SHIELD Security Research Center

Hisys Security Journal

VOL.48

HITACHI
Inspire the Next

日立システムズ

Hisys Security Journal VOL.48

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. https://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。

© Hitachi Systems, Ltd. 2023. All rights reserved.

Human * IT

セキュリティのスペシャリストになるにはジェネラリストを目指せ！

ニール・グリフター・ワイラー インタビュー

Neil Wyler a.k.a. Grifter

インタビュー・サポート＋通訳＝エル・ケンタロウ
取材＋文＝斉藤健一

Black Hat や DEFCON といったコミュニティでグリフター（Grifter）の名で知られているニール・ワイラー（Neil Wyler）氏。現在は、IBM X-Force の Active Threat Assessments 部門の Global Lead を務めている。今回のインタビューでは、セキュリティの専門家として 20 年以上の経験がある彼に、セキュリティを仕事にすることやコミュニティとの関わり方、そしてハッカーに求められる資質について話を伺った。

セキュリティを仕事にするということ

斉藤（以下 S）：現在、日本ではセキュリティ人材が不足していると言われています。その一方で、セキュリティ業界は成熟してきており、それぞれの仕事の専門性が高くなり、より細分化する傾向があります。こういった状況の中で、若い世代はどのようにスキルを習得したらよいのか、また、組織はどのように人材を育成したらよいのか、セキュリティ業界で 20 年以上のキャリアを持つあなたのご意見を伺いたいと思います。

ニール・グリフター・ワイラー（以下 G）：それは非常に興味深い挑戦だと思います。かつてのセキュリティ業界は、趣味で調査・研究を行うホビイストがたくさんおり、そういった人たちで構成されていました。現在、セキュリティの仕事は以前と比べものにならないほど重要となっていますが、質問のとおり、人材は不足している状況です。この仕事の特徴の 1 つはストレスの高さです。給料を得るためだけにこの業界に居続けることは難しいと思います。情熱がなければ、早い時期に燃え尽きてしまうのではないでしょうか。

S セキュリティを仕事にするまでにどのような経

ニール・グリフター・ワイラー
（Neil Wyler a.k.a. Grifter）

IBM X-Force の Active Threat Assessments 部門の Global Lead を務める。セキュリティの専門家として 20 年以上の経験を持ち、脆弱性評価、ペネトレーションテスト、物理セキュリティ、インシデント対応に注力してきた。Black Hat Briefings のスタッフ、DEFCON のシニアスタッフとしても 20 年以上活躍している。Black Hat、DEF CON、RSA Conference など、世界中の数多くのセキュリティカンファレンスで講演を行っている。また、オンライン、印刷物、映画、テレビなどさまざまなメディアのインタビューに応じ、情報セキュリティに関する書籍も多数執筆している。また、DEF CON や Black Hat の CFP レビューボード、Black Hat Training レビューボードのメンバー、DC801（DEFCON の地域コミュニティ、801 は米国ユタ州ソルトレイクシティ）の創設者、地元のハッカースペースである 801 Labs の創設者として、多忙な日々を過ごしている。

緯がありましたか。

G セキュリティというかハッキングには若い頃から興味があり、今なら違法とされるような行為も過去にしたことがあります。私は裕福な家庭で育ったわけではありませんし、地域の環境も良いとはいえませんでした。ですから、そこから抜け出すため、学校卒業後に軍に入隊したのです。軍では戦闘機のジェットエンジンを整備するエンジニアをしていました。ですが、服務期間を終える頃、このまま軍に残るかどうか自問したとき、この仕事が本当に好きなわけではないということに気づいたのです。そこで、軍を離れる決断をしました。結局のところ、私が仕事にしたかったのは、コンピューターのハッキングのスキルだったのです。

