研修風景

カンファレンス参加支援

国内外のカンファレンス参加の支援を行う
FIRST、BlackHat、HITCON、RECONなどの海外カンファレンスには年間延べ20名以上、国内カンファレンスを含めると50名以上の社員が会社の支援を受けて参加

勉強会やセキュリティイベントへの講師派遣

業務の一環として、次代のエバンジェリストor「伝える力」を育むため、地方で開催される勉強会などに若手を講師として参加させる

前述したHardeningも含め、国内のセキュリティイベントやカンファレンスの運営に携わる社員も複数います。今号の「ラックの顔」では、女性セキュリティ人材の支援活動を行うCTF for GIRLSの運営メンバーを取り上げています。

最後に

やりたいことに挑戦しやすいラックの文化に関わるものを中心に、社員の人材育成の取り組みを紹介しました。ただし、客先常駐、育児や介護をしながらの勤務者など、挑戦すること自体がハードルになるケースも存在します。そういったこともよく考え、社員一人一人のスキルアップしたい気持ちに応えられるような施策をこれからも考えていきます。

インシデントが起きたら こんな感じかもしれない をつかむ

ITプロフェッショナル統括本部 サイバーセキュリティ事業部
ラックセキュリティアカデミー　星 代介

Nov. 28, 2017　14:00 頃

ラックセキュリティアカデミーの星です。
私は今、平河町森タワーの2階、とある部屋でこの原稿を書き始めました。
11月も間もなく終わろうとしている、小春日和のある日です。平河町森タワーといえば、株式会社ラックの本社があることで有名なモダンなビルです。窓の外は首都高で、行き交う車が絶えません。
すぐ横では、インシデント対応が山場です。とても盛り上がっています。望んでか望まずか、部屋に缶詰めとなった緊急対応チーム。ヒートアップしているせいか、部屋の中は室温以上に暑く感じます。

「Webサーバーに脆弱性があったんじゃないか？」
「コールセンターからデータベースに不正アクセスされたのでは？」
「勝手にマスコミにしゃべったんですか？
必ずうちのチームを通すように言ってください！！」
「監視カメラ確認してくださいっ！！」
「サービスがいきなり止まったんで、社長が怒っていますよ」
「どうします？　警察に突き出しますか？？」

いろんな会話が飛び交っています。でもなぜでしょう。会話に似合わず、皆とても生き生きと楽しそうにしています。
チームの判断にミスがあったのか、取引先からクレームが入ったようです。「あちゃー、やっちゃったなー」と言いながらもチームの皆はまだニコニコしています。反省するとか落ち込むとかした方がいいんじゃないでしょうか。

「社長！ 記者会見の準備をお願いできますか！！」

顧客情報が漏えいしたということで、株式会社ラッコの代表取締役社長が謝罪会見を開くようです。

ラッコ？

株式会社 **ラッコ???**

そう、株式会社 **ラッ「コ」** です。

オンラインのショッピングモールを運営する株式会社ラッコは、インシデント訓練の舞台となる仮想組織。つまり、私が今までにお話ししたことは、すべて訓練上の出来事であり、フィクションです。
さまざまな企業、組織から訓練に参加している受講者は、たまたま今日同じテーブルに着いたメンバーで緊急対応チームとなり、インシデントの予兆（ぽい事象）に対してアクションを取ります。
冒頭で紹介した会話は、11月28日の訓練中、座ることも忘れ、ワイワイガヤガヤとやっている中で、実際に発されたものです。
今日の訓練はクローズドシナリオ、つまり受講者は、どのような事象が起こっているのか分からない中で判断・対応する、という訓練です。今何が起こっているか、何をすればいいか、一種の謎解きゲームのようにセキュリティ事故を体験する、という訓練です。本番さながらの空気に、気が付けば皆立ち上がってしまうという。

Nov. 28, 2017　15:30 頃

えー、今訓練が終わりました。
受講者の皆さま、充実した表情をしております。無事に復旧できたのでしょうか。
これから各チームそれぞれにうまくいった点や気付き、改善すべき点などを振り返ります。

Bチームは休憩を取れなかったように見受けられますが……。
休憩を取ることも非常に大事です。が、意外と休憩を取るのも難しいですよね。あれってどうなんだろう、こうしたらどうなるだろう、ああ、一つやり残していた……などと悶々と考えてしまう。これは本当のインシデント対応でも気を付けたいですね。

対応の進み方、振り返り方はチームによってさまざまです。記録の取り方一つとっても全く違いますので面白いですね。チーム同士で気付きを共有することで、より多く有意義なものを現場に持ち帰っていただきたいと考えております。

さあ、こんなインシデント対応訓練が、ものすごく売れています。商売の話で恐縮ですが、とても好評です。今週は、平日5日のうち4日も訓練をしています。残る1日も訓練の準備をしていました。
受講者の皆さまに多くの気付きを得ていただくとともに、我々講師も毎回新しい気付きがありますので、それを糧にブラッシュアップし続けています。

