HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.40

株式会社 日立システムズ

Human * IT

Hitachi Systems security Journal VOL.40

TABLE OF CONTENTS

●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

注目講演の見所・スピーカーインタビュー・CBCTF の紹介など

CODE BLUE 2020 ガイド

取材・文 = 斉藤健一

CODE BLUE 2020 の概要＋注目講演ピックアップ

本年 10 月 29 日・30 日の 2 日間、CODE BLUE 2020 が開催される。今回は新型コロナウイルス感染症（COVID－19）の感染状況を踏まえて、オンラインでの開催となった。また、10 月 9 日には本番に先立ちプレイベントが開催・配信されている。今号では、プレイベントの内容をちりばめながら、注目講演の見所やスピーカーへのインタビュー、さらに CODE BLUE CTF（残念ながらカンファレンスと同時開催ではない）の紹介など、さまざまな角度から CODE BLUE 2020 に迫ってみたい。

参加費無料により事前参加登録数は大幅増

今回の CODE BLUE の大きな特長は参加費を無料としたことだ。CODE BLUE 事務局代表を務める篠田佳奈氏はプレイベントの席で、参加費を無料にすることは大きな挑戦であり、スポンサー企業の協力や後押しがなければ実現できなかったと語っている。BlackHat をはじめセキュリティ・カンファレンスの多くがオンライン開催へと移行しているが、国際会議で参加費完全無料と謳うものはほとんどない。しかし、この英断によって日本開催という距離の制約、参加費という経済的制約から解放されることとなり、多様な参加者が集まってくることが期待される。現に参加の事前登録者数は大幅に伸びているという。オンサイト（会場）で行なわれた昨年の参加者数は、スタッフなどの関係者を含めて 1100 ～ 1200 名程度だったそうだが、今年に関して言えば、プレイベントが行なわれた 10 月上旬の段階で 2200 名を超え、その数はさらに伸びると予想される。

CODE BLUE のように、サイバーセキュリティに関連する最先端で多種にわたる情報が無料で提供されるカンファレンスは他になく、事前登録者数の増加にも納得がいく。

2 日間で行なわれる講演は 50 本

講演は 3 つのトラックで構成される。「ジェネラル」「テクニカル」「サイバー犯罪」「ロー & ポリシー」など CFP（論文募集）の審査を通った講演の他、フリーツールなどを紹介する Bluebox の枠が加わる。また初の試みとして、コミュニティによるセッションやパネルディスカッションも予定されている。さらに、スポンサー企業による講演である OpenTalks が独立したトラックとして併設される。すべてを合計すると、2 日間で 50 本もの講演が行なわれることとなる。また、スピーカーの国籍も世界 15 カ国・地域と多岐にわたっている。

注目の講演紹介

ここからは、注目の講演をピックアップしてご紹介する。プレイベントの際にレビューボードがオススメしたものが中心となる。

・基調講演「脆弱性調査をサポートするためのサイバー犯罪法の改正。英国の経験とその後」
オードリー・ギンジャード（Audrey Guinchard）
10 月 29 日 12:00 ～ 12:30 Track1

リサーチャーと社会との関係に問題を提起する内容。英国のコンピューター不正使用法（1990年）は他国と比較しても適用範囲が広く、ぜい弱性調査に影響を及ぼす可能性が高いと言われる。リサーチャーのリスクになっている現状で英国やEU の取り組みが紹介される。講演では、「公益の防衛」（public interest defence）という考えの導入が提案される。日本でも法の解釈と技術をめぐるトラブルが発生しており、他国の事例を知るよい機会だと言える。

•特別講演「デジタル•ソーシャル•イノベーション」
オードリー・タン（Audrey Tang）
10 月 30 日 14:40 〜 15:10 Track1

台湾がデジタル・ソーシャル・イノベーションの力を利用して新型コロナウイルスに対抗した方法を、デジタル大臣のオードリー・タン氏自らが紹介する。デジタル・ソーシャル・イノベーションとは、公益を目的にあらゆる分野からさまざまな人々が集い、そこから生まれた集合知によってシステムを変革しようとする取り組みだ。講演ではその背景にある台湾の開かれた市民社会や、市民ハッカーコミュニティ（g0v）についても紹介される予定だ。

