HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.41

株式会社 日立システムズ

Human * IT

Hitachi Systems security Journal VOL.41

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

大幅に刷新された SECCON CTF のネットワークインフラの概要

SECCON CTF NOC チーム インタビュー

取材・文＝斉藤健一

SECCON は、JNSA（NPO 日本ネットワークセキュリティ協会）が主催するセキュリティコンテストで、業界有志のボランティアによって運営されている。2012 年からスタートし、今では世界トップレベルの参加者が集う世界規模の大会へと成長した。今回のインタビューではその舞台裏に迫ってみたい。SECCON といえば、サイバー空間を独自に描写した競技の可視化システムが有名だが、焦点を当てるのはネットワークインフラチームだ。彼らが担当するのは、カンファレンス・競技会場の物理ネットワークや CTF の競技ネットワークの構築・管理などで、まさに大会の屋台骨を支えていると言っても過言ではない。今回は、2019 年に導入した競技ネットワークのクラウド化を中心に、SECCON ネットワーク改善の取り組みについて伺った。なお、インタビューは 2020 年 12 月にオンラインで行なっている。

SECCON ネットワーク改善のきっかけ

斉藤（以下 S）：早速ですが、2019 年の SECCON 会場で野村さんが登壇したインフラ &NOC チーム（以下 NOC チーム）のセッションを聴き興味を持ちました。以前の SECCON CTF では Windows 上の VirtualBox で問題サーバーを構築していたという話には驚かされました。これはいつ頃の話なのでしょうか。

野村（以下 N）：2015 年か 2016 年くらいまでだったと思います。

S 大会の規模からすると信頼性が低いというか貧弱な環境だと言えますね。

N 個人的には「サイテー」だと思っていました。草創期の SECCON は実行委員の手弁当で運営しており、ネットワーク構成なども古かったのです。実際のところネットワークが不安定で原因不明のトラブルが発生し、決勝戦の開始時間が遅れるという事態になったこともあります。

S 野村さんが SECCON に関わるようになったのはいつ頃からですか。

N 2016 年からです。元々 SECCON Beginners のスタッフとして参加してました。当時は東京電機大学の学生で、SECCON が母校で開催されるということで、会場ネットワークの構築にも携わるようになりました。このとき、自分の許容量をはるかに超えるタスクの山に閉口しました。そこで翌年から、問題作成よりもネットワーク構築に注力するようになりました。

S 2017 年からインフラの改善に取り組み始めたということですが、他の方が SECCON に関わるようになった時期や経緯を教えてください。

前田（以下 M）：私は元々 Beginners の NOC を担当しつつ、会場ネットワークにも携わっていました。そこで野村さんと親しくなったのですが、SECCON の NOC チームで人手が足りないからと、駆り出されました。2018 年のことです。

S 浅野さんはいかがですか。

浅野（以下 A）：前田さんとほぼ同じです。Beginners を手伝っていたところ、2018 年に野村さんから SECCON を手伝ってほしいと打診されたのがきっかけです。

S 小障子さんはどうでしょう。

小障子（以下 K）：参加は 2019 年からです。経緯については記憶が曖昧です。誘われたのは野村さんからだったのか、それとも会場のネットワークインフラを担当していた別の方からだったのか。