Nov. 28, 2017　16:30 頃

さて、今日の振り返りでは、

- **手順を事前に整備しておく大事さが分かった**
- **知識として知っているつもりだったが思ったように対応できなかった**
- **メンバー間での意思疎通が難しかった**
- **役割分担がうまくできなかった**
- **講師のコメントで理解が深まった**
- **他のメンバーの視点が参考になった**
- **調査に没頭してしまって対外対応がおろそかになってしまった**
- **サービスを再開できなかった…悔しい（;ー_ー）**
- **他社・他業種の、普段聞けない意見を聞けてよかった**
- **楽しかった！　また受けたい！！！**

などなど、たくさんの気付き（と感想）が発表されました。

考えてみれば、事前の準備が大事だということは、皆が知っているわけですけれども、それを身に染みて分かる機会はなかなかないわけですね。コンサルタントに言われて、親会社に言われて、上司に言われて、体裁だけ繕っちゃったというケースはままあります。その気持ちはとてもよく分かります。

インシデントなんか起こらない方がいいですし、起こったとしても最小の被害で防ぎたい、いや、やっぱり自分には起こってほしくない。そういったお悩みをお持ちでしたら、こんな訓練をしてみてはいかがでしょうか？　そんな思いでやっております。

実際にインシデントを経験されている組織では、必然的に力を入れているインシデント対応訓練ですが、インシデントを未経験の組織であれば、実際にコトが起こる前に訓練として緊急対応を体験することで、被害が大きくなる前に最適な対応を取れるようになっていけばよいなと考えております。

受講者の属性は本当にさまざまです。企業のCSIRTに属しているという本格的な方もいらっしゃいますが、あんまりITに慣れていないけどセキュリティ担当になっちゃった、という方もちらほら。
今日の訓練は机上訓練ということで、パソコンを使いません。そのため、IT知識レベルにかかわらず参加できて、それぞれが気付きを得られるというハードルの低さも売りです。
経験者や上級者であっても、思い込みから判断を誤ってしまうこともあり、講師の立場から見ても、インシデント対応は難しいなと感じます。（インシデント経験者が参加すると、経験談も聞けて非常に盛り上がりますので、ぜひご参加を！！）

Nov. 28, 2017　17:30 頃

受講者の振り返りも終わり、質疑応答も終わりました。警察にどんなタイミングでどんなふうに連絡するか、という話もとても面白い。確かに実際のところどうなの、という感じがしますよね。

もう気が付けば夕刻です。
今日も、皆さまによい研修を提供できた、よかった、といつも感慨深くなります。
皆さま、お疲れさまでした。

Nov. 30, 2017　13:30 頃

ラックセキュリティアカデミーの星です。
今日もインシデント対応訓練の研修です。
訓練の説明が終わり、リーダー決めが終わり、間もなく訓練の開始です。
今日は28日の机上訓練とは違い、実機を使った訓練です。パソコン、ファイアウォール、サーバーを実際に触ってインシデントの対応を進めていただきます。
そのため、机上訓練と違って、受講者のほとんどはIT系の技術者です。ちなみに、組織の中核を担うセキュリティ人材を育てたいという場合なんかには、この実機訓練をご提供するケースが多いです。
（とはいえ、机上訓練がそれに劣るかというとそういうわけでもなく。多分、実機がある方が臨場感が出てモチベーションが上がりやすいんでしょうか、フォレンジックの実機演習なんてすごく面白いですもんね。）

さあ、今日はどんなシナリオでしょうか。
皆さんよい気付きを得られますように！ と願いつつ、攻撃コマンドをお送りします！

ラックセキュリティアカデミーについて

ラックセキュリティアカデミーが提供しているセキュリティ教育・訓練を、ホームページにて紹介しています。

11月28日に実施していたのは「情報セキュリティ事故対応1日コース 机上演習編」、11月30日に実施していたのは「情報セキュリティ事故対応2日コース 実機演習編」です。そのほかさまざまなコースの紹介や、詳細をご案内するパンフレットも下記ホームページからダウンロードできます。

パンフレットに掲載している日程以外の個別開催や、ご指定の場所に伺っての個別開催も承っておりますのでお気軽にご連絡ください。

ラックセキュリティアカデミー
〒102-0093 東京都千代田区平河町 2-16-1 平河町森タワー
TEL 03-6757-0125　FAX 03-6757-0112
Email info-academy@lac.co.jp
https://www.lac.co.jp/service/education/

「すごうで」のその後…

学生に対する支援活動の意義

サイバー・グリッド・ジャパンは、ITを使って世の中を便利にしたい、自分を成長させたいと願う
若い皆さんの夢の実現をお手伝いする「ITスーパーエンジニア・サポートプログラム“すごうで”」を2013年から実施しています。
この「すごうで」は、2012年にある学生たちの活動を支援したことがきっかけで生まれました。
その支援対象であり、現在は株式会社Eyes, JAPAN❶に勤務する金子正人さんに、
「学生に対する支援活動」というテーマでお話を聞きました。