• テクニカル「Lamphone：電球の振動からリアルタイムな受動的音声復元」
ベン・ナッシ（Ben Nassi）
10 月 29 日 18:00 〜 18:30 Track1

音（= 空気の振動）によってわずかに振動する電球の表面を観測することで音声を復元しようとする研究を紹介。この技術の特長は、「リアルタイムで」「外部から」「受動的に」盗聴できる点にある。研究では、とあるオフィスの一室に吊り下げられた電球をターゲットに、建物から 25m 離れた地点から観測し、音声を復元できたと報告している。どの程度の精度で復元できたのか気になるところだ（次ページにインタビュー記事あり）。

CODE BLUE 2020 当社 Open Talks のお知らせ

下記のとおり OpenTalks を行ないます。ご参加いただいた方の中から抽選で Amazon ギフト券のプレゼント企画も実施。応募は講演中に出題される簡単なクイズに答えるだけ。2 日間とも参加すれば当選確率は 2 倍になります。ぜひ多くの方のご参加をお待ちしています。

●サイバー食堂シリーズ「洋定食」
10 月 29 日（木）17:50 〜 18:20

ゲストスピーカー：メイ・ネルソン（Mei Nelson）
コメンテーター：本川祐治
モデレーター：丹京真一

当社とグローバルパートナーがお送りする世界の台所シリーズ。「洋定食」では、ゲストスピーカーとして、米アクセンチュア社より、サイバー脅威インテリジェンス セキュリティプリンシパルであるメイ・ネルソン（Mei Nelson）氏にご出演いただき、米大統領選挙など、米国の最新トピックスについてお話しいただきます。

●サイバー食堂シリーズ「台九定食」
10 月 30 日（金）14:20 〜 14:50

ゲストスピーカー：スン•ティン•ツァイ（Sung-Ting Tsai）、チェ・チャン（Che Chang）、小出洋
モデレーター：折田彰

当社とグローバルパートナーがお送りする世界の食堂シリーズ。「台九定食」（台九とは、台湾、九州の頭文字を表します）では、ゲストスピーカーとして、台湾の TeamT5 社より、CEO であるスン・ティン・ツァイ（Sung-Ting Tsai）氏、インテリジェンスチーム サイバー脅威アナリストであるチェ•チャン（Che Chang）氏にご出演いただき、台湾の選挙などの最新トピックスについてお話しいただきます。
また、九州大学より小出教授にご出演いただき、当社との共同研究についてお話しいただきます。

・サイバー犯罪「10 万ドル相当のビットコインウォレットを盗んだのは誰か – 新しい詐欺的な餌で全員捕まえよう」
タン・キアン・ソン（Tan Kean Siong）
10 月 30 日 12:40 ～ 13:10 Track1

10 万ドル相当が入っているように見える " ニセ " ビットコイン・ウォレットをネット上のさまざまな場所に配置、犯罪者に盗ませてその後の動向を観察した実験結果を紹介。ニセウォレットには特別なアラート機能があり、ウォレットを盗んだ犯人を探知することができるという。ファイルはどのように盗まれたのか、また盗んだ犯人の実態とはどのようなものなのだろうか。講演に期待したい。

・ロー & ポリシー「World Wide Web でも政治はローカル：バルカン化するインターネットを生き残るための計画」
メイ・ネルソン（Mei Nelson）
10 月 29 日 14:40 ～ 15:10

地政学的な観点からインターネットの現状を分析した内容。インターネットの主権を強化する国家もあれば、強大なファイアウォールで通信を監視する国家もあり、現状はインターネットのセグメント化・バルカン化が進んでいるという。講演ではこうした状況下におけるサイバー脅威を分析しており、タイムリーな話題だと言える。

・ロー & ポリシー「脅威インテリジェンスによる中国の情報操作の分析」
チェ・チャン、シルビア・イェ（Che Chang, Silvia Yeh）
10 月 29 日 16:40 ～ 17:10

台湾の 2018 年の地方選挙、2020 年の総選挙において、攻撃者がどのような情報操作を行なったのか、探知して攻撃グラフを作成して分析。国家組織が関与する情報操作によって、民主制の土台が揺らぐと警鐘を鳴らす。わが国にはこうした情報が少なく、台湾の事例を学ぶことによって視点を補うことができるだろう。

