HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.36

株式会社 日立システムズ

Human * IT

Hitachi Systems security Journal VOL.36

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

モノ作りを軸に据えたセキュリティ人材育成プログラムを主導

園田道夫 インタビュー

日本のセキュリティ人材育成の取り組みの中で代表的なものと言えば、2004 年に開始された合宿形式のセキュリティ・キャンプや 2012 年に開始された SECCON CTF が挙げられる。どちらの取り組みも開始当初は周りから奇異の目で見られていたが、現在では当たり前のものとして受け入れるようになった。今回、話を伺う園田氏はどちらの取り組みにも携わるセキュリティ人材育成の指南役のような存在。そんな園田氏が今度は国立研究開発法人情報通信研究機構（NICT）で SecHack365 という新たなプログラムに取り組んでいるという。早速その概要について伺うこととした。

取材・文・撮影 = 斉藤健一

SecHack365 とは

斉藤（以下 K）：園田さんは国立研究開発法人情報通信研究機構（NICT）ナショナルサイバートレーニングセンターのセンター長を務められています。本日はセキュリティ人材育成をテーマに、NICT が主催する SecHack365（以下 SecHack）をはじめ、さまざまな視点から話を伺いたいと思います。よろしくお願いします。

園田（以下 S）：こちらこそ。よろしくお願いします。

K NICT の Web サイト※1 によれば、SecHack とは 25 歳以下の学生・社会人を対象とした「若手セキュリティイノベーター」の育成プログラムで

※1 **SecHack365** https://sechack365.nict.go.jp/

あり、サイバーセキュリティに関するソフトウェアの開発・実験・発表を行なう長期のハッカソンだとされています。この「セキュリティイノベーター」とはどのような人材なのか、この点から教えてください。

S セキュリティイノベーターを一言で説明すれば、セキュリティに関わるモノづくりができる人材ということになります。セキュリティ・キャンプ※2をはじめとする人材育成プログラムがいくつも立ち上がり、優秀な人材が出てくるようになりましたが、モノ作りの観点からすると、日本発のセキュリティ・プロダクトの数はいまだに少ないのです。

K こうした状況に危機感を持つ業界の方もいらっしゃいますね。

S ここ数年、セキュリティ・キャンプでもモノ作りに寄ったコンテンツが増えてきました。NICT内でもセキュリティ人材育成の取り組みを検討していた時に、この流れに呼応するアイデアが出ました。「1年間のハッカソン」というものです。ただよく考えるとこれは矛盾しているとも言えるのですが…

K 確かに。ハッカソンというと合宿をするなどして短期間で開発効率を高めていくイメージがあります。これは園田さんのアイデアなのですか。

S 発案者は別にいます。これまで誰もしたことがない試みですから、逆にチャレンジしてみる価値があると思いました。プロダクトはソフトウェアだけに限らなくてもよい。そんな仕組みにしたいとも思いました。例えば、セキュリティ啓発系のコンテンツであればストーリー仕立ての映像であっても構わないのです。

K 柔軟な発想ですね。

S 啓発系の話題が出ましたので、関連する話をすると、トレーニー（SecHackの受講者）がPythonのセキュリティプログラミングに関する技術書を執筆したという実績があります。これも技術に関心がある人を対象とした啓発コンテンツだと言えると思います。

K SecHackのスタートは2017年、園田さんがNICTのナショナルサイバートレーニングセンターのセンター長に就任したのも同じく2017年です。これには何か関連があるのでしょうか。

●園田道夫（そのだ・みちお）

工学博士。2004年より経済産業省、JIPDEC、IPA主催セキュリティ・キャンプに企画、講師、実行委員として携わる。2012年よりSECCON実行委員（事務局長）。2014年サイバー大学IT総合学部教授を経て、2016年NICTセキュリティ人材育成研究センター長、2017年ナショナルサイバートレーニングセンター長に就任。

S 経緯をお話しすると、NICTが人材育成に乗り出したのは2016年4月のことです。ナショナルサイバートレーニングセンターの前身となる人材育成研究センターが立ち上がりました。私がNICTに入所したのは同年6月のことです。人材育成の大きな事業としてすでにCYDER※3（CYber Defense Exercise with Recurrence）が立ち上がっていました。実践的なサイバー防御演習で、手間も時間もかかる事業です。入所した当初はCYDERをどのように運営していくのかがメインのミッションだったのです。