質問に熱く答えている金子さん

金子正人といいます。福島県会津若松市にある「株式会社Eyes, JAPAN」という会社（以下、EJ）で働いています。EJは会津大学の初の認定ベンチャー企業❷です。そのEJでお客さまのITシステムの構築と運用を行いつつ、コンサルティング業務も行っています。コンサルティングの中で寄せられる質問には、セキュリティに関するお悩み相談も含まれています。そのほか、EJの業務と並行して、独立行政法人 情報処理推進機構（IPA）の職員として月に4日ほど人材育成事業にも関わっています。

── セキュリティとの関わりはどのように始まったのですか？

中学生くらいのときからセキュリティにはぼんやりとした興味がありました。「あー、なんか面白そうだなあ。かっこいいかも」と。会津大学に入ってからUnixやプログラミング、ネットワークの勉強をするようになり、知人に誘われてEJでアルバイトとして働くようになりました。その時はまだ具体的にセキュリティの仕事をするようなイメージはなかったです。

アルバイトを始めてしばらくしてから、EJの社長の山寺に東京で開催される勉強会に連れて行ってもらった際、ロシア人のマラットさんと友達になりました。そして、そのマラットさんの声掛けで学生メンバーが集まり、CTF（Capture The Flag）チームが結成されました。2012年5月に開催された学生限定のCTFにその学生CTFチームで初めて参戦したときには、惨敗だった記憶があります。あの時は何もできず悔しかったです。その後、その学生CTFチームでいくつかのCTF大会を経験したころ、マラットさんから「ロシアにいる友達がPositive Hack Daysというカンファレンスの中でCTF大会を開催するからみんなで参戦しよう」と提案されました。

── そこからいきなりロシアのCTF大会ですか？　ずいぶんと飛び越えていきましたね。

その時は「ロシアとか行ったことないし、面白そうだ」と思って気軽に話に乗ったのですが、僕らのCTFチームはみんな学生なので、ロシアへの渡航費が問題になりました。安いチケットで行くとしても、1人30万程度はかかります。マラットさんがロシア遠征のスポンサーになってくれる企業がないかといろいろと声をかけていたようです。そこで出会ったのがラックの西本さん❸なんです。西本さんの「ロシアにまで行って戦ってみたいという学生の心意気を支援したい」というお言葉で、8人分全員の渡航費を負担していただきました。❹まさか本当にスポンサー企業が現れるとは思ってもいませんでした。この支援をしていただいたことがその後の「すごうで」につながったと聞いています。

そのロシア遠征が決まったとき、セキュリティ業界のあるベテランの方からアドバイスをいただきました。

「他の日本の学生は参加することができないロシア遠征のチャンスを得たのは大変光栄なことだ。思いっきりやってこい」

この言葉を胸に、身を引き締めてロシアに乗り込みました。

── 実は私もその話が決まった後、突然西本に呼び出されて「学生のロシア遠征を支援するから、お前も一緒にロシアに行って様子を見てきてくれ」と言われてロシアに行くことになりました。❺私は併設されているカンファレンス会場のセミナーをのぞきつつ、金子さんチームのCTFの様子をうかがっていましたが、慣れない場所でのハイレベルな戦い。大変でしたよね。

いざロシアに行ってみたら、街中の表示がロシア語、お店の人の会話も基本的にロシア語と戸惑いも大きかったです。ロシア到着の翌日にはCTFが始まりました。まず、つまずいたのが競技説明でした。ロシア語で競技説明が行われますが、当然ロシア語は全く理解できませんでした。ロシア語に続いて、英語でも説明が行われたのですが、その英語の説明もロシア語に比べて情報が少なく、競技環境やルールの把握に苦労しました。日本で行われるCTFに参戦する海外からの参加者の苦労が少し分かったような気がします。

そしてCTFの競技形式にも戸惑いました。それまで僕らが参加したことがあるのはJeopardy（ジョパディ）というクイズ形式のものでした。さまざまな問題がクイズのように提供されるため、得意なジャンルがあればポイントを稼ぐことができます。しかし、このロシアのCTFはチームごとに与えられた環境を防御しつつ、攻撃することが求められる「Attack & Defense」形式でした。この形式では、自分たちのチームの環境に存在する脆弱性を探して防御しつつ、他のチームの環境を攻撃して、ポイントとなる「フラグ」を取得する必要があります。ジョパディ形式よりも高度な能力とスピードが求められます。しかも、会場にはDEF CON CTF❻に参加するようなベテランチームも参加していました。当然、僕らのようなひよっこのチームはベテランチームのポイント稼ぎのターゲットにされ、たくさんの攻撃が行われました。自分たちで脆弱性をつぶしきれないまま、次から次へと攻撃され、ポイントを奪われていくのは悔しかったですね。「何が起きているんだか分からない」それがCTF開始後の数時間の心境でした。それでも、ゲームに徐々に慣れてきて、なんとか上位チームに攻撃された痕跡を調査し、まだ対応していない他のチームに同じ攻撃を行ってポイントを稼いだりしていました。