ベン・ナッシ氏（注目講演スピーカー）にインタビュー

スパイドローンを検出する講演も予定

前項でも紹介したとおり、CODE BLUE 2020 の注目講演の 1 つに、吊り下げられた電球の振動を観測することで音を復元できる Lamphone がある。イスラエルのベン・ナッシ氏によるものだが、彼は今回の CODE BLUE で別の講演を行なう予定もある。そのテーマは「スパイドローンを特定するための暗号解読」というものだ。海外では宅配に使われはじめるなど、幅広い用途でドローンが使用されるようになってきた。しかし、自分の生活圏内で見かけるドローンがどのような用途で使われているのか、その意図を外部から知ることはできない。もしかしたら悪意ある操縦者が誰かの生活をのぞき見るために飛ばしているのかもしれない。

この講演では、ドローンと操縦者との通信を傍受し、ビデオストリーミングが行なわれているか

ベン・ナッシ氏 近影

否か瞬時に検出する技術を紹介するという。もちろん、ビデオストリーミング自体は暗号化されているが、被撮影者（盗撮される）側がカメラに対して定期的に何かしらのアクション（動いたりライトのオンオフなど）することで、トラフィックに「透かし」のような情報が付加されるという。あとは、傍受した通信に「透かし」が含まれているかどうかを確認すればよい。場合によっては 2

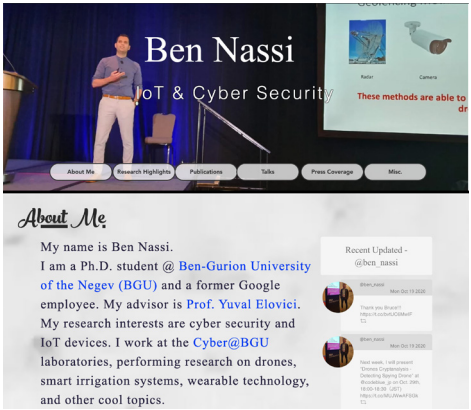
～3秒で検出できるという。

説明が長くなってしまったが、同一カンファレンスで方向性が異なる2つの講演（しかもどちらも着眼点がユニーク）のスピーカーとはどのような人物なのだろうか。研究テーマの選び方や研究環境などに興味を持ったので、メールでのインタビューを行なうこととした。

ベン・ナッシ氏にインタビュー

ベン・ナッシ氏のWebサイトでは研究成果などが紹介されている。プロフィールを見ると元Google社員で、現在はイスラエルのベン・グリオン大学（BGU）の博士課程に在籍している。まず、この点について質問してみると、Googleでの業務に関しては答えてくれなかったものの、大学に戻った経緯については「サイバーセキュリティ分野で研究することに情熱を感じ、博士号を取得しようと自分の時間をフルに使うことを決意した」と語ってくれた。一方、ベン・グリオン大学（BGU）を選んだ理由としては「学士・修士ともBGUで取得しており、博士課程も必然的に同大学となった」とし、「BGUはイスラエルでサイバーセキュリティの専門家がもっとも多い大学」とも評してくれた。

また、研究成果を見ると、それぞれの論文で共著者がいると分かる。この点を尋ねると「研究チームはボリス・ザヴドフ（Boris Zadov）博士が率いており、コンピューターサイエンス、ソフトウェアエンジニアリング、情報システムエンジニアリング、電気工学などの専門家が集まっている」のだそうだ。では、研究テーマは誰の発案なのだろうか。ナッシ氏は「Lamphoneの元のアイデアは、他のデバイスから音声を復元しようとしたもので、ザヴドフ博士と共同で発案したが、他の研究のほとんどは自分自身が決めたものだ」と答えてくれた。さらに、自身の研究テーマについて「セキュリティとプライバシーの分野で大きな影響を与えるものに焦点を当てている。最近の研究として、セキュリティでは、テスラに対するファントム攻撃（路上に、人間や道路標識などの画像をプロジェクターで照射することにより、テスラの自動運転をだます）、そしてプライバシーではCODE BLUEで紹介するLamphoneやドローンの暗号解析などに取り組んでいる」と語ってくれた。



