HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.44

株式会社 日立システムズ

Human * IT

Hitachi Systems security Jounral VOL.44

TABLE OF CONTENTS

さまざまな組織の要職を歴任、最前線で活躍を続ける
坂 明 インタビュー …… 3

インタビュー　RF CTF 参戦記
DEFCON 29 をオンラインで楽しむ …… 8

●はじめに

本文書は、株式会社日立システムズ の公開資料です。バックナンバーは以下の Web サイトで確認できます。
https://www.hitachi-systems.com/report/specialist/index.html

坂 明 インタビュー

さまざまな組織の要職を歴任 最前線で活躍を続ける

今回、インタビューするのは、JC3（日本サイバー犯罪対策センター）理事の坂 明氏。今夏無事に開催を終えた東京オリンピック・パラリンピック競技大会組織委員会の CISO を務められ、9 月からはデジタル庁の CISO に就任されている。さまざまな組織の要職を歴任し、最前線で活躍を続ける坂氏は、サイバー空間の脅威についてどのように考えているのであろうか。経験に裏打ちされた知見の数々を伺った。

取材・撮影・文＝斉藤健一

斉藤（以下 K ）：坂さんは、今夏無事に開催を終えた、東京オリンピック・パラリンピック競技大会（以下東京大会）で、組織委員会の CISO を務められ、今秋からはデジタル庁で同様に CISO の任に当たられています。今回のインタビューでは、JC3（日本サイバー犯罪対策センター）理事の立場から、サイバー空間をめぐる脅威情勢についてお話を伺います。警察庁から同様のテーマをまとめた資料が公開されていますので、こちらの話題も取り上げたいと思います※1。

坂（以下 S ）：折しも、本日（9 月 27 日）、サイバーセキュリティ戦略本部の会合があり、「次期サイバーセキュリティ戦略」が決定されることとなっています。資料が公開されていますので、あわせてここからもトピックを拾いたいと考えています※2。

東京大会における サイバーセキュリティ対策

S 早速ですが、「次期サイバーセキュリティ戦略」の資料の中で、東京大会におけるサイバーセキュリティ対策の結果がまとめられています※3。総括すると「大会運営に影響を及ぼすようなサイバー攻撃は確認されなかった」とあります。

大会期間中に確認された攻撃に類するものとしては、「大会関係組織に対するサイバー攻撃を呼びかける SNS 上の書き込み」、「米国コンテンツ配信サービス企業の障害による関係組織 Web サイトの一時的な閲覧不能」、「開会式や各競技などを装った不正な動画配信サイト」がありました。どれも組織委員会に対する攻撃ではなく、周辺で観測されたものです。

犯罪者は、その時々で話題になっているものを餌にしてフィッシングを仕掛けてきます。オリンピックが盛り上がればオリンピックで、新型コロナウイルスの感染が拡大すれば新型コロナで、といった具合です。場合によってはこの 2 つの要素を組み合わせることもあります。2019 年 9 月には国内向けの五輪チケットの抽選販売で、虚偽の個人情報で約 3 万件のＩＤが不正取得され、約 6900 枚が購入されるという事案が発生しています。最終的に東京大会は無観客での開催となりましたが、もし観客の皆さんもお迎えして開催した場合には、こうしたチケットをめぐる不正事案はより深刻な形で発生していた かもしれません。そういう意味では、競技大会に関する脅威の中には、EC サイトへの攻撃といった脅威も含まれることとなります。ですから、組織委員会としては、そうした攻撃にも備えておく必要がありました。

また、平昌オリンピックでは、大会の運営に影響を与えたサイバー攻撃があったといわれています。オリンピックデストロイヤーというマルウェアによる攻撃で、大会公式サイトで観戦チケットの印刷ができなくなったり、メインのプレスセンターでネットに接続できなくなったりといった事象が発生したと報道されています 。2020 年 10 月に公表された米国司法省の起訴状によれば、ロシアの関与が取り沙汰されるアクターによる攻撃だったとされています。

K 東京大会ではこうした攻撃は発生しませんでした。

S そのとおりです。ただ、最近の脅威の中で影響が大きなものといえばランサムウェアが挙げられます。以前のようなバラマキ型ではなく標的型が主流となってきました。さらに、攻撃手法も国家支援のアクターと変わらない高度なものへと進化しています。東京大会は開催が 1 年延期されることとなりましたが、その結果、こうした脅威にさらされることとなったのです。別の言い方をすれば、攻撃者の層が厚くなったとも言えます。