── 結果的には12チーム中9位で、初出場ながらかなり奮闘していたのではないかと思います。

なんとかビリにはならなかったですが、ポイントの多くはマラットさんが稼いでくれたもので、全てが僕らの実力とは言えたものではありません。気軽にロシアまで行ってCTFに参加してみたら、そこに集まっていた世界ランカーに「フルボッコ」にされた感じですね。この力の違いを見せつけられたことがとても刺激になって、自分が知らないことが多いということへの気付きが一番の収穫になりました。特にこの「Attack & Defense」形式のCTFがものすごく面白かったですね。

「こっちを止めれば攻撃は防げるけどポイントは下がる。でも、そのままにしておけば他のチームから攻撃されてしまう。しかし、ゆっくり考えている時間もなく、刻々と変わる状況で判断しなければならない」

「Attack & Defense」形式では他のチームとの駆け引きやリアルタイム性、作戦の取捨選択、そしてそれらのバランスを取る作戦を考えることが重要です。リアルな環境の制約の中でどう攻略するかを考えるのがとても楽しい。この形式のCTFをもっとやりたいと思うようになりました。

── ロシアのCTFに挑戦してからの、その後の活動を教えてください。

そのロシア大会の優勝チームはDEF CON CTFにも参戦したようです。そんな世界レベルのチームと戦い、レベルの高さに少しでも触れたことがとても刺激になりました。もっとCTFで上位に食い込みたいという思いが強くなりました。身近な会津でCTFに挑戦する仲間を集めようと周りに声をかけたのですが、人集めには苦労しました。地方に住んでいるとセキュリティの情報が少なく、CTFに興味を持つ人もほとんどいません。ここが東京と地方の悲しい差だなと思います。

EJに就職してから会津大学の課外授業で「Practical Application & Network Defense」という講義を持たせてもらいました。週に1回1時間半、5人～6人の学生を対象に、CTFという題材をきっかけにして情報セキュリティの面白さを伝える講義にしています。CTFや情報セキュリティの世界に興味を持つ人を増やしていきたいと思い、

❶ http://www.nowhere.co.jp/
❷ 会津大学は、大学の研究成果や資源等を活用して起業したベンチャーに「会津大学発ベンチャー」として称号を授与している　http://www.ubic-u-aizu.jp/incubation/venture.html
❸ 当社の代表取締役社長（2012年当時は取締役 兼 セキュリティ事業統括CTO）
❹ ラック、ロシアCTFに挑戦するチームTachikomaのスポンサーに https://www.lac.co.jp/news/2012/05/02_news_01.html
❺ 川口洋のセキュリティ・プライベート・アイズ（41）：ロシアでわしも考えた - @IT　http://www.atmarkit.co.jp/ait/articles/1208/08/news134.html
❻ https://www.defcon.org/

最初はsudo ⑦できなかったんですよ〜、と楽しそうに笑う金子さん

金子正人さん

現在まで4年ほど続けています。会津大学には、コンピュータの専門分野に関して強い関心や熱意をもった学生が集まる傾向があるので、そういう学生に情報セキュリティやCTFの世界観を伝えたり、自分で手を動かしていろいろと体験してもらうことで、知識や興味の幅を広げてほしいと思っています。最近ではその甲斐もあり、学生CTFチームも生まれています。

── 金子さんは育成される側から育成する側に回っています。

好きなことをいろいろとやろうと思っても一人ではどうにもならなかったんです。やはり仲間が必要だなと思っていて、少しずつ自分が持っている知識を人に教えながら輪を広げていきました。今は会津大学の学生やEJのアルバイトスタッフが興味を持ってくれるのがうれしいですね。そうやって人が集まり、コミュニティができあがって、動くようになってきたら、さらに人が集まってくるようになりました。徐々にいい流れができてきたのかなという感触があります。今度、後輩たちと一緒に仙台のCTF大会にも出場する予定です。

ただ、最初に刺激を受けた「Attack & Defense」形式のCTFはロシア遠征以降ほとんど体験できていないです。「Attack & Defense」形式は、別の形式で行われるCTFの予選を突破したチームが進む、本選に採用されることが多いんです。最近はCTFに興味を持つ人が増えたことで予選を突破することが難しくなっており、毎回悔しい思いをしています。CTFの数は増えていますが、それ以上に参戦する人数が増えているためですね。予選突破するためにも仲間を集めてさらに研鑽を重ねたいと思っています。

── そういえば、アルバイトからそのままEJに就職したんですね。

最初はEJのアルバイトとして働いていたのですが、EJの仕事が楽しすぎて、大学を中退して、そのままEJに就職しました。一緒にロシア遠征した学生メンバーはIT業界に就職していますが、セキュリティの仕事をしているのは私ともう1人くらいかもしれません。やはり会津でEJの仕事がしたかったんです。

── そんなふうに言ってもらえる会社は素敵です。でも以前、EJの山寺社長が「金子がアルバイトで入ってきたときには、危なっかしくてシステムの管理者権限を当分渡さなかった」と言っているのを聞いたことがあります。⑧そのエピソードの裏側も教えてください。