ベン・ナッシ氏のWebサイト https://www.nassiben.com/

これらのユニークな研究で彼自身が重要だと考えているものは何だろう。これに対してナッシ氏は「影響の大きな問題に取り組む際に重要なのは実際のセットアップ（ラボの外）で研究を実証することで、これによって多くの人々に研究の実用性を納得させることができる」と答えてくれた。その一方で、「興味深い問題を見つけてそれを明らかにすることは困難であり不確実性が伴う」としながらも「優れた研究を行なうのに重要なのは情熱と興味を失わないことである」と自身の研究に対する姿勢を述べてくれた。

いくつもの研究を並行して行なっているので、時間管理に関しても質問してみた。すると「普段は学部生と共に研究を行なっている。彼らの多くが修士課程に進んでいる」というコメントを得た。最後に次の研究のテーマを可能な範囲で聞いてみたが、「プライバシーの分野になると思うが、詳細については差し控えたい」との反応が返ってきた。

新奇性の高い研究を次々と発表し注目を浴びるベン・ナッシ氏だが、研究のアイデアを発表という形に仕上げるまでには、日々の小さな積み重ねがあったはずだ。特に具体的な言及があるわけではないが、メールの文面にはそれがにじみ出ているように感じた。

CODE BLUE CTF 主催者 TokyoWesterns にインタビュー

CODE BLUE CTF（以下 CBCTF）がはじめて開催されたのは 2017 年。以来毎年回を重ね、今回が 4 度目の開催となる。大会の運営は binja と TokyoWesterns という 2 つの CTF チームが担当する。CTF の最高峰である DEFCON CTF 決勝大会に何度も出場している日本屈指の精鋭たちだ。

CBCTF の大きな特長は、決勝戦で Bull's Eye と呼ばれる形式が採用されている点だ。2018 年から採用されている。CTF 大会の形式には、出題された問題を解くジェパディ（jeopardy）形式や、自チームのサーバーを防御しつつ敵チームを攻撃する攻防戦（Attack & Defense）形式などがある。だが、Bull's Eye はどちらの形式でもないオリジナルのものとなっている。

Bull's Eye とは

Bull's Eye が重視するのは攻撃の精度だという。通常の CTF ではフラグを取る過程でどんなに試行錯誤を重ねても問題にはならない。極端な例を挙げれば、攻撃によって問題サーバーをダウンさせたとしても、主催者に再起動をお願いすれば済む。ところが、現実のハッキングではそうは行かない。攻撃に失敗して対象マシンをダウンさせてしまえば、そこで終了となってしまう。

Bull's Eye では攻撃の正確さを評価するため、次のような手順で進む。参加者は一定時間ごとに Exploit（攻撃コード）を主催者に送信、提出された Exploit は主催者側が実行、スコアは攻撃の「成功数／試行回数」となる。なお、攻撃の成否は Exploit の実行環境に依存する部分も多いので、参加者が主催者に送るのは Docker（仮想環境）のイメージだという。

CBCTF は、これまでオンライン予選とオンサイト（競技会場）での決勝戦という形式で行なわれてきた。しかし、新型コロナ禍の影響により、今年は決勝戦もオンラインで行なわれることとなった。そこで、主催者である TokyoWesterns リーダーの市川遼氏に話を伺うこととした。余談だが、本誌 Vol.35 にて市川氏のインタビューを掲載している。興味のある方はぜひこちらもご一読を※1。

CODE BLUE CTF 2020 http://ctf.codeblue.jp/

インタビューは 10 月上旬にメールで行なった。この時点で、筆者は CBCTF の開催日程が未定だということを知らずにいたため、日程に関する質問は含まれていない。

CBCTF 主催者による パネルディスカッションが開催予定

10 月 30 日（15:20 ～ 15:50）に「我々はなぜ CTF を運営するのか？」というタイトルのパネルディスカッションが行なわれる。インタビューに回答していただいた市川氏のほか、チーム binja リーダーの小池悠生氏、CBCTF 運営に携わる米内貴志氏が登壇、レビューボードのはせがわようすけ氏がモデレーターを務める予定だ。

彼らが CTF に惹きつけられる理由が語られるとともに、開催日程を含めた CBCTF の情報がアップデートされる可能性もある。CTF プレイヤーならば視聴は必須だろう。

