SHIELD Security Reserch Center

Hisys Journal

VOL.11

HITACHI
Inspire the Next

株式会社 日立システムズ

Hisys Journal VOL.11

TABLE OF CONTENTS

●はじめに

本文書は、株式会社日立システムズ セキュリティリサーチセンタが運営するセキュリティ情報サイト、S.S.R.C.(Shield Security Research Center) の公開資料です。本サイトでは、本文書のバックナンバーをはじめ、S.S.R.C. によるリサーチ結果などを随時公開しています。
S.S.R.C. http://www.shield.ne.jp/ssrc/

●ご利用条件

本文書内の文章等すべての情報掲載に当たりまして、株式会社日立システムズ（以下、「当社」といいます。）と致しましても細心の注意を払っておりますが、その内容に誤りや欠陥があった場合にも、いかなる保証もするものではありません。本文書をご利用いただいたことにより生じた損害につきましても、当社は一切責任を負いかねます。
本文書に記載した会社名・製品名は各社の商標または登録商標です。
本文書に掲載されている情報は、掲載した時点のものです。掲載した時点以降に変更される場合もありますので、あらかじめご了承ください。
本文書の一部または全部を著作権法が定める範囲を超えて複製・転載することを禁じます。

さまざまな視点からセキュリティ人材育成について語る

宮本久仁男 インタビュー

Kunio Miyamoto

取材・文・撮影＝斉藤健一

人材発掘に貢献するセキュリティキャンプ

斉藤（以下 S ）：本日はお忙しい中、時間を割いていただきありがとうございます。今回は、主にセキュリティキャンプ（以下キャンプ）のことや、宮本さんが考えるセキュリティ人材像などについて話を伺っていきたいと思います。よろしくお願いします。

宮本（以下 M ）：こちらこそ、よろしくお願いします。

S では早速、キャンプについて伺います。今年も 8 月に全国大会が開催される予定です。宮本さんはこれまで講師 WG 主査として、そして今年からは企画・実行委員長という立場でキャンプに携わっておられます。まずはこれまでキャンプを実施してきた成果といいますか、セキュリティ人材育成でどのように貢献してきたか、お考えを伺いたいと思います。

M キャンプは、10 代前半から 20 代前半の若い世代で、やる気のある人たちを発掘することに貢献できていると考えています。発掘とは育成の前の段階です。単に育成といっても、育成対象となる人材がいなければ意味がありません。そこで参加人数に限りはありますが、キャンプというイベントを継続して実施することで、セキュリティに興味を持つ人たちに出てきていただこうとなったと考えています。もちろん、これは私一人の力で

は全くなくて、初期の立ち上げに尽力いただいた方々、協力していただいた講師・実行委員・事務局の方々をはじめ、セキュリティ業界内でキャンプについて意見をくださる方々など多くの人のおかげだと感謝しています。

S 確かに。キャンプ卒業生がその後セキュリティ業界で活躍する例は多数ありますから一定の成果はあったと私も感じています。続いての質問ですが、宮本さんから以前、キャンプの目的の１つについて伺ったことがあります。それは、セキュリティに興味を持っている若い世代は、往々にして共通の話題を持つ友人がいないことから、学校などのコミュニティで孤立しているケースが多い。キャンプでは彼らのコミュニティを作りたい、というものでした。この点についてはいかがですか。

M 当然のごとく、こちらも全員というわけには行きませんし、細かな地域コミュニティというところまで発展しているかどうかわかりませんが、日本横断や、限定された範囲ではあるものの国際交流といったレベルでのコミュニティ形成ではおおむね成功していると思います。例えばキャンプの同期という横のつながり、チューターを務めるキャンプ卒業生や講師といった縦のつながりなどがあります。また、それらのつながりと関連するコミュニティもありますから、コミュニティは徐々に大きくなっています。さらに、コミュニティの中に優れた人材や面白い人材がいると聞けば、周りから人が集まってきます。そして、このサイクルは順調に動いていると思います。

●宮本 久仁男（みやもと・くにお）

NTT データに在籍。社内では NTT データグループを対象とする CSIRT である NTTDATA-CERT のメンバーとして活動する一方、セキュリティ・キャンプをはじめとする若年層の人材を発掘・育成するプロジェクトにも深く関わる。2011 年 3 月に博士（情報学、情報セキュリティ大学院大学）取得、2014 年 3 月に技術士（情報工学部門）登録。