今思うと、EJにアルバイトで入ったころの自分には、セキュリティというジャンルが「面白そうだ」という理由だけでこの仕事をやりたがっていた節がありました。どうも社長にはそれが危なく映っていたみたいです。よく「若者にありがちな根拠のない万能感」と言われていました。実は、アルバイトとして入社してから2、3年程度の間は管理者権限をもらえませんでした。それから真面目に仕事を続けて、あるお客さまのシステムを一から作った時に初めてシステム管理者権限を与えてもらえました。それから徐々に仕事を任せてもらえるようになりました。

EJで仕事をしていると、社長の山寺のネットワークでいろいろな情報が入ってくるのが面白いんです。山寺は会津を中心として世界各地を飛び回り、ビジネスの種を探しています。復興庁の支援事業に採択されて、自転車を活用した観光・環境データの提供、車輪型広告事業をやったこともあります。また、医療機器のセキュリティ問題を考える「医療セキュリティハッカソン」を企画、開催するなど大変刺激的な活動をしています。そんな山寺の周りに刺激的な人が集まってきています。株式会社アスタリスク・リサーチの岡田良太郎さんもそうですね。こうやって集まっている人と一緒にビジネスやコミュニティ活動をやることが自分への大きな刺激となっています。

今は病院食の配膳のトレーサビリティを確保するプロジェクトを手掛けています。リリース前なので詳しいことは言えないのですが、病院食をどう効率的に作るかということだけではなく、どのくらい食べてもらえたのか、どういうものが必要とされているかというデータを次の病院食の配膳に生かすことにチャレンジしています。また、災害発生時に設置される避難所の物資を集計管理するようなシステムも手掛けています。災害発生時にできる避難所ですから、電気や通信回線もまともにないような状況でどのようにシステムを作り上げるかが課題です。また、システムに関する知識のない人にも使えるものでなければなりません。今、取り組んでいるプロジェクトでは「使用環境の制限がある中でどうやるか？」ということが大きなチャレンジです。

●会津でEJの仕事をしつつ、IPAのお仕事をされています。IPAの金子さんとしてはセキュリティ・キャンプ⑨でお会いすることが多くあります

IPAには月に4日ほど勤務しており、現在はセキュリティ・キャンプグループに所属し、セキュリティ・キャンプの事業に関わる業務を担当しています。具体的には、裏方スタッフとしてキャンプ事業が滞りなく進められるようにお手伝いをしています。最近では、キャンプ卒業生を対象としたワークショップも担当しています。キャンプに興味を持って参加してくれた学生の継続的な教育が目的です。

── 先ほどお名前が出てきた岡田良太郎さんと一緒にやっている「Hardening Project」⑩にも参加していただきました。確か、2013年の「Hardening One Remix」に初参加ながら、見事優勝されました。⑪⑫

当時、岡田さんから山寺に「こういうイベントがあるんだけど、参加してみないか」というお誘いがあったようです。山寺としては他流試合の経験を積ませる目的で、EJのメンバーを送り込むことにしたそうです。実はHardening Projectというイベントは知らなかったのですが、日常業務の延長と考えて、なんとかなるのではないかと思って参加してみました。実際に参加してみたら、次から次に攻撃が発生してんやわんやになって、目についた問題を片っ端から片付けているうちに競技が終わっていました。一緒にチームを組んだ他社の2人が過去のHardening Projectの参加経験者だったこともあり、いろいろと助けていただき、優勝することができました。

今度淡路島で行われるHardening 2017 Fes⑬でも優勝するべくチームメンバーと準備をしています。今度は社長と一緒にアルバイトの学生3人を連れて会津から淡路まで乗り込む予定です。前回参加したときと同じメンバーが2名いますので、また優勝したいですね。⑭

── 頼もしいですね。ぜひとも優勝を狙っていただきたい。このインタビューが誌面化される頃にはHardening 2017 Fesは終わっていますので結果が楽しみです。今後、学生に向けてやっていきたいことがあれば教えてください。

今後は「セキュリティ技術の面白さ」「CTFの面白さ」の両方を伝えていきたいと思っています。もともと「システムに対してこんなこともできるのか」という攻撃者の考え方に刺激を受けたことでセキュリティ技術を面白いと思うようになりました。普通にシステムを作っているだけでは出てこないような発想がとてもユニークで、この魅力を学生にも伝えたいと思っています。セキュリティに興味を持つ学生が増えて、その技術を使ったシステムで社会を安全にしたいと思って日々活動しています。

インタビュアー：川口 洋
（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）

「すごうで」のその後…　学生に対する支援活動の意義

⑦ システム管理者権限で作業をするためのUnixコマンド
⑧ セキュリティにおける次世代の育成〜被災地 福島からできること〜http://www.nisc.go.jp/security-site/month/h26/columu/20150318_01.html

⑨ https://www.ipa.go.jp/jinzai/camp/　⑩ https://wasforum.jp/hardening-project/
⑪ 優勝は会津若松市のITエンジニア集団：管理を無茶振りされたサーバを守り抜け！ Hardening One Remix開催 (1/2) - @IT
http://www.atmarkit.co.jp/ait/articles/1307/17/news092.html
⑫ Hardening One Remixに参加してきました - Eyes, JAPAN Blog　http://www.nowhere.co.jp/blog/archives/20130719-155220.html
⑬ https://wasforum.jp/hardening-project/hardening-2017-fes/　⑭ 取材時点はHardening 2017 Fes開催前。2017年11月23日〜25日に開催。