※1 **Hitachi Systems Security Journal** https://www.hitachi-systems.com/report/specialist/hj/

TokyoWesterns インタビュー

Q 現状を知る上での一般的な質問です。現在の CTF シーンにおいて、新型コロナウイルスが何らかの影響を及ぼしていると思いますか？

A 新型コロナウイルスが直接的にもたらしたものは、オンサイト CTF が開催できなくなったことだと考えています。以前から開催が決まっていたオンサイト CTF についてはすべて延期になり、また決勝戦が存在する CTF はオンライン開催となりました。

オンライン開催の場合、競技者は自分たちの地域からの参加になるため、オンサイトではある程度公平であった時差問題を考慮する必要が出てきます。

同様に、オンライン開催においては運営はインターネット回線の品質を保証することができず、結果として、大量のトラフィックを安定して送出する必要がある競技形式は、公平性の観点から行なうことが難しくなります。

また、オンサイト会場に入場人数を限定することによって担保されていたチームごとの人数制限は事実上不可能になり、そもそも人数制限をなくす、参加者の性善説に委ねる、システム上で人数を制限する、などの対策を取る必要が出てきました。

逆にいうと、元からオンラインで行なわれていた CTF についてはほとんど変化はないということです。

Q CBCTF では TokyoWesterns CTF（以下 TW CTF）がオンライン予選として位置付けられています。本年は TWCTF の参加チームが減少しているように思えました。CTF TIME で 2020 年[※2] と 2019 年[※3] を比較すると、2019 年の参加チーム 1005 に対して、2020 年は 648 でした。この原因をどのように分析しますか？

A 参加チーム減少の最大の要因は、CBCTF が DEF CON CTF (以下 DCCTF) 予選ではなくなったことだと考えています。CBCTF の過去 2 大会では決勝戦で優勝したチームは DCCTF の決勝戦に出場できましたが、今年は、その権利がありません。DCCTF を運営する OOO（Order of the Overflow）は、毎年その予選とする外部の CTF を選択しますが、今季はインターネット上で公募する形を取りました。しかし、今年は応募フォームが出るのが遅く、またわれわれ運営側でも意思決定のプロセスが遅かったため、申請が間に合いませんでした。

そのため、CBCTF の予選となる今年のは TWCTF は、CBCTF と TWCTF の純粋な知名度のみで参加チームを集める必要がありました。

しかしそれより過去の TWCTF の参加チーム数を見ると、2018 年は 810 チーム、2017 年は 901 チームの参加があります。

そこで原因を探してみると、実は今年の TWCTF と同期間に別の CTF[※4] が開催されており、こちらの参加チーム数が 1080 となっていることから、多くのチームが流れたのではないかと予想できます。実際に、当日の IRC (運営と参加者のコンタクト用チャット) も例年より閑散としており、参加者の数が明らかに減ったという実感がありました。

Q 今年で 4 回目の開催となります。まず予選に限定して、問題作成・CTF 競技運営などは慣れましたか？　また、運営上のトラブルなどありましたか？

A CBCTF の以前に TWCTF シリーズとしては 6 回目の開催になるため、所感としては例年どおりです。何度運営を経験しても依然としてトラブルはつきものですが、事前に予測できる範囲の深刻なトラブルはありませんでした。昨今の情勢を鑑みて、今年は初のオンラインのみでの運営だったため、運営スケジュールの大切さを実感しました。やはり担当者には叩き起こせる位置で寝ていてもらいたいですね。

※2　TokyoWesterns CTF 6th 2020 https://ctftime.org/event/1086
※3　TokyoWesterns CTF 5th 2019 https://ctftime.org/event/808
　　それぞれページで最下端までスクロールすれば参加チーム数が分かる
※4　DownUnderCTF https://ctftime.org/event/1084

Q 予選問題に関して、競技に参加したチームから「難しい or やさしい」などのフィードバックがあった場合、その代表的なものを教えてください。

A 難しいという声は少しありました。全体的に難易度に関するフィードバックは少なく、問題の質に対する言及が多かったです。今回は息抜きの意味を込めて、なぞなぞのような問題を数問出したのですが、guessing と評されてしまいました。