ここに、興味深いデータがあります。毎年、IPA が情報セキュリティ 10 大脅威をまとめているのですが、2017 年の順位を見ると、「ランサムウェアによる被害」が個人・組織とも 2 位となっています※4。WannaCry が猛威を振るった年です。と

※1 **令和３年上半期におけるサイバー空間をめぐる脅威の情勢等について**
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_kami_cyber_jousei.pdf

※2 **サイバーセキュリティ戦略（案）** https://www.nisc.go.jp/pdf/council/cs/dai31/31shiryou01.pdf

※3 **東京オリンピック・パラリンピック競技大会におけるサイバーセキュリティ対策（結果報告）等について**
https://www.nisc.go.jp/pdf/council/cs/dai31/31shiryou04.pdf

※4 **情報セキュリティ 10 大脅威 2017** https://www.ipa.go.jp/security/10threats/2017/index.html

●坂 明（さか・あきら）

1981 年、警察庁に入庁。目黒警察署長、通商産業省（現経済産業省）通商政策局中南米室長、兵庫県警察本部長、国土交通省大臣官房審議官（自動車局担当）等を務めたほか、生活安全局セキュリティシステム対策室長、情報技術犯罪対策課長として勤務し、サイバー犯罪対策に従事。

2002 年にはハーバード大学国際問題研究所（WCFIA）客員研究員としてサイバーテロの研究に従事し、2008 年から 2 年間は慶應義塾大学大学院政策・メディア研究科教授。

また、原子力規制委員会核セキュリティに関する検討会委員、国土交通省 IT 政策検討会委員、観光庁旅行業情報流出事案検討会委員、警察庁サイバーセキュリティ政策会議委員、国土交通省自動車検査証の電子化に関する検討会委員も務めた。本年開催された東京オリンピック・パラリンピック競技大会では、同組織委員会 CISO を務めた。

現在は、デジタル庁 CISO のほか、公益財団法人公共政策調査会（CPP）専務理事、日本サイバー犯罪対策センター（JC3）理事を務める。

ころが、2021 年には、組織で再び 1 位となりました※5。一方、個人の方は 10 位圏外となっています。つまり、現在のランサムウェアは、企業・組織をターゲットにした、非常に脅威度の高い標的型のものになっていることが見てとれます。

K 確かにバラマキ型で少額を要求するようなランサムウェアは減りました。一方で、標的型の中には二重脅迫を行なうものもあります。

S 情報や資産が影響を受けると運営に重大な支障をきたす組織、オリンピックもここに含まれるわけですが、攻撃者はこうした組織を標的にします。ですから、組織委のような組織はより一層、このような攻撃に備えなくてはなりません。

進化する攻撃者の手口
狙われるテレワーク環境

K ランサムウェアにかぎらず、オンラインバンキングの不正送金事案も 2016 年～ 2018 年にかけて減少していましたが、2019 年に急増しています。

S インターネットバンキングの不正送金事案は、現在は個人が被害の中心となっています。不正送金に利用される認証情報を窃取しようとするフィッシングは、非常に広範に行なわれています。最近では手法が変わっています。PC よりもスマートフォンを使うユーザーが増えたことから、攻撃対象もシフトしています。中には二要素認証を突破するものもありますし、SMS を悪用するものもあります。攻撃者側は常に技術を研究し、手法を高度化させています。

しかも、攻撃者の間では分業化が進んでいて、ゼロデイぜい弱性の売買から攻撃インフラの提供まで幅広く行なわれています。他にも、セキュリティ対策製品に検知されないよう、正規のツールが悪用されるケースもあります。その意味でいうと、一度下火になった攻撃であっても安心はできません。

経済的利益を狙った犯罪としては、インターネットバンキングの不正送金事案ばかりではなく、クレジットカードの被害が拡大しています。また、仮想通貨（暗号資産）が狙われたり、その他のさまざまな決済手段が狙われたりしています。

K 攻撃者は常に手法を磨き、新たな対象を探しているのですね。

S 最近の動向でいえば、テレワーク環境も挙げられます。ランサムウェアの被害に遭った大手ゲームソフト会社の事案では、海外法人が当地における新型コロナウイルス感染急拡大に起因するネットワーク負荷の増大に伴い、緊急避難用として残存していた旧型の VPN 機器が狙われたといいます。

また、2020 年に侵害を発表した通信事業者も、

※5 **情報セキュリティ 10 大脅威 2021** https://www.ipa.go.jp/security/10threats/2021/index.html