N 私から声を掛けました。小障子さんとは一緒にネットワークインフラを構築した経験が何度かあり、以前から声を掛けたいと考えていました。

SECCON インフラ &NOC チームのメンバー

野村敬太（nomuken）
全体的な調整、問題リポジトリ管理、スコアサーバー管理など

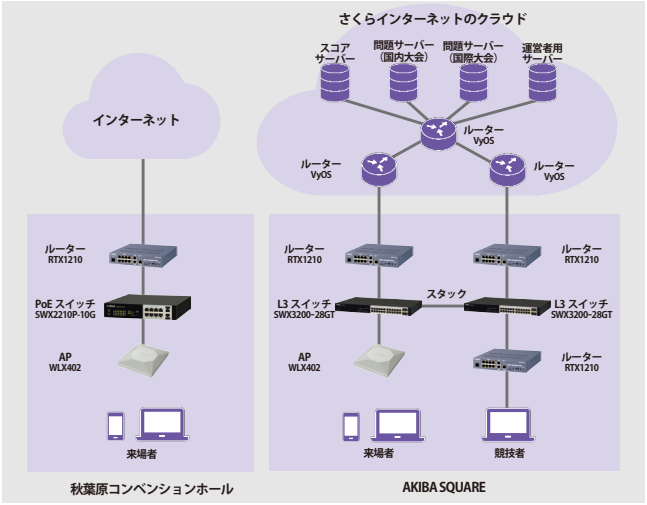
前田章吾 (akira)
CI 対応とクラウドリソース管理

浅野大我 (atpons)
問題の監視、チーム内サービス管理

小障子尚太朗 (koshoji)
競技含む会場ネットワーク構築と管理・運用

大幅刷新 !!
クラウド化した CTF 競技ネットワーク

S 2019 年に競技ネットワークをクラウドに移行することとなります。
N 個人的には「近代化」と呼んでいます。
S 話を伺う前に確認したいのですが、SECCON CTF のネットワークを構成する要素は何でしょう。こちらで思いつくところを挙げると、問題サーバー、スコアサーバー、競技参加者が利用するネットワーク、NIRVANA などの可視化システムです。
N 参加者側から見るとそのとおりです。加えて、問題作成にあたり検証用の問題サーバーがあったり、ネットワーク監視のダッシュボードがあったりします。
S 2019 年にクラウドに移行したものは、問題サーバー、スコアサーバー、可視化システムということでよいですか。
N そのとおりです。
S 2019 年の事例で考えると、会場の競技ネットワークからクラウドの問題サーバーにはどのようにアクセスしていたのでしょうか。
N 単純に拠点間 VPN で接続しています。また、競技トラフィックと会場のインターネットトラフィックは分割されています。
S 続いて、それぞれの方の担当について伺います。前田さんはクラウドのサーバー構築などを担当されたと伺っています。どのようなことに取り組まれたのですか。
M 同じ構成の仮想マシンをいくつも立ちあげるために、以前は、ボタンをポチポチと押してサーバー



SECCON CTF 2019 の会場ネットワーク構成図
物理ネットワークは YAMAHA の機材を利用し構築。問題や監視サーバーなどをさくらインターネットのクラウド側に置き、トラブル対策のため冗長構成となるようクラウドと物理ネットワークを接続した。

をセットアップしていましたが、手間も時間もかかるということで、これを自動化しようということになりました。インフラストラクチャー・アズ・コード（Infrastructure as Code：IaC）という手法です。構成管理ツールも数多くあります。設定ファイルを作成しておけば、サーバーのセットアップから各種設定、必須ソフトウェアのインストールまでを自動で行ない、さらに問題作成者に対してアクセス方法（IP アドレス・ユーザー ID・パスワード）の告知までを自動でできるようになりました。さらに構築環境のテストからデプロイ（利用可能な状態にする）までの自動化にも取り組みました。いわゆる CI/CD（継続的インテグレーション／継続的デリバリー）と呼ばれるシステムです。

S 大幅な省力化が図られたと推察します。クラウド移行前は当然物理マシンが何台も繋がっていたわけですよね。

M クラウド化以前のことは野村さんの方が詳しいと思います。

N 以前はシンクライアントのようなコンピューターがずらっと並んでいました。ネットワークスイッチにつなぐだけでも大変でした。

S クラウドに移行することで、ネットワーク構築の労力はどの程度減らせたのでしょうか。

N 当初、SECCON CTF は閉じたネットワークでの競技を想定していました。ですから物理マシンが必要だったのです。しかし、そうなると物理マシンが足かせとなって、問題サーバーのデプロイが遅れてしまいます。そもそも、日程や予算の都合から会場が借りられるのは 3 ～ 4 日間ほどです。これまでは、開催前に別の場所に物理マシンを設置していました。問題作成などの関係者はマシンを設定するためだけにわざわざその場所に行く必要がありました。

S それは効率的ではありませんね。

N 当時、問題作成には 5 名～ 6 名が携わっていました。もちろん、みなさんそれぞれお忙しい方々です。それでも、マシンの設置場所に来て準備しなくてはなりません。ネットワークも仮組みしておいたものをスケジュールに合わせて会場に発送する。会場では届いた機材を使ってネットワークを構築する作業を進めます。クラウドに移行することでそういった行程がなくなり、負担は大きく減ったと考えています。

S NOC チームだけでなく、問題作成者の負担も大幅に軽減できたのですね。前田さんに再び伺います。IaC や CI/CD の導入は SECCON には画期的なことだったと言えますが、IT 業界では広く普及しているものなのでしょうか。

M ソフトウェア開発などで多くの企業が導入しています。

S 野村さんの発言で「近代化」という言葉が出てきましたが、前田さんとしても同じ感覚ですか。

M 自分の中でも同様の感覚です。

S 続いて浅野さんに伺います。問題サーバーの監視やチーム内サービスの監視を担当されたとのことですが。

A はい。この背景には問題サーバーの稼働状況に関する質問が多かったことが挙げられます。SECCON CTF の予選はオンラインで行なわれています。質問は IRC などで受け付けていますが、問題サーバーの稼働を確認する質問も多いのです。競技は 24 時間体制で行なわれているので、質問がある度に、作問者にリレーして確認してもらうのは、なかなか大変です。そこで、作問者にあらかじめ問題が解けるようなスクリプトを書いてもらっておき、例えば 10 分おきに実行するようにしておきます。スクリプトの実行結果に問題が発生した時だけ NOC チームに通知するようにしました。また、各問題に対して Solve Badge を設けることにしました。これは、その問題が解ける状態にあるかどうかを参加者に示すものです。本戦でも問題サーバーが稼働しているか否か、どの程度の負荷がかかっているのかなどを可視化して、インフラチーム内で情報の共有を行なっていました。