S LinkedIn で経歴は拝見していましたが、軍に在籍していたのにはそうした背景があったのですね。

G 2000 年代初頭に会社を立ち上げましたが、当時はセキュリティだけではなかなか稼げない状況で、ネットワークの環境設定やコンサルティングなども請け負っていました。そのような中で、ネットワーク侵害にあった組織の調査・復旧・コンサルティングなどを地道に続けていくうち、人づてに評判が広がり徐々に仕事が舞い込むようになりました。今から考えると、こうした経験によって得たネットワークやコンピューター OS の知識がセキュリティの仕事にも大いに役立っています。

コミュニティへの貢献

S Black Hat や DEFCON のコミュニティとはどのようにつながりを持ったのでしょうか。

G Black Hat では現在、シニア・ネットワーク・オペレーション・リードを務めています。スタッフとして参加するきっかけは、DEFCON の Web フォーラムでした。当時、参加者の立場だった私は、Black Hat の参加費用が高いとさんざん文句を言っていたのです。すると、ラス・ロジャース氏（Black Hat・DEFCON の統括スタッフ）から、ボランティアスタッフとして参加してみないかと打診されたのです。それから数年後、Black Hat Europe を開催するために渡った欧州で、米国から輸送するはずだったネットワーク機器が届いていないというトラブルに見舞われました。原因は担当者のミスでした。機器がなければカンファレンス会場のネットワークを構築できません。私は急きょ機材集めに現地を奔走することとなりました。ですが、あいにくこの日は休日だったため、思うように集めることができず、カンファレンス・ネットワークも満足いくものを提供できませんでした。

S 聞いただけで顔面蒼白になりそうな凄まじい体験です。

Gその後、Black Hat のネットワークを担当してほしいと依頼されました。メンバーの選定も私に一任するというのです。当時のカンファレンス・ネットワークは、当たり前のように攻撃パケットが飛び交っており悪評が絶えませんでした。そこで、私は気の合うメンバー 2 名とネットワーク構築に挑みました。以前は開催期間中の約半分の時間はネットワークがダウンしているような状況でしたが、私たちが担当すると、この時間をわずか 15 分にまで減らすことができました。しかも、この 15 分というのは、あるトレーニング講師が Wi－Fi AP に対してゼロデイ攻撃を行ったという特殊な事案だったのです。こうした安定的な運用が評価され、その後も引き続き Black Hat のネットワークを担当し続けています。

S DEFCON に携わるようになった経緯は。

G Black Hat のときと同様です。最初は一参加者に過ぎませんでしたが、ラス・ロジャース氏からボランティアスタッフの誘いを受けたのです。まずは、来場者の整理・誘導から始まり、ベンダー出展エリア運営の手伝いなどをしてきました。自分で言うのも何ですが、その時々の仕事に私は熱心に取り組んできました。DEFCON 主催者であるジェフ・モス氏とも古くからの付き合いで、ある年にカンファレンスの部門リーダーになってほしいと頼まれたのです。私は、コミュニティのために引き受けることにしました。子供のころに趣味で始めたハッキングが、今では生活の糧となり家族を支えられるまでになりました。ボランティアスタッフとして活動したり、講演を行ったりすることは、私を育ててくれたコミュニティに感謝を伝えることであり、恩返しをすることなのです。

S DEFCON や Black Hat では長きにわたりボランティアスタッフを続ける人も多いのですか。

ユタ州ソルトレイクシティに暮らすニール・ワイラー氏とのインタビューはオンラインで行われた

G はい、もちろんです。中には DEFCON が始まったころから携わっている人もいます。DEFCON の魅力の 1 つは、参加した人の多くが、仲間や居場所を見つけられたと感じられる点にあります。参加者はコミュニティから受け入れられていると深く感じるのです。これは強いつながりです。ですから、スタッフとしてこの体験を提供する側に立つと、それを手放したいとは思わなくなるのです。DEFCON のようなイベントの運営はとても大変です。企画から開催までには多くの時間や手間がかかります。翌年の企画はイベントが終了した直後から始まります。古くからのスタッフの中には、次回を最後に引退しようと言う人もいます。ですが、実際にイベントに参加すると、引退はもう 1 年だけ先延ばしにしようと決心が鈍ってしまうのです。というのも、会場に行けば、長い時間をかけて作り上げた企画が目の前に広がっているわけですし、さらにその場にいる参加者たちの興奮も感じられるからです。これに勝る喜びはありません。次回もまたがんばろうと思うのです。