撤去の予定だった海外拠点の機器が攻撃の端緒だったと報告しています。「よくそんなところを狙ってくるな」と思う反面、攻撃者は常に弱い所を探索しており、資産管理と機器の設定をしっかりとしておかないと、たとえセキュリティ対策をかなり講じている会社であっても、侵入を許してしまうということかと思います。

K 警察庁の資料を見ると、ランサムウェアの被害にあった企業にアンケートをとっています。侵入・感染経路としては、やはり VPN 機器やリモートデスクトップ（RDP）からの侵入が多く、割合としては半分以上です。

S ご指摘の点については、テレワークが急増した状況を踏まえて、攻撃者は熱心に狙ってきます。また、彼らは SQL インジェクション やパストラバーサルなど、従来から攻撃に使われた手法も、いまだに活用し、ぜい弱性があれば侵入するべく探索してくるのです。

「情報共有」と「備え」の重要性

S 海外メディアのセキュリティマガジンで、東京大会のことを取り上げていただきました。タイトルは、“The Tokyo Olympics are a cybersecurity success story（東京大会はサイバーセキュリティのサクセス・ストーリー）というものです※6。

われわれの仕事は「何事も起きないことが大切」なのですが、それは、世間から見ると、「当たり前」のことですから、評価していただくことは珍しいことです。 記事中には「オフェンシブ」と書かれていますが、これは、攻撃するということではなく 、先制的にインテリジェンスを駆使して防御態勢を整えてきたという意味で、これまでお話してきたとおりです。

また、先ほどの「次期サイバーセキュリティ戦略」の資料に、東京大会の運営で培ったノウハウをレガシーとして継承し活用していく旨の記述があります。東京大会期間中に NISC で運営していた情報共有プラットフォーム（JISP）の活用も考えられると思います。また、東京大会で構築したサイバーセキュリティ対処調整センターについて、その対処態勢や運用により得た知見やノウハウを広く全国の事業者等に対する支援として積極活用する、とされています。

他に「備え」も非常に重要だと感じています。東京大会では、サイバーインシデント対応演習というものがありました。サイバー攻撃だけではなく、ネットワーク障害の発生を想定したもので、データセンターの切り替えを実際に訓練として行ないました。プライマリをセカンダリに切り替えるのですが、実際に行ってみると、さまざまなことが分かり、訓練の重要性を改めて実感しました。

K 東京大会のセキュリティの組織体制として、CIRT2020 という名称が使われていました。大勢の方が携わられたと思うのですが、外部の人間からするとその規模が分かりません。実際のところ、CIRT2020 はどれくらいの規模だったのでしょうか。

S これまで、数字のことは公表していませんでした。これにはいくつか理由があります。開催前に数字を発表すれば、攻撃者にも知らせることになりますから、あえて伏せていました。大会も終了しましたから、現在とりまとめが行なわれていると思います。

CIRT2020 は大会開催前の比較的早い段階に使われてきた名称です。CIRT は文字どおり、インシデント対応や SOC の監視メンバーを指すのだと思い

※6 **The Tokyo Olympics are a cybersecurity success story**（閲覧にはユーザー登録が必要）
https://www.securitymagazine.com/articles/95880-the-tokyo-olympics-are-a-cybersecurity-success-story

ますが、実際のオペレーションではスポンサー企業の方々をはじめ、数多くの企業の方々にサポートしていただきました。正直に申し上げると私の方でもその実数は把握しきれないほどです。

K 東京 2020 大会は、結果として開催が 1 年伸びました。この間、もっとも苦労されたこととは何でしょう。個人でも組織でも構いませんので教えていただけますか。

S 先ほどもお話したとおり、サイバー脅威の状況がこの 1 年で大きく様変わりして、より一層厳しくなりました。常に新しい攻撃手法が出現して、それに備えるためにやるべきことが多く大変でした。

Kさまざまなご苦労があったのだと想像します。話題が飛びますが、警察庁の資料の中に、令和 4 年にサイバー局を設置するとの記述がありました。この点に関して、何かご存じであれば、教えてください。

S 公表されている以上の情報は持ち合わせていませんが、私が理事を務めております JC3 ではさまざまな攻撃を分析し警察と連携して対処しております。海外からの攻撃の場合、都道府県警が海外の法執行機関に照会をかけなくてはならず、捜査はかなり難しくなります。サイバー局が設置されることによって、国内では全国的な状況を踏まえた対応が可能になると思います。また、国際的に見ても、連携・調整・コミットメントがより一層進むと期待しています。