ラックの顔

第5回

同性からのサポートがセキュリティ業界で働く女性の未来を創る

比較的新しい産業であるIT業界は、他の職種に比べて男性の比率が高いという特徴を持つ。中でもその傾向がひときわ強いセキュリティの分野で、コンサルタントやアナリストとして働く鈴木悠と青羽真利は、社内外を問わず多様な場面で女性のセキュリティ人材に対する支援活動を行っている。日々の業務だけでも多忙を極める彼女たちが、女性の人材育成に注力する理由はどこにあるのか。活動の目的と、信念を聞いた。

文系でもセキュリティ業界で活躍できるという「気付き」が自信に

「読書が好きで、将来は本の道に進みたいと考えていた」という鈴木がセキュリティの世界に足を踏み入れることを決めたのは、高校生の頃だったという。「当時は、Windows95、98、と画期的なOSが発売され、パソコンが急速に普及し始めた時期でした。それを目の当たりにし、これから物事がどんどんデータ化していく、ITが将来的に拡大していくんじゃないか、そう思ったんです（鈴木）」

とはいえ、「壊滅的に数学が苦手だった」という鈴木は大学進学時に理系に進むという決断ができず、大学では心理学を専攻。卒業後に専門学校でネットワークセキュリティについて2年間学ぶという珍しいプロセスを経て、ラックに入社した。入社後は、テクニカルコンサルティング部で、セキュリティアセスメントやシステム構築のためのガイドラインの作成、国内外のセキュリティの調査研究など、幅広い業務を経験。コンサルタントという職種には、圧倒的な知識量が必要となるが、文系出身ということもあり、特に技術の面において不安があったという。「ただ、1年ほど経った頃、プログラムを完璧に書くことができなくても、読むことができ、変更すべき箇所が判断できれば問題はないと気付きました。なんとかこの世界で生きていけそうだ、そう思えるようになったのはその頃です（鈴木）」

現在もセキュリティコンサルティング部に所属し、顧客のセキュリティ基準やガイドライン、ポリシーなどを最新の技術に合わせて改定する仕事に従事している鈴木。顧客に対して不安やニーズをヒアリングしたり、それに対するアウトプットを出したりと、コミュニケーションの面では文系出身の利点が生かせているという。「長い文章を書くことにも比較的慣れています。過去には、厚さ11センチもの報告書を書いたこともあるんですよ（鈴木）」

技術面での不安は知識で払拭し、常に挑戦を続ける

入社4年目を迎えた青羽も、鈴木と同様に文系出身だ。「情報セキュリティやITに関する知識は全くといっていいほど持ち合わせてはいなかった」という青羽がこの業界に進むきっかけとなったのは、就職活動を通じて国際訴訟支援を手がけている企業に出会ったことだ。「その会社がコアな技術として活用していたのがフォレンジックやe-ディスカバリ。当時の日本では、まだあまり聞かない技術で、希少価値がありそうだと興味を持ちました（青羽）」

大学卒業後、青羽はその企業で1年半ほどコンピューターフォレンジックの技術者として業務に従事する。知識を持たないままにセキュリティ業界へと飛び込み、技術職に当たることにはずいぶん高いハードルがあったのではないかと推察されるが、「一通りのトレーニングはありましたし、調査のメインは高度な技術が問われるマルウエア解析といったものではなく、監査寄りの不正調査というフォレンジック分野の中では入りやすい種類のものだったので、なんとか挫折せずに続けられていました」と青羽はほほ笑む。

仕事を通じ、サーバーやネットワークに関わる部分にまでスキルの幅を広げたいと感じ始めた青羽が見つけたのが、ラックだった。鈴木と同じく技術への不安があったというが、「一から育てる」という採用メッセージに背中を押され、セキュリティアナリストとして入社。3年間、顧客のセキュリティオペレーションセンターでアナリストとして勤務した後、現在はラック本社のJSOC（Japan Security Operation Center／セキュリティ監視・運用サービスの拠点）のアナリストとして活躍中だ。「ラックの技術者はとてもレベルが高く、自分がどこまで勉強すれば追いつけるのかは未知数なので、不安は今でもゼロではありません。それを埋めるため、プライベートの時間をうまく活用し、資格取得も含め、知識を拡充していくことで自分の自信につなげています（青羽）」

同性ならではの配慮がなされたCTF for GIRLSのワークショップ

鈴木と青羽が現在、企業の壁を越えて取り組む女性セキュリティ人材の支援活動が、CTF for GIRLSだ。CTF for GIRLSは、情報セキュリティ技術に関心を持つ女性を対象としたコミュニティで、CTF（Capture The Flag／情報セキュリティ技術を競う競技）のワークショップや、CTFイベントなどの開催・運営を行っている。