S 話はそれますが、CODE BLUE 2022 のあなたの講演※で、個人的に印象に残っている言葉があります。“I love Security, I live Security” です。これまでの話を伺い、この言葉がより深く腑落ちしました。

G 多くの人から他の趣味について尋ねられますが、セキュリティは仕事であり、趣味でもあるのです。もう、生き方と言ってもよいほどです。

ジェネラリストの視点とスレット・ハンティング

S CODE BLUE の講演について伺います。講演では、組織のネットワーク管理で見落とされたミスの事例が紹介されました。例えば、許可されていない FTP サーバーが実は稼働していたり、本番サーバー稼働後には終了させるべきテストサーバーが放置されたりしていたというものです。他にも、ネットワークの外に対しては堅牢だけれどもネットワーク内部のセグメントがフラットになっていて、1 度侵入を許せば後は自由に横展開できる例も紹介されていました。それぞれの組織にはセキュリティ担当者がいたはずです。彼らはなぜ気づくことができなかったのでしょうか、逆に、なぜあなたは気づくことができたのでしょうか。この違いはどこにあるのでしょうか。

G 組織の内部というのはトンネルの中のようで、

※ **CODE BLUE 2022「基調講演：サイバーセキュリティの圧倒的な課題を理解するために」**
アーカイブページでは講演動画やプレゼンテーション・スライドが公開されている
https://codeblue.jp/2022/result/?content=Neil_Wyler

全体が見えにくくなってしまうからだと思います。例えば、組織の文化、組織の属性、通常の運用方法といったことがバイアスとなり、ものの見方や考え方に影響を与えているのです。組織のバイアスに影響されない外部の人間の方が純粋にセキュリティの観点からネットワークを診断できるのだと思います。また、セキュリティ担当者の多くは、新たに発見される脆弱性のニュースには注目しますが、組織ネットワークの基礎部分に常に関心を持つ人はまれです。ですが、この部分が大きなインパクトを及ぼす事案につながるのです。

S そのとおりですね。

G また、先ほど、それぞれの仕事の細分化が進んだという話も出ました。各自の専門性が高くなるにつれ、自分がカバーしている技術分野には精通しているけれど、それ以外の分野はそれほどでもないという人たちが増え、全体像を見られる人が少なくなっているとも感じています。私のような古い世代の人間は、ネットワークの設定やサーバーの設定なども含めてセキュリティ全般に携わってきたので、広範囲に知識を得ることができました。ですので、担当者はセキュリティを確保するために、コンピューターの OS やネットワークのプロトコルなどについても十分な知識を得ておくべきだと思います。別の言い方をすれば、スペシャリストになりたければ、まずジェネラリストとして広範囲の知識をカバーすべきだと思います。

S ご自身の経験に基づいた含蓄ある言葉です。

G 現在、私は IBM X-Force でスレット・ハンティングを統括する部署に在籍していますが、このジェネラリストの視点はスレット・ハンティングをする上でも役に立ちます。

S スレット・ハンティングについて、簡単に説明していただけますか。

G スレット・ハンティングとは組織内の脅威を発見するプロセスの一手法です。従来であれば、SIEM などがネットワークやセキュリティ機器のログデータやアクティビティを収集して脅威となりうるものを通知していました。ただし、通知が発せられるためにはきっかけとなる侵害行為を検知しなくてはなりません。逆をいえば、通知が発せられなければ脅威を把握できないわけです。