N CTF では Web サービスが正常に動作しなくなることも多々あります。このとき、参加者からすると、環境に問題があるのか、それとも自分たちのやり方が間違っているのか、分からないことがあります。こうした理由から競技中の参加者からの問い合わせがひんぱんに来ます。世界各地から参加者が集まってくるのでタイムゾーンもバラバラです。日本では深夜であっても「サーバー生きてる？」という問い合わせがしょっちゅう来て、われわれも寝ることができません。作問者も人間ですから当然睡眠が必要です。こういった事態に陥らないように、実際に問題が解ける状態にあるかどうかを参加者に示したかったのです。そこで、浅野さんにさまざまなツールを作ってもらうなどの準備をお願いしました。

S 他にはどんな不便があったのでしょうか。

A 作問者に問題サーバーを引き渡す時には、ID やパスワードに加えて監視サーバーのダッシュボードのアカウントやインフラチームが使用しているサービスのアカウントなど、いくつもの ID やパスワードも伝えていました。これらは NOC チーム内で Wiki を用意するなどして管理していましたが、やはり手間がかかります。また、クラウドでは設定ファイルを実行するとインスタンスがすぐに起動するので、作問者にパスワードを渡すタイミングも見定めにくいのです。そこで、「ゼロトラスト」を取り入れ、自分たちでパスワードを管理することはやめることにしました。

S 具体的にはどのようなシステムなのですか。

A まず、リバースプロキシを用意して、前段で ID/ パスワードを受けます。その後 IRC サーバーや監視ダッシュボード、問題サーバーなどにアクセスするのですが、ここで使われる個別の ID/ パスワードをなくすことにしました。作問者の Gmail アカウントを ID プロバイダーとして設定に取り込み、このアカウントをパスワードなしで通すようにしたのです。

S 続いて小障子さんに伺います。競技を含む会場ネットワークの構築と管理を担当されているそうですが、物理ネットワークを構築する上で重要な点とは何でしょうか。

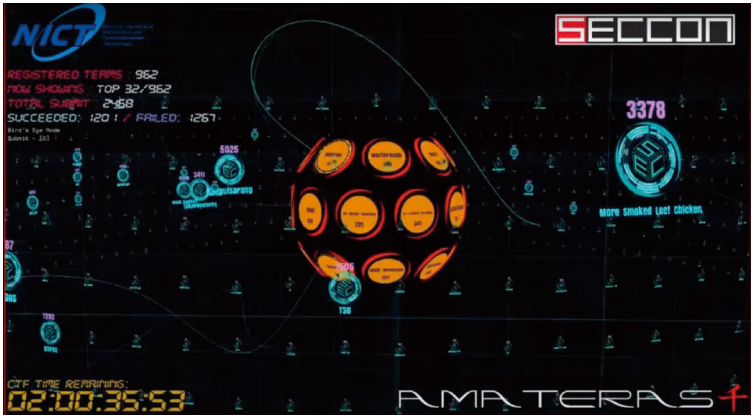
K 物理ネットワークで重要な点は「落ちない」ということです。CTF 決勝戦には日本国内はもとより世界各国から参加者が集まってきます。彼らが競技に集中できるようにしなくてはなりません。ですから、ネットワークが落ちて競技時間を削るようなことがあってはならないのです。

S VPN 接続とはいえ、競技ネットワークはインターネットを利用しています。攻撃が競技ネットワークの外に及んでしまったり、クラウド側で何か異常を検知したりするようなことはありませんでしたか。

N 競技ネットワークに制限を加えることはしたくありませんでした。というのも、参加者は制限を嫌う人たちだからです。何が競技に影響を与えるかわれわれには分かりません。ですから外部への攻撃は厳禁というルールを設けました。とはいえ、これはあくまで紳士協定です。もし何か問題が発生すればわれわれが責任をとらなくてはなりませんし、情報も提供しなくてはなりません。そういった点を考慮して、すべてのパケットをキャプチャーしておき、万が一トラブルが発生した場合でも、調査・回答できる体制は整えていました。

S なるほど。

N クラウド側でも対策はしていました。参加者が



AMATERAS 千
中央にはオレンジの円を配した黒い球体が浮かぶ。それぞれの円は各ジャンルの問題を表している。一方、球体周辺は無数の円が取り囲んでいる。こちらの円は参加チームを表している。そして、周囲の円から球体に伸びる線は攻撃を表す。AMATERAS 千にはいくつかの表示モードがあり、図は得点上位 32 チームでフィルターをかけたところだ。

制圧したサーバーが外部ネットワークに対して攻撃できないようにする制限や、トラフィックに影響が出ないような設定にはしていました。

S 競技ネットワークのパケットをすべてキャプチャーされているとのことですが、DEFCON CTF のように、これを公開する予定などはありますか。

N 個人的にはやりたいのですが、プライバシーの観点から難しいと考えています。というのも、参加者が競技ネットワークから所属組織のコンピューターに接続したり、さらに平文パスワードが含まれていたりするからです。

S 公開すればひんしゅくを買いますね。

N 話はそれますが、競技参加者が問題サーバーに対してどのような攻撃をしているかというデータについては NICT（情報通信研究機構）に提供しています。また、パスワードつながりでいえば、NOC チーム内で、DEFCON の Wall of Sheep なども面白いと話題になることがあります。ご存じだと思いますが、これは会場ネットワーク内に流れる ID/ 平文パスワードを掲示してしまう企画です。もちろん、実行委員会内での議論・調整が必要ですが、参加者に対して面白いものを提供していきたいという気持ちは持っています。