参加チームが求めているものは純粋な CTF の問題だけということなのだと思います。来年以降はもう少し考える必要がありそうです。

Q 今年の予選を勝ち上がったチームを見て、何か感想はありますか？ 例えば「○○チームは順当な勝ち上がり」や「××チームが彗星のごとく現れた」といったものです。

A PPP、Balsn、p4、0daysober、hxp など常連のチームはやはり強く、着実に点数を取っていました。

perfect blue、ALLES! などの近年見るようになった強豪チームも常連チームに引けを取らない成績を残しています。一方で、今回初めて見た D0G$、KoreaSuperPower はそれぞれ韓国のチームがベースとなっている連合チームです。D0G$ については後述しますが、日本も加えて 4 チームの連合という巨大なチームでした。KoreaSuperPower も韓国のよく知られたチームの連合であり、これら 2 つは TWCTF のために結成されたようです。

Q 決勝戦に関して、一般の人が競技の進展を知るにはどのようにすればよいですか？ Web サイトなどが作成されるのでしょうか？

A オンラインでの開催になりますので、スコアボードを公開する予定です。続報をお待ちください。

Q Bull's Eye を採用している CTF は他にはなく、CBCTF が唯一無二だと伺っています。この点に変わりはありませんか？

A Bull's Eye はわれわれ CBCTF が発祥であり、システムのソースコードを公開しているとはいえ、他の CTF で運用されることを想定したドキュメントなども存在しないため、正しく運用するのはかなり困難だと思います。
実際にこのシステムを運用したい場合はソースコードを全部読むか、われわれにコンタクトを取るかのいずれかが必要になると思いますが、少なくとも後者についてはそう言った話は聞きません。

Q この 1 年間で Bull's Eye に何らかの進化はありましたか

A 一昨年から去年にかけて大きな改修を行ない、パフォーマンスは飛躍的に改善されました。今年は 1 つ大きなチャレンジがあり、鋭意実装中です。続報をお待ちください。

Q 競技参加者からの Bull's Eye の評判はいかがですか？

A おおむね好評ですが、システム以前にそもそも問題が難しすぎるという声がありました。Bull's Eye の特性上、単純なぜい弱性はすぐに高得点解法につながってしまうことが多いため、仕込むぜい弱性は自然と高難易度になってしまうことの現れだと考えられます。

Q 例年、決勝戦はオンサイトで開催されていましたが、今年は決勝戦もオンライン開催となりました。何かやりにくい点などはありますか？

A 以前からシステム自体はオンラインで動作しているため、何ら変わりはありません。変わった点を強いて挙げるならば、オンサイト会場のインフラ問題を気にしなくてよくなったことです。

Q Bull's Eye の Web サイトの説明を見ると、Exploit を submit するのには、Docker のイメージを主催者に送ることとなっています。素人考えですが、Docker のイメージファイルは容量が大きく、オンラインの大会には不向きなのではないかと思いました。Docker のイメージファイルの容量はどれくらいなのでしょうか？また、大きなファイルをオンライン競技でやりとりすることのリスクはないのでしょうか？

A Docker のイメージファイルが大きいという懸念はそのとおりで、初回の push 時にはかならず大容量のデータを送ることになります。しかし Docker のイメージデータは実際には細分化されて保存されており、共通する部分については使い回すことができます。

そのため、例えばソースコードを少し変えて push する程度ならば、その差分しか送信されないためさほど問題にはなりません。
オンサイト会場で開催していた時は参加者全員のネットワーク環境を用意することによって公平性を担保していましたが、オンライン開催の場合はインターネット回線の品質によって競技のやりやすさが左右される懸念はあります。

Q CODE BLUE 2020 カンファレンスを視聴する人に向け、メッセージがあればお願いします。

A 今年はオンライン開催となったため、より多くの人が気軽に参加できるのではないでしょうか。CBCTF は残念ながら CODE BLUE 2020 カンファレンスと同時には行なわれませんが、もし興味を持っていただけたなら、スコアボードだけでもぜひご覧になってください。

CODE BLUE CTF 2020 決勝戦出場チーム（予選順位順）と市川氏による各チームのコメント

1　D0G$

Definit (韓国)、zer0pts (日本)、GoN (韓国)、$wag (韓国) からなる連合チームです。
それぞれの得意分野を生かし、予選の TWCTF では 2 位を大きく離しての 1 位となりました。