今後の抱負・仕事での心構え

K デジタル庁の CISO に就任されました。抱負をお聞かせください。

S デジタル庁は、行政機関のさまざまな情報システムを、より効率的なものへと統合し、日本における仕事のやり方を含め、Society 5.0 の実現を支えていきます。先に紹介した「次期サイバーセキュリティ戦略」でも謳っていますが、「国民の誰ひとり取り残さない」というスローガンを掲げ、国民一人ひとりに寄り添う形で、業務を進めていくことになります。その中で安全というものも非常に重要だと考えています。国民の方々にデジタルを享受していただけるような環境を構築する、また、行政機関・地方自治体も含めて、安心して使っていただけるようにシステムのサイバーセキュリティを確保していくことが重要だと考えています。しっかり取り組んでいきたいと思います。

K ありがとうございます。坂さんのプロフィールを拝見すると、警察庁に入庁以来、人々の生活や社会を守る立場に長くいらっしゃいます。国営放送の某番組ではありませんが、坂さんの仕事の流儀や内的な動機について、伺いたいと思います。 特に、何か仕事で心がけていることなどありませんか。

S 記事にできるかどうか分かりませんが、母方の家系がお寺でして、いまでもお寺の境内に建っているようなマンションに暮らしています。なんと言ったらよいでしょう、うまく説明できませんが、そうした環境にいると、自分の存在がちっぽけに思えるといいますか、より大きな存在を感じるといいますか、そういった心持ちになるのです。そして、大きな存在を感じるためには、より謙虚にならなくてはと思うことがあります。ですから、仕事をする上では謙虚になることを心がけています。

K ありがとうございます。十分に記事になると思います。今回のインタビューから
「坂さんは人を楽しませるのが好きな人」なのだと想像していましたが、最後の回答を伺って、坂さんの人柄のより深いところに触れられた気がします。自分自身も見習いたいと思います。本日はありがとうございました。

DEFCON 29 をオンラインで楽しむ

インタビュー　RF CTF 参戦記

取材・文＝斉藤健一　協力＝エル・ケンタロウ

オンラインでは味わえないリアルの感覚

2021 年 8 月 5 日～ 8 日、ハッカーの祭典である DEFCON29 が開催された。新型コロナウイルス感染症（COVID-19）の影響を考慮して、米国ラスベガスのリアル会場（In-person）とオンライン配信（Virtual）を組み合わせたハイブリッドでの開催となった。オンライン開催のみだった 2020 年と比較すれば、コロナ禍からの復活の兆しが見て取れる。

今夏、米国へ渡航するには、入国後 14 日間の待機が課せられていたため、参加者のほとんどはオンラインを利用したはずだ。　筆者もいくつかの講演をオンラインで視聴した。オンラインの特徴は距離の制約を受けないことだ。もちろん、時差の問題は残るが、メリットの方がはるかに大きい。昨年はオンライン初開催ということもあり、期待に胸を膨らませて視聴したのだが、今年の DEFCON では、なぜかそのような気分にはなれなかった。

これは個人的な感想だが、事前の調査不足なのか、それともテーマが小粒なのか、タイムテーブルに並ぶ各講演の内容に興味を持てなかったことが大きな理由だ。また、視聴しているディスプレイの向こう側には、現地で参加して楽しむ人たちがいるかと思うと、自分だけが取り残されたようなもどかしい気持ちにもなった。おそらく、これも理由の 1 つだろう。　例えば、縁日の境内や学園祭などを想像していただきたいのだが、多くの人が集う祭りには、その場にいるだけで味わえる高揚感がある。そして DEFCON にも現地でしか味わえない同様のワクワク感があるのだと思う。

DEFCON に対する気持ちが盛り上がらなかった理由には、社会全体の「コロナ疲れ」などの要因も関連しているだろう。こちらについては、自分の考えを整理した上で、他に機会があれば改めて紹介したい。

オンラインで
カンファレンスを楽しむには

オンラインで DEFCON を楽しむには、何か目的を持つことが重要だ。2022 年の新型コロナの感染状況を今から見通すことはできないし、DEFCON がどのような形態で開催されるかも分からない。ただ、事前に準備をしておけば、リアル会場参加でもオンライン参加でも、イベントを楽しむことができるだろう。今回は、DEFCON RF（Radio Frequency）CTF に参加したエル・ケンタロウさんに話を伺った。