2020 年の SECCON CTF

S 話題を移して 2020 年の SECCON CTF について伺います。今大会はオンラインに移行するとともに予選と本選が 1 つとなりました。

N 本戦の会場がないというのは寂しいと思いつつも会場ネットワークの設営がない分、楽ができるという両方の気持ちがありました。とはいえ、オンライン上ですべて完結させるわけですから、そこに力を注いでいかなくてはなりません。

S 運営面で大きく変化したことはありますか。

N これまでも予選はオンラインで開催していましたから、実際のところ変化はそれほど大きなものではありませんでした。しいて挙げるとすれば、ミーティングがすべてオンラインになったことと、チーム内のコミュニケーションに使っている Discord の利用頻度が上がったことでしょうか。

S 力を注いだのはどのような点だったのでしょうか。

N 開発に力を注ぎました。スコアサーバーを独自のものに変更しようと作業を進めていました。ただ、開催直前にちょっとした問題が発生して例年のものを利用することになってしまいましたが。

S 会場ネットワークの設営がなくなりましたが、小障子さんの作業はどのように変わりましたか。

K 会場ネットワークの準備は結構大変です。開催前から業務後の時間に会場へ通い、ケーブルを敷設したり設定を行なったりします。オンラインへの移行でそれらの準備がなくなりましたから、今回は開発の手伝いをしました。

S 前田さんの作業に変化はありましたか。

M IaC はインフラの管理をコード化することです。コードなので当然、再利用が可能です。今年は昨年のコードを使うことによって、短時間で作業を済ますことができました。その分、開発に力を注

ぎました。この点が大きな変化です。

S 浅野さんはいかがでしょう。

A SECCON CTF 決勝戦では、例年 NIRVANA 改による競技の可視化が行なわれていました。可視化システムの開発は NICT が担当しています。今年はオンライン大会でも可視化を行なうということで、NICT の方が Twitch で配信を行ないました。ですが、例年の決勝戦と今年の大会は競技方式が異なるのでスコアサーバーのシステムが異なります。つまり例年だと予選で使っているスコアサーバーと可視化システム（AMATERAS 千）をつなぐ必要が出てきました。この接続部分を担当することとなり、開催直前まで作業を続けました。

S なかなか大変そうな作業です。

A われわれにとってもチャレンジでした。NICT 側では参加1000チームまで対応するようにしました。われわれの作業は、問題が解かれた瞬間にデータベースを更新して可視化システムに連携するというものでしたが、この作り込みに苦労しました。

N 可視化システムについて補足なのですが、NIRVANA 改は King of the Hill という形式を可視化するシステムです。一方、今回の大会はジェパディ（Jeopady）形式で開催されました。NIRVANA はこの形式には対応していないので、CTF for Girls が攻殻機動隊とコラボした大会で利用したシステムをベースとしました。

S 読者の方に補足すると、King of the Hill は大雑把に、問題サーバーを制圧・占有し続けることによって得点を得る形式で、ジェパディはいわゆるクイズ形式です。

N 準備期間中、NICT 側もわれわれも互いに「モノ」がない状態で作業を進めなくてはならないので、例年の状態を変更しないように仕様のすり合わせを行ないました。その結果、過去のスコアサーバーに仕様を合わせざるを得なくなりました。

S 先ほどの発言にあった、開催直前に元のスコアサーバーに戻した理由とはこのことなのですね。お話の端々から相当のご苦労があったように感じます。

今後に向けて

S SECCON CTF 2021 の話は出ているのですか。

N 現時点ではまだ決まっていないことが多いです。あくまで個人の意見ですが、新型コロナの勢いはまだ収まらないだろうと思っています。そして、2021 年の大会の枠組みがオンラインでの予選・決勝戦となったとしても対応しなければならないと考えています。

S 最後の質問です。みなさん、NOC チームの活動を通じて、さまざまな知見を得てきたと思いますが、今後の活動はどのようにお考えですか。このまま続けるのか、それとも次世代へと繋げていこうと考えているのか。

N 良い質問であり難しい質問でもあります。あくまで個人の意見ですが、SECCON の NOC チームを後進に譲るのはまだまだ難しい状況だと感じています。というのも、現状は、前田さん・浅野さん・小障子さんそれぞれが業務や個人の活動を通じて得た知見を集めたに過ぎないからです。SECCON という組織を考えると、いまだ「負債」を抱えている状態だと感じています。

S 負債とはどういうことでしょう。

N いまだ安定した運営ができる状態にないということです。まずは負債を返す、つまり余裕を持つことが先決です。そうすれば、仮に新たにことにチャレンジして、たとえそれが失敗したとしても、「失敗だったね」と済ませられます。こうした余裕がないと次の世代にバトンは渡せないと思います。

S 余裕は必要ですね。

N 2020 年にようやく「手法」が安定してきたという状況です。ですから 2021 年〜 2022 年にかけて新たな人たちに声をかけてバトンを渡していきたいと考えています。バトンを渡すというのはきれいな言い方ですが、悪くいえば「押しつける」になるかもしれませんが、いろいろな形で機会を回してきたいと考えています。