フォローの役割を果たす地方大会とジュニアキャンプ

S 次に、地方大会について伺います。先ほどの回答でキャンプ全国大会の参加人数の制約について触れられていましたが、地方大会は人材発掘の取り組みを広げることを目的に開催されているのだと思います。個人的にユニークだと感じたのは、本年 5 月に高知で行われたジュニアキャンプの合宿講座です。参加者を中学生に限定しましたが、この意図についてお聞かせください。

M 残念ながら、私自身、高知のジュニアキャンプには直接的に携わってはいないのです。ただ、本件のキーパーソンに伺ったところ、全国大会・地方大会とも主な参加者は高校生・大学生であり、下の世代が参加できるものを企画したかったとのことです。高知高専の先生方にもご協力いただき、多くの中学生に集まってもらえたとのことで、一定の成果はあったと認識しています。

S キャンプ全国大会の応募に際して、中学生はやはり不利ですか。

M そうですね。応募時点の経験や知識・スキルなどを比較すると、中学生よりは高校生、高校生よりは大学生の方が豊富であることは否めませんから。もちろん、将来性に期待して中学生に参加してもらうこともありますが、その将来性を上回るほどの知識やスキルを持った高校生・大学生がいたとすれば、選考ではそちらが有利になると思います。ただ、全国大会の選考で見た感じですが、高校生・大学生顔負けの知見や技量を持つ中学生も少ないながらいます。そういう人たちがもっと出て来てくれればとも感じています。

S ジュニアキャンプはそういった若年層をフォローする意味合いもあるのですね。

卒業後も成長できるチューター制度

S キャンプではかつての卒業生をチューターとして招き入れています。この仕組みもチューター自身のスキル形成などに役立っていると思うのですが、いかがでしょうか。

M チューター制度は開始 2 年目から取り入れました。出発点は、何かしらの形で卒業生をフォローアップしたいという思いからでしたが、ちょうどその頃はキャンプ運営を手伝ってくれる人が不足していたので、チューターとして参加してもらうことにしました。この点で言えば成果はあったと思います。ところが、数年経った時点で、ある問題に気が付きました。キャンプの卒業生は毎年一定の数で増えていて、現在は 400 名を超えています。チューターも応募制ですから、その選考には苦労しています。

S チューターも応募制だとは知りませんでした。倍率はどの程度なのでしょうか。

M ここ何年かは数倍程度で推移しています。チューターの場合、講師のサポートや参加者への配慮など、セキュリティの知識やスキル以外の要素も求められますから、年々ハードルは上がっているように感じます。ただ、こういった経験を積むことによって、エンジニアとしてより成長できるとも思っています。

S チューターでも人数の制約の問題があるのですね。

M はい。もっとも、ミニキャンプなどの地方大会もありますから、講師やチューターとしてそちらの運営をサポートしてくれる人を募るなどしてフォローしています。

クラス制からトラック制へ

S そういえば、今年からキャンプでは講義の体制が変更になりますね。これまでは「ネットワーク」「Web」「ソフトウェア」などジャンル別のクラス制でしたが、今年からはジャンルを超えて好きな講義を受けられるようになります。これにはどのようなお考えがあったのでしょうか。

M クラス制自体はこれまでうまく機能していたと認識していますが、他の分野やクラスで扱うテーマを外れた場合のフォローアップに制約がありました。今年からは上野宣氏に講師 WG 主査をお願いすることとなりましたが、上野氏は面白い考え方の持ち主で、寿司屋のカウンターのように参加者の前に講義という「ネタ」をいくつも並べておき、自由に選べるようトラック制に変更しました。参加者に興味の幅を広げてもらおうという狙いがあります。また、これによってさらなる多様性も生まれると思います。もちろん、これまでのクラス制のように同じジャンルの講義を受けることもできます。

S よいアイデアだと思います。

M 複雑化するサイバー脅威に対するセキュリティを考える上で、特定の専門分野に加えて、聞きかじり程度であっても早い時期から幅広い分野の知識や考え方に触れておいた方がよいと私自身も考えていますから、トラック制には期待しています。

セキュリティ人材に求められるマインド

S 今度はテーマを変えてセキュリティ人材について、技術者としての宮本さんに意見を伺いたいと思います。現在、日本において 8 万人ものセキュリティ人材が不足していると言われています。個人的には数字ばかりが注目されており、求められる人材像などがメディアで語られることは非常に少ないと感じています。スキルの面では ISOG-J と OWASP Japan が共同で取り組む「脆弱性診断士スキルマップ」※などの指標が出てきていますが、それ以外の面、例えばマインドなどで何かお考えはありますか？