K なるほど、そうでしたか。

S そしてもう1つ、サイバーコロッセオ※4事業も決まっていました。こちらは東京オリンピック・パラリンピック2020競技大会の安定的な運営に向けて大会関連組織のセキュリティ関係者を対象に行なわれるサイバー演習です。以上の2つは形

※2 **セキュリティ・キャンプ** https://www.security-camp.or.jp/
※3 **CYDER** https://cyder.nict.go.jp/
※4 **サイバーコロッセオ** https://www.nict.go.jp/press/2017/12/07-1.html

が見えていましたが、事業の柱がもう 1 本欲しいと検討していました。この時に出たのが先ほどのアイデアだったのです。

K SecHack スタートの経緯がよく分かりました。

SecHack で求められる人物像

K 長期間のプログラムといえば、経済産業省が主催している未踏事業が挙げられると思いますが、未踏と SecHack との違いは何でしょうか。

S 未踏の場合はすでに作りたいモノが決まっていて、作り方は採択された人に任されています。一方、SecHack は作りたいモノがおぼろげな人であっても指導し、アウトプットを出していこうとする取り組みですから、未踏未満だとも言えます。もちろん SecHack でも作りたいモノが最初から決まっている人たちもいます。どちらの人たちにもトレーナー（指導者）が持つモノ作りのノウハウを存分に注いでいます。

K NICT の Web サイトによると、CYDER やサイバーコロッセオは中級者程度のスキル、ピラミッドでいうところの中間を対象にしています。一方、SecHack はピラミッドの頂点をターゲットにしています。どのような人たちが集まってくるのでしょうか。

S 未踏未満とはいえ、選考基準はセキュリティ・キャンプと同等ですから、集まるのは三角形の頂点の人たちということになると思います。その中からできるだけユニークな人材、具体的には人と違った視点から発想できる人、さまざまなスキルを持っている人を採っています。

K 先ほどと同様に Web サイトからの引用ですが、選考は毎年 4 月に行なわれていて、応募方法は課題の提出となっています。2019 年は 295 名の応募に対して合格者が 50 名ほど。この課題というのはどのような内容なのでしょうか。

S SecHack にはいくつかのコースがあり、課題はコースによって異なります。コースをいくつか紹介しながら質問にお答えします。1 つは開発駆動コースです。ここには開発したいモノが決まっている人たちが集まっています。活動の内容としては、2 カ月に 1 度の割合で進捗の確認を行なったり、プロダクトの工夫すべきポイントなどを議論したりしながら完成へと向けて進めていきます。

K 開発の分かりやすいイメージですね。

S それとは全く別で思索駆動というコースがあります。どちらかというと人間を作るアプローチです。世の中の常識に疑いを持ち、社会を良い方向に変えるような課題に基づき議論を深めていくような活動をしています。順調に成果物が出てくるとは限りません。

K 哲学的なコースともいえそうですね。

S このようにコースによって活動は異なりますし、求められる人物像も異なります。話を質問に戻すと、開発駆動コースを希望する人に求めるのは、過去に何を作ったかという実績で、課題ではそれを中心に聞きます。一方、思索駆動コースの人たちには、現代社会においてセキュリティの分野でどのような課題があるか、何か未解決な課題はあるか、あるいは未解決の問題に対してどのようなアプローチが考えられるか、といったことを聞きます。

K 選考方法は書類審査のみですか。

S はい書類審査オンリーです。

K だとすると書類から感じ取れる応募者の熱意が合否のポイントになると思うのですが、審査する側は書類だけを見て、その熱意をキャッチできるものなのでしょうか。

S なんといったらよいか迷う部分もありますが、正直に言うと感覚で分かります。というのもこれまで 16 年間、セキュリティ・キャンプで書類を見てきました。多いときで 300 ～ 400 名分の書類に目を通します。それによってかなりの暗黙知が蓄積されていますし、試験対策として先輩から後輩へと応募書類の書き方が伝授されているようですが、いわゆる大人が喜びそうなフレーズ（わたしはこれまでこれだけ沢山手を動かしました的なもの）が書いてあったとしても、その人の GitHub アカウントを見れば、それが本当かどうか裏をとることは可能です。

K セキュリティ・キャンプの話題が出ましたが、セキュリティ・キャンプと SecHack とで参加者の重なりなどはあるのでしょうか。

S 重なる人は一定の数います。先にお話ししたとおり、セキュリティ・キャンプでも近年モノ作りを基軸にしようとしています。2 つの取り組みのコンセプトは似た部分もありますから、応募者が似てくるのも必然だと思います。