RF Village と Wi－Fi ハックの復興

RF CTF の説明の前に、まずは競技を主催する RF Village について紹介しよう。このビレッジは以前の Wireless Village が改称されたもので、RF Hackers Sanctuary が運営にあたっている※ 1。改称の背景には、IoT の普及などに伴い、Wi－Fi をはじめ、Bluetooth、Zigbee、RFID といった無線通信規格を実装したデバイスの増加や、SDR（ソフトウェア定 義無線）の発展などがあるという。

また、エル・ケンタロウさんによると、Wi－Fi ハックの技術は、ここ数年で大きく進歩し、今まさにルネサンス（復興）を迎えているという。Wi－Fi ハックというと、Aircrack-ng といったツールを使い、WEP などぜい弱な暗号化プロトコルをターゲット

※ 1 **RF Hackers Sanctuary** https://rfhackers.com

に、鍵を解析するような、いわゆる初心者向けの行為というイメージがつきまとっていた。そして、WPA2、WPA3へと暗号化プロトコルが強化されるにつれて解析も困難となり、人気も徐々に下降していった。

ところが、近年、WPA3（パーソナル）の辞書攻撃に特化したツールが発表されたり※2、かつてWi-Fiハックツールとして名を馳せた"Kismet"が、Wi-Fiに加えて、Bluetoothや Zigbee、rtl_433（RF信号解析ツール）なども扱える無線通信解析の統合ツールとして生まれ変わり、今年8月には新バージョンがリリースされたりしているという※3。「新バージョンの完成度は高く、Unicodeにも対応しているので、絵文字や日本語のSSIDにも対応。かつてのKismetユーザーならその進化に驚くはず」とエル・ケンタロウさんは語る。

RF CTFの競技

話を戻そう。RF CTFはオンラインで開催される。競技は大きく分けて2つ。1つは競技用の仮想環境で行なわれるSDRチャレンジだ。DEFCON開催期間が競技期間となる。用意された問題サーバーでは、ポートごとに「モールス信号」、「ハム通信（アナログ・デジタル）」、「デジタル変調信号（ASK）」、「ブラックボックス（通信方式が明かされていない）」などの信号が送信されており、プレイヤーはこれを取得・解析し、解答のフラグを見つけ出す。中には数時間に1度しか信号を発信しない問題もあるそうで、魚釣りのように気長に待つ必要があるという。

もう1つの競技は、ワールド・ワイド・ウォー・ドライブだ。世界中の無線ネットワークの位置と情報を収集するWiGLE.net※4（ウィーグル）というサービスと連携して行なうオンラインのウォー・ドライビング・コンテストだ。WiGLE.netでは、スマートフォンアプリを使い、ゲーム感覚でAP（アクセスポイント）を発見・収集し、地図上に表示する。こちらは、DEFCON開催の3日前から競技が開始されていた。住む場所が異なる人々がどのように競技を行なうかというと、各プレイヤーが地図上で16km以上、99km四方以下のエリアを選択し、その中でウォー・ドライビングを行なう。エリア内にある新たなAPを発見したり、主催者側があらかじめ指定したFOXと呼ばれる特別なAPを見つけ出したりすることでポイントが得られる。もちろん、都市部と郊外とでは、APの数が大きく異なるが、エリアによる差が出ないように統計的な調整を行なった上でポイントが算出される。

有能な通訳であり、ハッカーのエル・ケンタロウさん。DEFCON20周年記念のドキュメンタリームービーの日本語字幕制作をボランティアで行なうなど、ハッカーコミュニティへの貢献を続けている。
DEF CON 20 ドキュメンタリー 720p 日本語字幕フルバージョン
https://www.youtube.com/watch?v=N4TlvXXXVGE

チームの作戦と勝敗の行方

RF CTFに参加したのは19チーム。プレイヤーの総数は定かではないが、得点を獲得しているアクティブなプレイヤーは50名ほどだ。また、1名でもチームとして登録できるため、中にはSDRチャレンジには手を出さず、ワールド・ワイド・ウォー・ドライブだけに注力するプレイヤーもいる。

エル・ケンタロウさんが所属したのは"WhatTheFreq!"というチームで、結果を先に言うと、みごと優勝を果たした。ただし、この背後にはある作戦があった。ワールド・ワイド・ウォー・ドライブがCTFの競技に加わったのは昨年からだ。先述のように、単独で参加するプレイヤーが一定数いたといい、エル・ケンタロウさんもその中の1人だった。CTFの競技全体から見れ