CTF for GIRLSの立ち上げは、国内最大のCTF大会を開催するSECCON実行委員会の女性メンバーによる「日本国内に存在する、数少ない女性技術者を盛り上げるコミュニティをつくりたい」という声からスタートした。SECCON実行委員会に所属するラックの男性社員が、その企画を社内の女性社員に展開。鈴木と青羽はそれに賛同する形で運営メンバーの一員となった。「CTF for GIRLS立ち上げ前の2013年は、CTFの経験がある女性技術者は国内でも数えるほどしかいなかったと思います。私は社内の同期メンバーでつくったチームでCTFに参加していたこともあり、興味を持ちました（鈴木）」

CTF for GIRLSの最初のミーティングには、さまざまな企業や組織から6名が集まったが、そのうち半数の3名がラックの社員だったという。「企業によっては、情報を外部に出すことに抵抗があったり、上司の理解が得られにくかったりと、社外での活動にリソースを割きづらいということもあるようです。その点ではラックは、社外での活動に対して非常に寛容で動きやすいと感じています。また、ラックの女性は比較的、積極性が高いということもあるかもしれませんね（青羽）」

2014年の6月に、「20名くらい参加者が集まれば」という期待を込めて開催した第1回のワークショップは、募集開始の翌日に参加の応募が50名を突破。3日間で80名を超える参加申し込みがあり、運営

鈴木　悠
haruka suzuki

青羽真利
mari aoba

スタッフからはうれしい悲鳴が上がったという。

ワークショップの開催に当たって、運営サイドでは「初心者向けの内容を基本とすること」と「気軽に質問できる態勢を取る」ことの2点に配慮しているという。「CTF for GIRLSのワークショップの参加者は、学生や、CTFになんとなく興味があるという方、セキュリティ関連の製品の営業をしている方など、技術者に限りません。そのため、出題レベルは基本的に初級のものとしています。ワークショップの構成は、前半が講義、後半は講義の内容を応用した演習問題を解く時間になっていますが、後半は、スタッフが会場を歩き回って質問をしやすい環境をつくっています（鈴木）」

この2点の配慮は、「女性限定」のCTFコミュニティという観点において非常に大切な要素だ。女性のCTF経験者がまだまだ少ない現在、一般に開催される勉強会などではどうしても男性の比率が高くなり、レベルも上がりがちだ。大勢の男性の中に混じってそういったイベントに参加することは女性の心理的負担が大きく、また積極的に手を挙げ質問をすることに対してもレベルと性別、双方の面でハードルが高い。そういった、「同性ならではの悩み」に裏打ちされた配慮なのである。「休憩時間中にスイーツが提供されるというのも女性ならではのコミュニティの特徴ですね。スイーツがあると参加者同士のコミュニケーションが深まりますし、ツイッターやインスタグラムなどのSNSへの投稿も増えるので、毎回運営スタッフが気合いを入れ、味だけでなく“インスタ映え”も意識したスイーツを選んでいます（笑）（青羽）」

国境を超え、ますます多様化するCTF for GIRLSの活動

4年目を迎えるCTF for GIRLSの活動は、さらに進化しつつある。「平日の夜は大学の講義があって参加ができない」「交流会に出席したいが夜が遅くなるので難しい」といった学生の声から生まれた、学生限定のワークショップ「CTF for SchoolGIRLS」や、国内初の女性限定CTF大会「攻殻機動隊REALIZE PROJECT×SECCON CTF for GIRLS（攻殻CTF）」など、進化の仕方も多様だ。2017年11月に開催された第3回の攻殻CTFは、海外からの参加者も多数あり、国際CTF大会としてさらなる飛躍を遂げた。「韓国や台湾など海外にも、積極的に活動をしている女性のCTFコミュニティがあります。今後はこういった組織とも連携し、国際コミュニケーションを深めていきたいと考えています。また、第3回の攻殻CTFで3位にランクインした韓国からの参加者は、将来ラックで働きたいと話していました。あくまで社外での活動ではありますが、優秀な技術者とラックとの接点をつくることができたという点でも、会社にとって良い成果を生み出していると思います（青羽）」

また、2017年春には、テレビドラマにハッカー役として登場する女優に、ハッキングシーンのパソコン所作担当として現場指導も行った。取材への対応や、「女性のセキュリティ人材の育成」をテーマとした学会誌への寄稿など、イベントの運営だけでなく対外的な広報活動も活発化しているという。

鈴木 悠
haruka suzuki
ITプロフェッショナル統括本部
エンタープライズ・セキュリティサービス事業部
セキュリティコンサルティング部 第一グループ

2006年ラック入社。セキュリティコンサルタントとして、お客さま環境におけるさまざまなセキュリティ関連支援を行う。2014年にCTF for GIRLSの立ち上げに参画し、運営メンバーとして活動。現在は業務の傍ら、大学時代に専攻していた心理学の知識を活かし、人の脆弱性を狙った攻撃手法であるソーシャルエンジニアリングの国内外調査研究をしている。私生活では、6歳と2歳の2児を育てる母。