M あくまで個人の見解ですが、モチベーションを持ち続けることが大事なことだと考えています。そのためには、対象への「こだわり」や「思い込み」があった方がいいと思います。こだわりを持っていれば、その事柄には積極的に関わっていくようになりますし、思い込みがあれば、周囲の意見に左右されることなく突き進むことができます。例えば、常識外れだと周囲からの反対に遭ったとしても、思い込みを貫き通し完成させたシステムやソリューションが常識そのものを変えていくこ

※ **脆弱性診断士 (Web アプリケーション) スキルマップについて（PDF 形式）**
http://isog-j.org/output/2014/about-pentester-web-skillmap-201412.pdf
脆弱性診断士 (Web アプリケーション) スキルマップ Ver.1.0（PDF 形式）
http://isog-j.org/output/2014/pentester-web-skillmap-201412.pdf

とだってあり得るわけです。ですから、こうした気概は持っておいてほしいと思います。それに、きちんと動いて役立ちそうなものが目の前にあると、反対している人の見方や意見も変わってくるように思います。

S 確かにおっしゃるとおりだと思います。

M 余談ですが、こだわりや思い込みは、それぞれ「オタク」や「中二病」の特徴でもあります。ですから「成長するにはオタクや中二病の気質が必要だ」とも言い換えられますね（笑）。

S それは面白い意見です（笑）。

組織に必要な調整役という存在

S 次に視点を変えて、組織全体から見た人材像について伺いたいと思います。宮本さんから見て、現在組織で求められる人材について、何かご意見はありますか。

M セキュリティでいえば、必要な人材についてはおおまかに「技術者」「インテリジェンスアナリスト」「オーガナイザー」が考えられると思います。ただ、それぞれの職種の立場や役割がきっちりと区切られてしまうと、かなり窮屈な組織になってしまうとも思っています。ですから、職種の枠を超えて間を取り持つ「調整役」のような存在も必要だと感じています。日本ではオーガナイザーが調整役も務めることが多いのですが、組織を統括して向かうべき方向を指し示しつつ、メンバーの調整も行うというのは、大変なことだと思うのです。

S よくわかります。

M おそらく、調整役のイメージとしては、軽いフットワークや幅広い人脈、そして自身が持つ情報や見識をもって動きまわる感じです。そして時には、組織内にいるだけでは知ることができない外部の情報を伝える役割も持っています。語弊があるかもしれませんが、個人的にはこれを称して「遊び人」とか「吟遊詩人」などと呼んでいます（笑）。

S なるほど（笑）。これも先ほどと同様に面白い例えですね。ところで、「遊び人」や「吟遊詩人」になるにはどうしたらよいでしょうか。

M 知識を持っているだけではなれませんし、経験だけでもダメ。総合知識をもって歩き回っていると、経験が知識を生み、知識が経験を連れてくる。そしてこれを支えるためのモチベーションも重要だと思います。まずは、勉強会などに積極的に参加して、さまざまな知見に触れてみるのがよいと思います。

S 道のりはなかなか険しそうですが、挑戦する価値はありそうですね。

自らも強いモチベーションを持って さまざまなことに挑戦

S ここからは宮本さんご自身について伺いたいと思います。最近、宮本さんは技術士の試験に合格されたとお聞きしました。また、以前は博士号を取得されるなど、公私含めて積極的に活動されています。こういった活動は、これまで伺った「モチベーション」の話に通じるように思えるのですが、いかがでしょうか。

M 全くそのとおりです。博士号は、以前からチャンスがあれば取りたいとは思っていたのですが、幸運なことに、2005 年頃、会社から打診があって機会を得ることができました。大学院ではセキュリティの研究を行っていたのですが、その当時、大学をはじめとする学術の世界と企業などの実務の世界とではかみ合わない部分があるように思えて、この間を埋めるために何かしたいという思いがあったのです。また、セキュリティも情報科学に属する部分がありますから、これに真剣に取り組みたいという気持ちもありました。

S 技術士の方はどうでしょう。

M 将来を 10 年〜 20 年というスパンで考えたときに、情報システムを作る人たちに何らかの資格が課せられるのではないかと思ったのがきっかけです。話は変わりますが、建設業の世界では、設計においても施工においても、仕事を進める上でさまざまな資格が求められます。その中で技術士はメジャーな資格の 1 つです。そして、今後成熟していく ICT の世界も、もしかしたら建設業の世界のようになっていくのかもしれないと考えたのです。これはあくまで個人的な予測であり、自分自身、今後 10 年〜 20 年後も仕事を続けていくのかという話もありますが、考えたことを何かしらの形で示したいと思ったのがモチベーションになっ