S おっしゃるとおりです。

G これではセキュリティ運用がツールに依存してしまいます。先ほど、ネットワーク管理者が見落とした設定ミスを、私たちが見つけることができたという話をしました。その理由は、スレット・ハンティングにより、通知に頼らなくとも多くの状況を把握できていたからなのです。

S では、スレット・ハンティングにおけるジェネラリストの視点というのは、どのようなものなのでしょうか。

G スレット・ハンティングではセキュリティチームだけではなく、組織の IT 部門などとともに情報を収集し、議論を重ねて、知識を蓄積していきます。一例ですが、それは営業チームのノート PC にインストールされるアプリケーションについてだったり、ネットワーク設計の背景や経緯についてだったりします。こうして知識を積み重ねることによって、ネットワーク内で起きていることの見え方が変化してくるのです。これがジェネラリストの視点です。

S 日本では、スレット・ハンティングというと、とかく侵害指標（IoC）などに目が行きがちです。ですが、今回のお話を伺い、実はネットワークの通常時の動きを把握しておくことが重要なのだと感じました。

G そのとおりです。乱暴な言い方ですが、IoC は検索可能な情報です。むしろ、ハンターが注目すべきはアクターの TTPs（戦術・技術・手順）です。組織を狙う特定のアクターがいるならば、彼らがどのようなビジネスを展開し、どのような攻撃を仕掛けてくるのかを把握しておくことで、特定のファイルハッシュや IP アドレス、ホスト名に頼らない証拠探しが可能となります。

S なるほど。

G また、ハンターが探すのは、ネットワーク内に潜むアクターだけではありません。ネットワークの設定ミスやシステム間の連携ミスなどにも目を光らせます。というのも、こうしたミスは、アクターがネットワークに長く留まるために役立つ可能性があるからです。

スレット・ハンターの育成

S 仕事の立場上、ハンターを育成することもある

と思いますが、この時に念頭においていることなどあれば教えてください。

G 良い質問です。先ほども言ったとおり、スレット・ハンティングでは広範囲の知識が求められます。ですから対象者には、まず各自のスキルの習熟度を自己評価してもらい、彼らのスキルにどこか不足しているような分野があれば、その分野のスキルを伸ばせるよう情熱を傾け指導しています。とはいえ、このようにスキルを強化し、レベルを上げるためには、彼ら自身の強い意志というか覚悟も必要となってきます。

S まさしく教える側・教わる側の双方が本気でなくてはならないということですね。他にハンターに求められる資質はありますか。

G 仕事では膨大なデータを扱うこととなりますから、まずは、こうした作業を苦と思わない人でしょう。さらにデータの山の中から些細な違和感を見つけられる人です。パズル好きや、書類の誤字・脱字にもすぐ気づく人でしょう。直感的なものなので、教えることは本当に難しいのです。

S 最後の質問になりますが、今後の目標を教えてください。仕事のことでも良いですし、コミュニティのことでも構いません。

G 仕事も趣味も人生もセキュリティですから、毎日の生活が楽しくて仕方ありません。この情熱は持ち続けたいと思っています。また、自分の情熱を新しい世代のハッカーに見せていくことで、彼らの心にも情熱の火が灯せたら良いとは思っています。

S 本日はありがとうございました。

社会のさまざまな動向を把握し、リスクの変化に対応したセキュリティ体制を構築

HISYS CSI (Cyber Security Intelligence) Watch 4月号

文＝ SHIELD Security Research Center

特定社会基盤事業の重要設備を守る政府施策についての考察

【概要】

2022 年に成立した経済安全保障推進法の制度運用に向けて、2023 年 2 月 8 日に有識者会議が開かれ、基本指針案に関する審議が行われた。審議では、特定社会基盤役務の安定性確保が議題の 1 つとなった。本法の制度運用開始に向けて、特定社会基盤役務に携わる事業者やその取引先事業者の対応について考察する。