K SecHack のコースはいくつあるのですか。
S 開発駆動・表現駆動・思索駆動・学習駆動・研究駆動の 5 つです。
K 応募はどのコースが多いのですか
S 応募が多いのは表現駆動です、このコースではテーマは決めていても決めていなくてもよいというフレキシブルな受け入れをしています。学生からするとこういった点が応募しやすいのだと思います。
K SecHack のトレーニーは開発したいものが最初から決まっているのか否か、インタビューをする前は疑問に思っていたのですが、話を伺い合点がいきました。

十全な研究・開発環境

K SecHack では NICT の遠隔開発環境 NONSTOP が使われているとのことですが、NONSTOP とはどのようなものなのでしょうか。
S NICT では 30 万 IP アドレスを対象にダークネットを観測しています。ここではマルウェアの検体などを含めて怪しいデータが収集されています。SecHack ではこうしたデータも提供しようと考えました。ネットに拡散すると危険ですから、解析ツールも含めた環境のすべてを隔離されたクラウドの中に構築しています。これが NONSTOP というシステムです。もちろん検体をクラウドの外にコピーすることはできません。
K Web サイトには StarBED という名称も出てきますが、こちらはどういったものなのでしょうか。
S StarBED とは大規模なインターネットシミュレーターです。先ほどの NONSTOP は、この StarBED というプラットフォーム上で稼働しているシステムなのです。
K NONSTOP と StarBED との関係は理解しました。ちなみに怪しいデータを研究・開発に活かしているトレーニーは多いのですか。
S 多くはありません。選択肢の 1 つとして提供しています。というのも、学生では NDA（秘密保持契約）をクリアするのは難しいですから、怪しいデータに触れられる機会は非常に少ないのです。そういった意味でニーズはあります。

トレーナーによる指導と法律の問題

K SecHack では 2 カ月に 1 回程度、「集合回」と呼ばれるオフラインイベントが催されています。こちらは Web サイトにレポート記事などが掲載されているので、活動内容をうかがい知ることができますが、普段のオンラインではどのような指導が行なわれているのでしょうか。
S 各コースにはトレーナーが就いています。トレーニーは日々さまざまな障壁にぶつかっています。例えば調べても分からなかったこと、調べ方が分からないこと、うまく対処したつもりでもつまずいてしまったことなどです。そういったことに対応するにはトレーナーとトレーニーが日常的に接している必要があります。普段のやりとりはオンラインチャットなどが用いられていますが、そのトラフィックは膨大な量になります。
K 伺っていると、指導する側も多大な労力がいると思うのですが、トレーナーはどのような基準で選ばれているのですか。
S 運営側から依頼しています。個人的なつながりからお願いすることが多いと思います。過去に仕事を共にして、人となりが分かっている方が、トレーニーのためにも良いのではないかと思っています。とはいえ、SecHack の今後の拡大を考慮すれば公募制なども視野に入れておいた方がよいとも思っています。
K 集合回のレポートを見ると、SecHack では開始早々の時期に情報倫理の講義をされています。セキュリティ・キャンプなども同様だと思いますが、この講義の意義について伺いたいと思います。

S 法律を含めたルールを知ることは重要です。セキュリティではルールの周縁部を扱うこともあります。例えば攻撃を研究テーマにした場合「それを本当に実行してもよいのか？」といった問題が発生することもあります。それに対して公明正大に「実行してもよいのです」と言いたいのです。そうなると、法律の専門家にきちんと相談して、ここまでなら大丈夫という範囲を設定しなくてはなりません。また、ルールを説明することは研究倫理を考えるきっかけにもなります。

K 若者が自らの判断だけで突き進んでしまうと法律の一線を踏み外してしまうことだってあります。場合によってはその後の社会生活に支障をきたしかねません。その意味からいうと、SecHackのように先達の指導を仰ぎながら学ぶのは良いことだと思います。

S 何事であっても、指導者の下で学ぶ方が圧倒的に効率がよいと思います。セキュリティに関して言えば独学で学ぶなら法律も学ばなくてはなりません。それに法律とは解釈論でもありますから、過去はこうだったけれど現在も同じだとは限りません。過去に出た判決の背後にある考え方も知っておかなくてはならないのです。