ています。

S 私も、この取材の前に技術士について少し調べてみたのですが、建設業界ではメジャーな資格ですが、情報の世界ではそれほどメジャーではないことがわかりました。ちょっと不思議に思っていましたが、お話を伺い納得しました。ところで、宮本さんのモチベーションの源泉はどこにあるのでしょうか。

M やはり「自分の興味」に尽きるのだと思います。自分の活動を振り返ると、関わっているのはすべて興味ある分野です。会社の業務もやりがいがありますし、キャンプの場合は、開催期間中の参加者の成長ぶりを見続けたいとも思っています。例えば、イベントでは、参加者・演者・主催者などいくつかの参加形態がありますが、より中心に近い位置にいる方がより大きな楽しみを得られると思うのです。そして、より中心近くに居続けるためには、自分の腕を磨き続けなくてはなりません。また、「自分が楽しむ」というと手前勝手に聞こえるかもしれませんが、自分が楽しむには、当然、周囲がよい方向に向かって進んでいることが重要になります。ですから、自分ができるところは積極的にお手伝いするというスタンスなのです。

ベテランと若手が「共創」できるコミュニティ作り

S 最後の質問になりますが、セキュリティ業界の年齢構成について伺ってみたいと思います。セキュリティ業界で活躍している人たちを見ると 40 代の方々が多いように思えます。一方、オープンソースの世界など他のコミュニティでは 20 代が中心になっているところもあるそうです。業界やコミュニティの高齢化に関して、宮本さんはどのようにお考えですか。

M 40 代を高齢と呼ぶには語弊があるので、ここではベテランという言葉を使わせてください。まず、業界やコミュニティの年齢構成ですが、若い世代の人たちが入ってくれば、相対的にベテランの割合は減ることになります。キャンプや SECCON などの取り組みには、若い世代の人たちに出てきてほしいという思いがあります。他にもセキュリティ業界では若手の技術者を支援する取り組みを行っていて、徐々にではありますが成果は出ていると感じています。あと、若手を育成するといっても、知識やスキルを継承するにはベテランの方の協力なくしてはできないと考えています。

S 確かに。教える側・教えられる側の両方がいないと育成は成り立たないですね。

M あと、ベテランの方には、若い世代の人たちを不当に排除するのはやめてほしいと思います。例えば「若手はすっこんでいろ!」といった、頭ごなしというか上から目線のような姿勢です。もちろん、お互いが時には楽しんで、時には本気で競い合うのはよいと思います。おそらく、ベテランになるまでには、酸いも甘いも噛み分けていると思いますから、獲得した知見は相当のものがあることはわかります。ですからそういった知見は、若手へのスキル継承などに役立て、悪い意味での競争ではなく「共創」ができるようになるといいですね。

S 共創とは言い得て妙ですね。

M 話は少しそれますが、ベテランの方が第一線を退いた後のコミュニティとの関わり方にも興味を持っています。セキュリティ関連の仕事や業種が成立したのは最近のことですから、将来の姿が見えないと思うのです。まだ、漠然としたアイデアレベルですが、現役を引退した方々が地域のコミュニティでセキュリティの相談役になるのはどうだろうと考えています。ちょうど現役を引退された医師の方々がボランティアとして医療相談に携わるような形です。

S 一般ユーザーへの脅威も拡大してきていますから、そういった相談が地域でできるようになるとよいですね。

M はい。ただ、理想を言えば、現在のようにセキュリティに多くの人員が必要とされる社会ではなく、社会やシステムに守る仕組みがあらかじめ組み込まれるようになるとよいと思います。実現は難しいとは思いますが。

S セキュリティ人材増という流れの中では見落としがちですが、本質を突いていると思います。インタビューを通じて示唆に富んだ数々の意見を伺うことができました。本日はありがとうございました。

ハッカーやセキュリティにまつわるニュースを独自の視点から捉える時事コラム

Threat Scope

#09 ディフェンダーのジレンマ

文＝エル・ケンタロウ

激化するサイバー攻撃、セキュリティ企業も標的に

サイバー攻撃による企業や組織の情報漏えい事件が後を絶たない。標的となった企業や組織の規模や業種もさまざまだが、日本年金機構のようにセキュリティポリシーや運用体制の不備といった意識の低さが情報漏えいにつながっている例も多い。

また、先日には政府機関などに監視ツールの販売を行っていたイタリアのセキュリティ企業である Hacking Team もサイバー攻撃を受け、機密情報が漏えいしたことが明らかとなった。