S みなさんの今後のご活躍に期待しています。ありがとうございました。

国内最大の CTF 大会がオンラインで開催

SECCON CTF 2020 レポート

インタビュー・文＝斉藤健一

新型コロナ禍でオンライン開催となった SECCON CTF 2020

2020 年 10 月 10 日・11 日の 2 日間、SECCON CTF 2020 がオンラインで開催された。SECCON とは Security Contest の略であり、情報セキュリティをテーマに多様な競技を開催するコンテストイベントだ。人材の発掘・育成などを目的に掲げている。JNSA（NPO 日本ネットワークセキュリティ協会）内にボランティアの実行委員会が組織され運営にあたっている。

2012 年にスタートし、現在では世界トップレベルの CTF チームも参加する国際的なコンテストへと発展した。また、カンファレンスやワークショップといった幅広いコンテンツの提供にも力を注いでいる。

例年どおりなら、大会はまずオンライン予選が開催され、それを勝ち抜いた上位チームが一堂に会して決勝戦を戦うはずだった。しかし、新型コロナ禍の影響により 2020 年の大会はオンラインへと移行した。また、予選と決勝という区分もなく、1 回の競技にまとめられることとなった。

2020 年の大会はジェパディ（Jeopady）という、いわゆるクイズ形式が採用された。問題は、Pwn（攻撃コード）、crypto(暗号)、reversing（リバース・エンジニアリング）といったジャンルから合計 28 問（ウェルカム問題・追加問題などを含む）が用意され、参加者を待ち受ける。

競技時間は 10 月 10 日 15 時〜 11 日 15 時（日本時間）までの 24 時間となる。参加者登録もオンラインで行ない、主催者への問い合わせは Discord が使われた。

競技をリアルタイムに可視化する Amateras 千

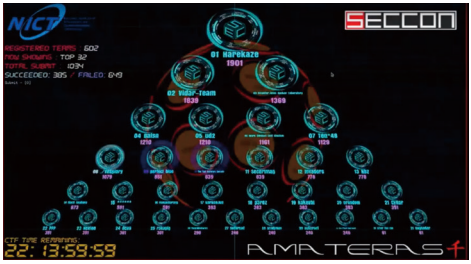
競技の模様は Twitch でリアルタイムにストリーム配信された。競技の可視化には NICT（情報通信研究機構）が開発する「Amateras 千（アマテラス・セン）」というシステムが使われている。SECCON ではこれまで NIRVANA というシステムが使われていたが、これは King of the Hill という競技形式を可視化するものだった。King of the Hill とは、問題サーバーを制圧・占有し続けることによって得点を得る形式で、前述のジェパディ形式とは異なる。Amateras 千は、参加 1000 チームにまで対応し、かつオンラインで行なわれる競技をリアルタイムに可視化しなくてはならないという高い技術が要求されるものとなった。開発は NICT サイバーセキュリティ研究室の井上大介氏を中心に 5 名のメンバーによって進められた。井上氏によると、とてもチャレンジングな課題であり、競技開始後もシステムのデバッグを続けなくてはならなかったという。なお、Amateras 千の概要は次頁の図をご覧いただきたい。

得点が動的に変化する ダイナミックスコアリング

SECCON CTF 2020 では得点が動的に変化する「ダイナミックスコアリング」という仕組みが取り入れられている。競技開始時点で各問題の得点は 500 点に設定されているが、正答するチームの数が増えるとそれに応じて得点が下がっていく。得点上位にランクインするためには正答チームが少ない難問の攻略が鍵となってくる。

CTF 大会の中にはいち早く正答したチームに

Amateras 千の通常の描画。中央の黒い球体が問題サーバーで、背後にある小さなリングが参加チームを表している



順位を表示するモード。ピラミッドのようにリングが並ぶ

問題を表示するモード。円柱の高さで得点が表されている

問題の解答状況を表すモード。各問題と正答したチームが線で結ばれており、よく解かれている問題が一目でわかる

ボーナスポイントが与えられることもあるが、ダイナミックスコアリングではこうしたボーナスはなく、正答までに要した時間は得点に影響しない。つまり、正解のフラグをスコアサーバーに登録せずにため込んでおき、競技終盤に一気に登録して順位を急浮上させる戦略も可能となる。はたして、競技終盤に劇的な展開があったのだろうか。勝負の行方については後ほど紹介したい。

競技の裏ではライブ配信も

2020 年の SECCON CTF では競技の裏でライブ配信も行なわれていた。「SECCON CTF 2020 チャンネル」（以下チャンネル）と銘打ち、スポンサー企業によるセッションや実行委員によるリモートビデオ会議などが配信された。実行委員長の花田智洋氏、副実行委員長の寺島崇幸（tessy）氏、事務局長の園田道夫氏らが出演しており、その内容はオープニング・クロージングといった形式的なものから、NICT 井上氏を交えた Amateras 千の解説、さらにオンラインで実行可能なワークショップのアイデアをブレスト的に出し合う企画会議など幅広い。どれも手作り感に溢れており、和気あいあいとした時間が流れる印象だった。なお、配信動画は SECCON の YouTube チャンネルにまとめられており、アーカイブ視聴が可能だ※ 1。