2　perfect blue

2 年ほど前から登場したチームです。国籍は米国となっていますが、実際はカナダをはじめとしたさまざまな国籍の人が参加しているようです。さまざまな CTF に参加しており、優秀な成績を収めています。2020 年 10 月現在において、CTFtime のランキングで 2 位をキープしています。強豪チームの 1 つである dcua というチームから移籍したメンバーが複数おり、その影響もあってかさまざまなジャンルに強いようです。

3　KoreaSuperPower

韓国連合チームです。詳しいことは不明ですが、CodeRed (韓国) チームのリーダーが指揮を執っているようです。予選の TWCTF で出題した問題の 1 つを、新たに発見した 0day で解答し、作問者一同驚いていました。

4　Balsn

NTU (National Taiwan University) の Network Security Lab のメンバーを中心としたチームです。Network Security Lab を略すと NSLab、これを逆さにして baLSN → Balsn というのがチーム名の由来だそうです。
5 年ほど前に登場し、3 年前くらいからさまざまな CTF の決勝戦で見かけるようになりました。幅広いジャンルに精通しており、安定した強さを持ったチームです。

5　hxp

ドイツのチームです。学校名は失念しましたが、ドイツにある大学の学生を中心としたチームのようです。10 年ほど前からさまざまな CTF に参加している歴史の長いチームで、海外の決勝戦でも見ることも少なくありません。去年 CCC (Chaos Communication Congress) の CTF の運営を務めており、非常に質の高い問題が多数出題されたのが印象に残っています。

6　ALLES!
ドイツのチームです。5 年ほど前から活動しており、3 年前くらいから海外の CTF の決勝戦で見かけるようになりました。このチームのメンバーでとりわけ有名なのは LiveOverFlow 氏です。YouTube でさまざまな動画を配信しており、この界隈の人は一度は見たことがあるのではないでしょうか。あまり交流がないため多くの情報を持ち合わせていないのですが、pwnable に強い印象があります。

7　Plaid Parliament of Pwning
説明不要だと思いますが、CMU (Carnegie Mellon University) のチームです。事実上の世界トップですが、最近は卒業した OB が忙しいためか、ぶっちぎっている様子はあまり見なくなりました。代わりに CMU の現役の学生がメインとなって参加しているようです。OB がいなくても十分な強さを持っており、サークル内で定期的にミーティングを開いたり、解いた問題の復習などを行なって良い循環を作っているようです。強さの秘訣ここにあり、という感じでしょうか。

8　p4
ポーランドのセキュリティコミュニティをベースとしたチームです。同じくポーランドでは Dragon Sector というチームが有名ですが、今回はあまり参加するメンバーがいなかったようです。p4 の特筆すべき強さは何と言っても misc というジャンルの問題に対してであり、他の CTF でも solve 数が少ない問題を唯一解いている様子を見かけます。misc だけでなく web、pwnable にも安定した強さを持っており、強豪チームの 1 つです。

9　TSG
東京大学の TSG というサークルのメンバーで構成されたチームです。crypto に強いメンバーがいる印象が強く、もちろん他のジャンルについてもバランスが取れています。前回の CBCTF は惜しくも TWCTF で予選敗退となってしまったため、今回は新 Bull's Eye を楽しんでいただけたらと思います。

10　BlackBauhania
香港のチームです。去年から活動しているチームのようですが、詳細は全く知りません。しかしながらメンバーを見ると、VXRL のメンバーが複数人見られるため、香港のセキュリティコミュニティをベースとした新チーム、といったところでしょうか。香港のチームを見る機会はあまりなかったので、今後どこかの CTF の決勝戦で会えるのを楽しみにしています。

Twitter で幅広い層にアピール

みんなの「サイバーセキュリティコミック」好評配信中！

文＝斉藤健一

JNSA が Twitter を使ってコミックを配信

JNSA（NPO 日本ネットワークセキュリティ協会）は、本年 9 月 18 日より協会の Twitter アカウント（@jnsa）にて、“ みんなの「サイバーセキュリティコミック」” の配信を開始した。ツイートに添付する画像をページに見立てた 4 ページの短編コミックとなる。毎週金曜日に 1 話ずつ配信され、11 月 6 日まで続く予定だ（全 8 話）。