※2 **blunderbuss-wctf wacker** https://github.com/blunderbuss-wctf/wacker
※3 **Kismet** https://www.kismetwireless.net/
※4 **WIGLE.net** https://wigle.net/

ば、彼らが獲得した得点が優勝争いに関与することはない。今年、これに目を付けた"WhatTheFreq!"のチームリーダーが、単独で参加するプレイヤーたちに声を掛け、自チームに引き入れたというのだ。この作戦は物議を醸したそうだが反則にはならなかった。まさに、ルールの範囲内で最大の効率をめざすハッカー的なやり方だと言える。

ウォー・ドライブの流儀

エル・ケンタロウさんに自身の作戦について聞いてみた。他のプレイヤーがクルマを使ってウォー・ドライブする中、エル・ケンタロウさんは「ウォーキング」にこだわったという。特に競技に有利だからという理由ではなく、普段からプレイしている WiGLE のやり方で挑戦したかったからだそうだ。選んだエリアは自宅と事務所の間で、AP が密集する駅前や繁華街は避けたという。開催期間中、新型コロナウイルス・ワクチンの 2 回目の接種と重なり、副反応の影響から 2 日間の休養を挟んだが、4 日間の実働で歩いた距離は約 90km にも及ぶという。

ちなみに、ウォー・ドライブでトップの成績をとった grimOus というプレイヤーは、ラスベガス郊外の新興住宅地をエリアに選び、3 日間をクルマの中で過ごしたという。エル・ケンタロウさんも「新興住宅地は新たな AP を発見できる狙い目」だと語る。

Wi－Fi ハンティングの魅力
コミュニティとのつながり

「Wi－Fi ハンティング（ウォー・ドライブ）の面白いところは、装置に凝ろうと思えば、いくらでもカスタムできるところにある。数台のスマホをバックパックに入れてオートバイで走り回る人間もいれば、クルマ 1 台をまるごと Wi－Fi ハンティング用に改造してしまう人間もいる」。エル・ケンタロウさんは Wi－Fi ハンティングの魅力をこのように語る。また、「もう 1 つの面白さはプレイするためには外に出なくてはならない点にある」とも語ってくれた。

エル・ケンタロウさん自身、WiGLE を真剣にプレイし始めたのは、コロナ禍になってからだ。もちろん、コロナ禍以前もプレイしていたそうだが、そのときは、海外出張で訪れる地域で WiGLE ユーザー未踏の地を探したり、特徴のある名前の AP を探して登録したりするようなユーザーだったそうだ。ところが、コロナ禍で海外出張はゼロとなる。また、昨年に参加した RF CTF で、上位入賞プレイヤーの取り組みを目の当たりにして、本格的に始める決意をしたという。「本格的にプレイしてみると、身の回りにあるワイヤレスデバイスの数の多さに驚いた」と言い、「同じ地域を何度もスキャンすると、コロナ禍で在宅勤務が増えた影響からか、Wi－Fi ルーターのファームウェアが軒並みバージョンアップされていることも分かる」とも語る。

WiGLE.net の登録ユーザーは 3 ～ 4 万人で、アクティブユーザーは 4000 人ほどだ。さらに、ランキング上位のヘビーユーザーともなればその数はさらに限られる。本格的にプレイし始めたエル・ケンタロウさんも Twitter などでヘビーユーザーたちとの交流をはじめた。彼らは WiGLE でのライバルであり同士でもある。

また、WiGLE.net のユーザー・コミュニティはフレンドリーで、初心者のサポートをベテランが率先して行なっているという。余談だが、先述の Kismet の開発者である dragorn ことマイク・カーショウ氏は、田舎暮らしで自身が開発したツールを検証する環境が十分ではない。そこで、WIGLE コミュニティがベータテストを行なうなどして開発に協力しているという。

2022 年の DEFCON は 30 周年のメモリアル

エル・ケンタロウさんのように、海外のハッカーコミュニティの中で自分の居場所を見つけるのは難しいかもしれない。だが、何かしらの目的を持っていれば、それがリアル会場であっても、オンラインであったとしても、得られるものに違いが出てくるはずだ。2022 年、DEFCON は 30 周年を迎える。リアル会場で開催されれば、大きなイベントとなるに違いない。来年の参加に向けて、各ビレッジのフォーラムやアーカイブを見るなどして今から予習するのも悪くないかもしれない。

Human * IT

人と IT のチカラで、驚きと感動のサービスを。

Hitachi Systems Security Journal VOL.44

株式会社 日立システムズ
本社 〒141-8672 東京都品川区大崎 1-2-1