勝負の行方

初日、開始直後の混戦をいち早く抜け出したのは HangulSarang（韓国）だ、17 時すぎに連続得点でトップに立つ。一方、TokyoWesterns（日本）も 18 時すぎに得点ラッシュで逆転し、2 位と 500 点以上の差を付ける。3 位以下はいまだ得点が拮抗している状態だ。19 時にチャンネルはいったん終了するが、競技は引き続き行なわれていた。

順位の変動があったのは夜の時間帯だ。HangulSarang が得点を重ねて合計 5000 点以上を獲得し首位に返り咲いた。TokyoWesterns も奮闘したが得点の伸びは HangulSarang におよばず

※ 1　**SECCON の YouTube チャンネル**　https://www.youtube.com/channel/UCw0dReE5dMUZb90k3gUn2dw

3000 点台にとどまっていた。初日の競技を盛り上げたこの 2 つのチームだが、結果として快進撃はここまでとなり、その後得点を追加することはなかった。

2 日目の競技を盛り上げたのは海外勢だ。More Smoked Leet Chicken（ロシア）は順調に得点を重ね、12 時すぎには TokyoWesterns を抜いて 2 位に浮上する。また、NaruseJun（日本）や ./Vespiary（日本）も得点を重ねて上位に食い込んできた。

このまま大きな順位変動もなく競技は終了するかと思われたが直前になって連続得点するチームが現れた。Black Bauhinia（香港）と perfect blue（米国）だ。特に perfect blue の方は、競技終了まで残り 10 分を切ったタイミングでの連続得点だったので、チャンネルで中継していた実行委員も驚いた様子だった。

最終的に競技には 982 チーム、1862 名の登録があった。最終順位と得点は表とおり。各チームの国籍は CTF TIME ※ 2 の情報を参考にしている。ダイナミックスコアリングによって得点は徐々に下がるため記事中の表記とは異なっている。

なお、記事では CTF の問題には触れていない。気になる方は参加者による WriteUp（解答例）をご覧いただきたい。「SECCON CTF 2020 writeup」といった検索で簡単に探すことができるだろう。

SECCON CTF 2020 最終順位

順位	チーム名（国）	最終得点
1	HangulSarang（韓国）	4750
2	perfect blue（アメリカ）	3875
3	More Smoked Leet Chicken（ロシア）	3462
4	TokyoWesterns（日本）	3240
5	Black Bauhinia（香港）	3057
6	NaruseJun（日本）	2810
7	./Vespiary（日本）	2689
8	Disaster-level Hacker Laboratory（不明）	2615
9	PPP（アメリカ）	2407
10	The Flat Network Society（フランス）	2131

「電脳会議」と題した講演・ワークショップも開催

2020 年 12 月 19 日には「SECCON 2020 電脳会議」がオンラインで開催された。講演は国際色豊かで、DEFCON CTF チームのリーダーを招き、CTF の教育的な側面について議論したり、世界各地の女性セキュリティコミュニティの実情などが語られたりしていた。こちらも SECCCON の YouTube チャンネルでアーカイブ視聴が可能だ。機会があれば本誌でもレポートしたいと考えている。

不要不急の外出の自粛が求められ、自宅で過ごす時間が増える中、こうした動画などを視聴するなどして、スキルアップに繋げてみてはどうだろうか。

※ 2 **CTF TIMES** https://ctftime.org/

オンライン・カンファレンスをリアルと同等に楽しむ

CODE BLUE 2020 オンライン参加レポート

文＝相戸浩志

何だね君はぁ！「ども！ニュースサイトでセキュリティ・コラムを書いている者です！いつも2次元の彼女推しばかりですが、今回はHitachi Systems Security Journalに出張し、2020年10月29日、30日に開催されたCODE BLUEの参加レポートを書かせていただきます」。

CODE BLUEを全力全開で楽しむために

CODE BLUE第1回が開催された2014年2月から本年の第8回まで、筆者はそのすべての回に参加している。もちろん全日フル参加。全力全開で楽しむために、休暇を取得し、費用も自分で負担している。

「自分が聴きたい講演を聴き、自分が繋がりたい人と繋がる」というスタンスだ。業務での参加となると、関連する講演を優先しなくてはならなかったり、会議などの都合で時間どおりに参加できなくなったりするおそれもある。

ラスベガスに行けなくてもBlackHatやDEFCONに匹敵するクオリティの講演が日本国内で聴ける、年にたった一度のチャンスは1秒たりとも無駄にしたくないのだ。

内容が貴重で濃厚なカンファレンスであるほど、参加者もまた全力全開で楽しもうとする濃い人たちが集まってくる。期間中に開催されるネットワーキング・パーティには、講演者をはじめCODE BLUE CTFの出場チームメンバーなども加わり、国際色豊かなハッカー交流の場となっている。