【内容】

近年、国際情報の複雑化、社会経済構造の変化および地政学状況の変化に伴い、安全保障を確保するための施策拡大が必要とされている。そこで、安全保障の要素「DIME(Diplomacy: 外交、Intelligence: 情 報、Military: 軍 事、Economy: 経済)」のうち、「経済」に関して既存法では対応できない懸念に対応することを目的で、2022 年 5 月、経済安全保障推進法が成立した。

この法律は安全保障の確保に関する経済施策を推進することを目的として制定され、①特定重要物資の安定的な供給の確保、②特定社会基盤役務の安定的な提供の確保、③特定重要技術の開発支援特許出願の非公開、の 3 政策が柱となっている。

本稿では、ビジネス活動への影響が大きいと考えられる②特定社会基盤役務の安定的な提供の確保について解説する。

特定社会基盤役務とは国民生活や経済に不可欠な役務を指し、電気通信・放送・金融・航空・空港・鉄道・電力・ガス・水道・自動車運送・外航貨物・クレジット・石油・郵便の 14 分野において特定社会基盤役務を提供する事業者を「特定社会基盤事業者」と位置付けている。

この法律では、特定社会基盤事業者を指定することや、特定社会基盤事業で利用する特定重要設備※1 の導入計画の事前審査が必要となるといったさまざまなことが定められているが、それらの多くは基準が書かれておらず「主務省令で定める」という記述に留まっており、具体的なことは有識者会議、国会審議等を経て決められることになっている。そして、2023 年 2 月 8 日に開催された有識者会議における議題の 1 つが「特定妨害行為※2 の防止による特定社会基盤役務の安定的な提供の確保」であり、②の基本指針案が示された。示された基本指針案には下記の内容が含まれている。

- 特定重要設備の供給者や維持管理の委託先について、名称、住所、設立国、役員や議決権保有者の国籍、設備の製造場所等の提出を義務付ける
- 特定重要設備が特定妨害行為の手段として使用される恐れが大きいか審査する考慮要素の 1 つとして、「供給者等が我が国の外部にある主体から強い影響を受けているかどうか」がある
- 特定社会基盤事業者が講ずるリスク管理措置の 1 つとして、「特定重要設備の供給元や維持管理の委託先が外国の法的環境等により影響を受けないことを確認すること」が求められる
- 特定重要設備が特定妨害行為の手段として使用されるおそれがある場合など、合理的に必要と認められる限度において主務省庁が事業者へ導入や維持管理委託の中止を勧告・命令できる

※1　事業者の役務の安定的提供における重要性や外部からの妨害に用いられる危険性を考慮して主務省令に定められる基準に該当する設備
※2　特定重要設備の導入又は重要維持管理等の委託に関して我が国の外部から行われる特定社会基盤役務の安定的な提供を妨害する行為

いずれも特定重要設備が安全保障上の懸念国から妨害行為を受けることを防ぐために示されたものであり、いくつかの国や企業で利用されている製品が不適合となる可能性がある。そして、その審査基準が明確化されなければ事業者側が対応することができなくなってしまうため、今後、特定の国を明記するような書き方を避けた上で何らかの規制が作られると予想される。

本制度の開始は 2024 年の春頃である。時間はあるものの、制度開始までの準備として特定社会基盤事業者やその取引先事業者は、特定社会基盤に使われる製品がどの国の製品であるか、委託先企業および再委託先企業がどの国の企業であるか、開発・運用拠点はどこにあるかなどを事前に整理しておくことが必要だ。

また「特定重要設備の対象範囲」も留意しておきたい。特定重要設備と連携するシステムがどこまで対象範囲なのか、クラウドサービス事業者は何をすべきかなど検討する必要がある。場合によっては自社製品やサービス、委託先の情報などを主務省から提示を要求される可能性があり、事前に整理しておくことが必要だ。

今後、設備導入における届出に関する考え方や再委託に関する考え方などの Q&A やガイドラインも公開される予定であり、それらを確認しながら並行して体制を準備する必要があると考える。

【情報源】

https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/4index.html