女性のセキュリティ人材増加のため、長期的な視点で活動を続ける

また、青羽は社内でも女性の人材育成を掲げた活動をしている。それが「ラック女子部」だ。「ラックには優れた女性のセキュリティ人材がたくさんいます。そういった方に話を聞いてみたいと常々思っていましたが、せっかくであれば大勢で聞いた方がよいではないかと思い、立ち上げたコミュニティです。ランチタイムを活用して2、3カ月に一度のペースで、女性社員から簡単なプレゼンテーションをしてもらっているのですが、現状では部活のようなカッチリとした組織ではなく、口コミを中心としたゆるい体制で運営しています（青羽）」

プレゼンテーションのテーマは技術に関わる内容に限らず、資格の取得やワーキングマザーの働き方についてなど幅広く、鈴木も運営をする側の社員として参加している。参加者も、セキュリティに携わる人間だけでなく、SIや管理部門のスタッフなど、多岐にわたるという。

CTF for GIRLSとラック女子部、ともにセキュリティ業界で働く女性に特化した活動だが、鈴木は「決して“女子会”をやっているわけではない」と強調する。「私たちの趣旨は、単に女性だけで集まって楽しもうということではありません。女性が女性をサポートすることで、女性を勇気付け、自信を持って次のステージへ進んでもらう、それが目的です（鈴木）」

自身も2児の母親である鈴木によると、セキュリティ業界、特に技術職におけるワーキングマザーの数は極めて少ないという。そこには、セキュリティがビジネスとして起こり始めた当初、そこに参入した女性の数が非常に少なかったこと、そして彼女たちがようやく、子育て世代を迎えているという時代背景がある。「セキュリティ業界では、これから続々とワーキングマザーが増えていくでしょう。ロールモデルが増え、それに比例してこの業界に入ってくる女性が増える――。そういったよい流れを生み出すことが、私たちの活動の狙いです（鈴木）」

実際、CTF for GIRLSのワークショップでは、運営スタッフが子どもを同席させ、会場内で一緒に過ごしながら講師として登壇するという試みも行われている。今後もこういったトライを積み重ね、今後は参加者が子どもを連れて参加できるように託児の態勢を整えるといった、「女性にとってより参加しやすい」運営手段を取ることも視野に入れているという。

「女性技術者の数を増やすためには、まず“この仕事に就きたい”と多くの女性に思ってもらうこと、つまり幼い頃からセキュリティに触れてもらうことが重要だと思っています。一方で、“技術者になりたい”という子どもの思いを理解していただくためには、親の世代にもセキュリティを知ってもらわなければなりません。セキュリティについて親子で見聞きし、体験できる機会を増やして、将来的な女性の人材を生み出す。私たちの活動が、そういったサイクルの一翼を担えたらうれしいですね（鈴木）」

青羽真利
mari aoba
ITプロフェッショナル統括本部
サイバーセキュリティ事業部 JSOC アナリシスグループ

2013年ラック入社。前職では不正調査を主としたフォレンジックに従事する。現在はセキュリティアナリストとして、お客さまのプライベートSOCやラックのセキュリティ監視センターJSOCにおいてお客さま環境の監視業務を務める。鈴木と同じく2014年からCTF for GIRLSの立ち上げに参画し、活動。他、(ISC)2 Japan Chapterの女性コミュニティ活動にも携わる。

サイバー・グリッド・ジャパンは、高度に巧妙化するサイバー攻撃とそれによる被害発生を防ぐため、2014年に発足しました。

「サイバー・グリッド・ジャパン」という名称には、複数の企業・組織が連携し、防御の「網（グリッド）」を張り巡らせることによりサイバー攻撃から日本を守る、という意味が込められています。すなわち、我々サイバー・グリッド・ジャパンにとって、社外の組織との連携（オープンイノベーション基盤の構築）は重要なミッションです。

社外組織との連携の形態として、共同研究開発のほか、企業や政府機関、地方自治体との協働で取り組むサイバーセキュリティの啓発活動や、業界団体等を通じたセキュリティの普及活動も、サイバー・グリッド・ジャパンの主要な活動の一つです。これらの活動の対象には、ITの利用者はもちろん、セキュリティ関係者も含まれます。セキュリティ関係者とは、今まさにセキュリティ対策の必要性に直面している組織の担当者や、将来のサイバーセキュリティを担う若手技術者等を指します。セキュリティ関係者に当社の知見を提供することにより、セキュリティを担う人材層の厚みが増し、ひいては日本のサイバーセキュリティレベルの向上につながります。この「セキュリティ関係者を対象とした普及啓発活動」が、サイバー・グリッド・ジャパンの人材育成活動の成り立ちです。

昨今のサイバーセキュリティのニーズの高まりと、サイバーセキュリティ人材の不足という情勢を受けて、今年度のサイバー・グリッド・ジャパンは、人材育成を研究開発や啓発活動と並ぶ主要活動として位置付けました。本誌で紹介したような活動を通じて、セキュリティ人材の裾野を広げ、当社とともに日本を守る「グリッド」を作る仲間やパートナーが増えていくことを期待しています。

サイバー・グリッド・ジャパンは、ラックの長年の経験・技術力を結集し、産官学連携を通して、ICT環境を強く、安全に進化させ、日本の発展に寄与すべく邁進いたします。

CYBER GRID JOURNAL VOL.5

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