充実の法制度関連セッション

今回のCODE BLUEで筆者が聴きたかったのは、初日に行なわれた法制度関連（Law&Policy）のセッションだ。国内にはセキュリティ系のカンファレンスやシンポジウムが数多くあるが、この分野が最も充実しているのはCODE BLUEだと思う。国際間でのサイバー犯罪の取り扱いや海外の法執行機関の取り組みを、世界トップクラスの専門家から直接聴くことができる。

例えば、ぜい弱性の扱いを取っても、規制の範囲強化はセキュリティ研究者を萎縮させ、攻撃者優位にしてしまうおそれがあり、その線引きはEUでも解釈がさまざまだ。こうしたグレーゾーンでの葛藤は、講演を1つ聴いただけでは分からない。テーマはさまざまだが、すべての講演を通して聴くと全体像がおぼろげに見えてくる。毎年参加して聴けば、さらにはっきりと分かるようになる。

サイバー攻撃が国際犯罪化していくなら、法制度も変わらなくてはならない。諸外国と比較することで、観点も広がり、理解を助けてくれるはずだ。

オンライン開催によるさまざまな変化

毎年、会場は押すな押すなの熱気に包まれていたCODE BLUE。今回はオンライン開催となったが、その熱量に変化はあったのだろうか。また、参加者は満足を得られたのだろうか。

筆者の感想を言えば、オンライン開催でも満足度に変わりはなかった。これは素晴らしいことだ。講演者や運営側がオンラインでは伝わりにくい面があることを承知しており、意識的にカバーしていたからだ。新型コロナ禍でにわかに開催されるようなオンライン・セミナーとの差は質・量ともに明らかだ。

講演者のラインナップを見れば、国内は過去に

好評を博した実績のある面々が、とっておきの新ネタを用意していた。オンライン開催を盛り上げるために一肌脱いでくれたのだろう。CODE BLUE レビューボードの苦労話や CTF 運営の舞台裏といった凄いメンバーが一堂に会したパネルディスカッションは、オンラインでも十分すぎるほどの熱量だった。

脅威インテリジェンスの最前線、IoT 機器にも強い台湾からは、アジア最大級のセキュリティカンファレンスである HITCON の講演者や TeamT5 関係者の講演が目立った。台湾からの友情に胸が熱くなる。その中でも、台湾の新型コロナ対策で世界が注目する天才 IT 担当大臣オードリー・タン氏は、日本のメディアで名前を見ない日はないほどだ。彼女が陽気に分かりやすく説明するデジタル・ソーシャル・イノベーションはとてつもなくスピーディで理路整然としていた。

もちろん、参加側にも、リアルとオンラインの差を埋める意識が必要だ。講演会場に行けば海外から来たハッカーがちらほらコーヒーを飲んでいて、どこかのシンポジウムで基調講演した有名人が客席にいる、そんなテンションが高まる例年の会場参加と、会社の自席でイヤホンを付けて聴いているような状況を、そのまま比較してはいけない。オンラインならなおさら、集中して聴けるように、自宅で邪魔が入らない、広い画面と静かで快適な環境を用意すべきだろう。

会場では例年、講演後には優れた質問による討議が聴け、ネットワーキング・パーティで講演者と議論する機会が設けられていた。ここをどうカバーするかだが、今回、意見を聴く場面は Ask the Speaker というビデオ会議が用意されていた。同時通訳のスタッフが常時待機してくれていたが、筆者は英語が苦手なので、Google 翻訳を駆使して質問した。ここはオンライン開催ゆえに助かったところだ。

オンラインで参加した感想は？

参加無料は苦渋の決断だっただろう。多少の機材トラブルもあったが、参加人数を考えれば問題ないレベルだった。セキュリティ業界は、新型コロナ禍で会場が不要になった分、多くのオンライン・セミナーを開催している。しかし同じような話が多いセミナーと、厳しいレビューボードによってアレンジされたプログラムでは、情報の有益性が桁違いだ。

ちょっと知りたいけれどまとまった情報がない、中国のチャット・コミュニティ QQ の中で何が飛び交っているか、これは翻訳ソフトを駆使しても自分で調べることは困難だ。ネット・スラングや独特の検閲を回避するための言い回しが行なわれているなどは、研究者の説明を聞いて初めて腹落ちする話だった。

NATO を例に同盟国と協力関係を築く必要性を説いたケネス・ギアス氏の講演の後、Ask the Speaker に繋いだら、立派な自宅の応接間だろうか、時差にも関わらず待っていてくれた。「あなたの日本での講演は 10 年以上前の BlackHat Japan から、全部聴いているよ」と伝えたら、凄く喜んでくれて、あの頃は諜報機関の立場で話し、今は NATO で同盟や協調を担っている、10 年で随分立場は変わってしまったよと笑っていた。

BlackHat Japan の講演者・スタッフと打ち上げで行なった新宿のイタリアン・レストランはとても楽しい思い出だ、ぜひ来年はリアルで会おうと約束してくれた。「いつもの CODE BLUE じゃないか。来年、きっと会える」。