このように、どんな組織であっても被害に遭う可能性はあり、さらに報道されているのは氷山の一角でしかない。常に変わり続ける脅威状況の中で、企業や組織はセキュリティとどう向き合い、いかにして情報を守ればよいのだろうか？

企業のセキュリティ問題を明確に分析するレポート

軍事・政策・経済など多岐にわたって分析を行っていることで知られる米国ランド研究所は、この度『ディフェンダーのジレンマ：サイバーセキュリティへの道標』なるレポートを発表した。162 ページにもおよぶ本レポートでは、従業員 1000 人以上、売上が 100 億円以上の企業の CISO（最高情報セキュリティ責任者）18 名にインタビューを行っている。

他にも現在セキュリティ業界が提供しているさまざまなソリューションの有効性を検証したり、ソフトウェア業界が抱えるセキュリティ問題の分析を行ったりするなど、サイバーセキュリティに対して包括かつ発見的な研究（ヒューリスティックアプローチ）を行った。

レポートの内容は、セキュリティ業界関係者にとってはこれまで言われてきたことが多いだろうが、クライアント（ソリューションを導入する一般企業）が抱えるセキュリティに対する問題を明確に分析したものだと言えるだろう。

レポートではまず、セキュリティに対するクライアントの悩みや認識を紹介している。組織のセキュリティ体制は組織の業種や規模などにより異なるが、ベンダーが提供するセキュリティソリューションの多くは、中小企業には向いていないこと。組織内のネットワークを物理的に隔離することは状況によっては有効な策であること。社員が自身の端末を企業内ネットワークに接続するニーズは組織にとっての脅威状況の複雑化を加速させていること。CISO の多くはセキュリティを取り巻く現状は攻撃者優勢と考えていることなどだ。これらは従来セキュリティ関係者の間では共通認識として考えられていたことが間違っていないことを裏付けている。

また、多くのクライアント組織は自分たちがどのようなソリューション、インテリジェンスが必要か、またこれらのソリューションをフルに活用できるかどうか不安を抱えていることも明らかになった。

レポートではさらにクライアントの傾向にも言及している。

サイバー攻撃の被害に遭った際、知的所有権よりも組織の世評への被害の方が多くの CISO にとっては重大な問題であること。攻撃による被害状況把握の多くは完全とは言えないこと。多くの組織ではネットワーク侵入によるリスクの明確化と組織内の共有がうまく運用できていないことなどだが、この状況は今後も変化しない可能性が高

い。また、多くの CISO はセキュリティソリューションに予算を割く場合、SOC（セキュリティオペレーションセンター）のような人間が介在するソリューションを好むのだそうだ。

ランド研究所による組織のセキュリティへの提言

このようなクライアントが抱える悩みの多くは今までセキュリティ企業からは見えにくく、明確化できずにいた部分だ。これらの研究結果を受け、ランド研究所はクライアント側、ベンダー側へのサイバーセキュリティに関する改善案とフレームワークを本レポートの最後に提案している。

1. 組織内で防御が必要な資産の明確化、また対象資産がどれほどの防衛が必要か、明確にすべきである。
2. 組織全体としての防衛、ネットワーク境界線の防衛、内部の組織体制、情報管理などリソース分配を明確にし、最重要要素に注力できるようにする。
3. CISO の多くは政府機関への期待は低いが、政府機関は協力する体制を準備しておく必要がある（CISO の多くは、有事以前は政府側からの協力に対して懐疑的な見方をしているが、有事の際には政府との協力が重要という考え方を持つ傾向にある、とインタビューから判明している）。

レポートではセキュリティが抱える悲観的なパラドックスこそが実はセキュリティ向上への鍵であるとランドは締めくくっている。大規模な情報漏えい事件や、毎日のように増加し複雑化する脅威状況を受け、数年前に比べれば組織における CISO の重要性は認識されるようになり組織内での影響力も強くなってきている。この影響力と OS や各種ソフトウェアなどのセキュリティ機能の強化、セキュリティソリューションの多様化などによって、サイバー攻撃が成功するハードルは日々高くなっていることは確かだ。とはいえ、IoT がもたらす脅威状況の複雑化が予測される現状、さらにハッキングがビジネスとして確立してきていることから今後も攻撃者と企業・組織の攻防は続くだろう。

●参考 URL

- **The Defender's Dilemma: Charting a Course Toward Cybersecurity**
  http://www.rand.org/pubs/research_reports/RR1024.html