ご承知のとおり、サイバーセキュリティは政府をはじめあらゆる組織が抱える喫緊の課題である。さらに、この課題は個人にも大きく関係している。例えば、個人宅に設置されたルーターをはじめとする IoT 製品。セキュリティが考慮されていない古い製品が使い続けられることも多く、マルウェアに感染してサイバー攻撃の踏み台にされるといった問題も指摘されている。ところが、一般の人にとってサイバーセキュリティを自分のこととして捉えることは難しい。これは、サイバーセキュリティの啓発に取り組む際に、もっとも苦労する点だ。人気アニメやコミックのキャラクターとタイアップするなどして啓発活動を行なったり、コンテンツをマンガにしたりすることで、分かりやすさを訴求した事例は過去にもあった。

今回の取り組みがユニークなのはメディア（媒体）として Twitter を選んだことだろう。近年、プロアマを問わずクリエイターが Twitter を使ってイラストやコミックを発信しており、「100 日後に死ぬワニ」のように大ヒットした作品もある。1 回のツイートで伝えられるのはテキスト 140 字と添付画像 4 点までに限られている。その反面、お手軽に発信できるのが Twitter の特長であり、ツイートを見たユーザーも気軽に RT（リツイート）

みんなの「サイバーセキュリティコミック」第 3 話より
JNSA の Twitter アカウント（@jnsa）で配信中
https://x.com/jnsa/

して情報が拡がっていく。つまり、“ みんなの「サイバーセキュリティコミック」” とは、コミックが持つ物事を分かりやすく伝える力と、Twitter の拡散力との合わせ技の企画だといえる。

サイバーセキュリティの現在が分かるテーマ設定

“ みんなの「サイバーセキュリティコミック」” の企画がスタートしたのは本年 4 月下旬だ。コミッ

クのテーマは一般から広く募集し、その後テーマに沿ったストーリーとコミックが制作された。運営には角川アスキー総合研究所と KADOKAWA が携わっており、原作・作画ともに第一線で活躍するクリエイターが担当している。ストーリーは以下のとおり。

社会人 1 年目の藤宮ユリルは何に対しても積極的で、ふとしたきっかけからサイバーセキュリティのプロフェッショナルたちと交流するようになる。そして、彼らの力を借りながら、社内や身の回りで起きたサイバーセキュリティのトラブルを解決していく、というものだ。

記事執筆の時点（本年 10 月 23 日）で、第 6 話まで公開されている。そのラインナップは、

第 1 話「AI を活用したセキュリティ対策」
第 2 話「リモートワークのセキュリティ対策」
第 3 話「ネットワークに繋がる工場へのサイバー攻撃の脅威」
第 4 話「クラウドのセキュリティ対策」
第 5 話「サイバー攻撃の温床となる IoT 危機」
第 6 話「フェイクニュース」

となっている。どのテーマも現在の社会が抱えるセキュリティのトピックだ。Twitter ユーザーからの評判も上々のようで、毎回着実に「いいね」を集めている。

もちろん、4 ページという分量では、できることも限られているし、絵の好みもあるかもしれないが、Twitter アプリや Web ブラウザーで、ものの数分で読むことができる。また、気軽に「いいね」を付けたり、「RT」したりすることがきっかけとなって、セキュリティには無縁の「誰か」に作品が届くかもしれない。本誌読者の皆さまにもぜひこの手軽さを愉しんでいただきたい。

Hitachi Systems Security Journal を
最後までお読みいただきありがとうございます。

CODE BLUE 2020 開催期間中、このページを見つけた人は、OpenTalks での応募に加えて、計 3 回の応募が可能となります。
アマゾンギフト券 2000 円を抽選で 10 名様にプレゼントしますので、当社ページに設置した応募フォームに下記のキーワードを入力してご応募ください。

【キーワード 1】
みんなの「サイバーセキュリティコミック」第 1 話に登場する
セキュリティエキスパート（女性）の「HN(ハンドルネーム)」
※ヒント：会期中に流れる当社 CM にも紹介されます

【キーワード 2】
ベン・ナッシ氏が発案した新しい長距離盗聴手法
「L 〇〇〇〇〇〇 e」

※ 日本の居住者が対象です。 海外からの参加者は対象外です

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.40

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