筆者注目の講演

「国境を越えたデータへの法執行機関のアクセス：提案された EU e-Evidence 規制の国際的な範囲」アンナ-マリア・オスラ

各国の法執行機関は協調できるのか、守らない国にはどのように対応するのか。サイバーインシデントの捜査において必要な証拠が海外にあるケースは多い。他国の機関に協力を求める刑事共助条約も存在するが、時間がかかるなどの理由から非効率的だと批判されてきた。一方、Tor などの匿名性の高いテクノロジーが使われることによって、データがどの国のどの場所にあるのか特定できないケースや、クラウドコンピューティングの利用でデータの一部が分散しているケースもあるという。さらに、協力を求める際にも国際法に準拠した手続きが必要なのだそうだ。

アンナ-マリア・オスラ氏による「国境を越えたデータへの法執行機関のアクセス：提案された EU e-Evidence 規制の国際的な範囲」の講演動画

イーヤル・イトキン氏による「馬鹿なことはしないで - それはただの電球です」の講演動画

講演タイトルの e - Evidence とは、EU でサービスを提供するサービスプロバイダーに対して、国を通さず直接電子証拠の提出を依頼できる仕組みであり、いまだ議論の最中だという。例えば、EU に拠点がない日本のサービスプロバイダーであっても、EU でサービスを提供していれば e - Evidence の対象となる。一方、米国のプロバイダー法は、もはや国ではなくプロバイダーに主体が移ってきている。

講演者はこれらの問題に対して EU の立場から国際協調に当たっている世界的な権威であり、こうした著名な人物から分かりやすく説明してもらう機会は本当に貴重だと思う。

Ask the Speaker では、当初ツールになれていなくて緊張したけれど、日本が EU にこの問題をアプローチするにはどうすればいいかと投げかけたら、すでに EU 全体としてさまざまなチャンネルが用意されているとのことだった。

「馬鹿なことはしないで - それはただの電球です」イーヤル・イトキン

IoT ネットワーク（電球）を使った、ネットワークへの侵入方法。Philip の Hue という Smart 電球はイギリスで 31% 近いシェアがあるとのこと。この電球では ZigBee という近接ネットワークの無線通信プロトコルが使われているが、その通信はたったの 127bit。講演者は ZigBee のカスタムライブラリのぜい弱性を利用してネットワークへ侵入したという。

攻撃のシナリオは以下のとおり。まず、ターゲットのオフィスにある Smart 電球の色を変更する。すると、ターゲットはスマホから元に戻そうと操作するけれど、画面には「到達不能」と表示されてしまい、それを故障と誤認して、新しい電球に交換し、リセットしてしまう。それは、たくさんの電球をコントロールしているブリッジに対し、故障した電球を削除し、取り換えた新しい電球を検索するようにする操作を伴う。そのタイミングを悪用し、正規の電球になりすまして、ネットワークに侵入する。

「最高です」。日本は網羅的なセキュリティ対策をめざしてチェック項目を増やしていくやり方が主流だけれど、この攻撃を予想して守ることは難しい。こんな回りくどい攻撃を成功させてしまうのは、他には攻殻機動隊くらいじゃないかとさえ思える。マルウェアでもいかに偽装して内部の人間にプログラムを実行させるかが肝になるが、故障を装うあたりは真面目な運用管理者の裏をかく高度なテクニックだと思う。

そこで、これは直接 Speaker に話がしたいと興奮して、講演後に Ask the Speaker に突撃することに。「完全なエアギャップで行ける攻撃だ」、「距離は 50 フィートくらい行けるんじゃないか」、「オフィスだと現実には複数の電球があって干渉するので難しいんじゃないか」と、議論は大いに盛り上がった。

来年の参加は？

今回参加して、筆者は昨年と同じくらいの満足が得られた。オンラインで聴くというのはリアルとは違う集中力のコントロールが必要だったが、覚悟をもって臨めばどうということはなかった。要は、参加者がどう捉えるか、どう準備するかに

かかっている。講演者も、運営側も、コロナ禍でもできることは、分かっている。CODE BLUE は文字どおりのベストを尽くしてくれた。

来年もオンライン開催になったら、参加するのか…「答えはもちろん Yes だ」。CODE BLUE でしか得られない有益な情報が、刺激が、ネットワーキングがある。オンラインでも Speaker と出会える。無償でも有償でも、参加する。もちろん自費で休暇を取って、ベストな視聴環境を用意して。

来年もオンライン開催になったとしたら、それは世界の危機が続いているということだろう。ならば、なおさら危機に立ち向かって意識が高まるのが、セキュリティ担当者だと思う。リアル開催だったら？「そりゃ、講演会場近くのホテルを予約して、終電を気にせず夜中まで酒を飲んでネットワーキングですよ」。

相戸浩志（あいど・ひろし）
情報セキュリティに携わって 20 年。海外含め講演多数。CISSP、CISA、情報セキュリティ監査人。2003 年に上梓した『よくわかる最新情報セキュリティの基本と仕組み』（秀和システム）は第 3 版まで版を重ね、累計実売は 3 万 3000 部。某金融機関 CSIRT の中の人。政府機関の中の人だったことも。現在、ScanNetSecurity にて、コラム「ここが変だよ日本のセキュリティ」を連載中。
https://scan.netsecurity.ne.jp/

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.41

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