K 話はそれますが、私自身、以前「ハッカージャパン」という雑誌の編集に携わっており海外のハッカーに話を聞く機会も多くありました。そういった時、あなたにハッキングのメンター（師）はいるかと聞くのですが、多くの場合「いる」という答えが返ってきます。一方、日本では「独学で」という答えが多いのです。「師」というと大仰なイメージになってしまうのかもしれません。

セキュリティ人材育成と世代交代

K SecHackに限らず人材育成プログラムの世代交代についてお話を伺いたいと思います。

S 世代交代が進んでいるのはSECCONやCTFではないかと思っています。SECCONをはじめた頃からの意見ですが、世界のCTFで勝っているチームは、自分たちでもCTFを開催しています。これは結果を見れば明らかです。ですからやるべきだと主張してきました。そこから数年が経ち、さまざまなチームがCTFの主催をはじめました。現在では、さまざまなレベルの大会が登場しています。

K 今では猫も杓子もCTFですよね。

S セキュリティ・キャンプも協議会の佳山さんたちのご尽力のおかげで若手の登用が進んでいます※5。私自身も以前はミニキャンプ全ての回に参加していましたが、今では若手に完全に任せられるようになりました。事業ごとに見ても世代交代は進んでいるように思います。ただ、SecHackは立ち上がったばかりですから、世代交代もなにもありません（笑）。

K 最後の質問です。中期的なものでも長期的なものでも構いませんので、園田さんの今後の目標をお聞かせください。

S 業務として関わるという意味では現状で手一杯なのですがヴィジョンはあります。GAFAの人たちがすごいのはデータを握っていることだと思っています。一方でわれわれの手にデータはないのかといえば、握っているものもあるはずです。例えばCYDERでは、受講者が演習環境でどんなツールをどう使ったのかなど、操作データのすべてを記録しています。演習に参加した人が解析でどのようなことを行なったのか、また、どんなものを見たのかなどを知ることができます。これも立派なビッグデータです。NICTには観測網もありますから、こうしたデータを軸にして研究・開発人材を育てられる枠組みにしていきたいと考えています。SecHackを終えたトレーニーの次の研究ステップにも適しています。

K 興味深い取り組みですね。

S あくまでもヴィジョンであり、実現までにどれくらいの時間がかかるのか分かりませんが、この枠組みから優秀なエンジニアがたくさん出て、良いプロダクトもたくさん出てくればと願っています。

K 本日はどうもありがとうございました。

※5 **目指すは"地産地消"の人材育成！セキュリティ・キャンプの新たな挑戦（マイナビニュース）** https://news.mynavi.jp/itsearch/article/security/3528

女性による女性ための情報セキュリティ・コミュニティ

4-Girls CTF 2019 レポート

取材・文・撮影＝斉藤健一

2019 年 12 月 7 日、東京・大崎の当社（日立システムズ）にて、4-Girls CTF 2019 が開催された。主催は、情報セキュリティに興味を持つ女性を対象としたコミュニティの CTF for GIRLS。2014 年に活動を開始、運営も女性が行なっており、これまでに開催されたワークショップは 10 回以上、CTF 大会も今回で 4 回目を迎える。会場には 28 名の参加者が集まり、ネットワークやセキュリティのスキルを競い合った。

CTF for GIRLS とは

コミュニティの代表である中島明日香氏（NTT セキュアプラットフォーム研究所）に CTF for GIRLS 発足の経緯や活動内容について話を伺った。

セキュリティ業界では男性が圧倒的に多く、中島氏によれば、技術に興味を持った女性が勉強会などに参加しようとしても、好奇の視線に晒されたり、気後れしてしまったりと、何かとハードルが高いという。そこで当時の SECCON 実行委員長である竹迫良範氏に女性限定の勉強会を提案、SECCON の連携イベントとして CTF for GIRLS を立ちあげた。女性限定にすることで心理的・社会的なハードルを下げ、技術に触れる機会や交流の場を増やすことをめざしたという。当時、業界内での反応はさまざまで、女性限定のコミュニティに賛同する声もあれば、技術や CTF に男女の差はないのになぜ女性限定なのか、といった懐疑的な意見もあったそうだ。

一方で参加者からは「講師も参加者も全員女性で相談も質問もしやすかった」や「同世代の女性と情報交換ができた」といった好意的なコメントが寄せられた。

第 1 回目のワークショップの時には 7 ～ 8 名だったスタッフも参加者を運営側に勧誘することで増やし、現在では 30 名ほどになったという。最近ではワークショップの模様を動画で配信しており、地方在住の方やワーキングマザーなど、会場に来ることが難しい人たちに対してもコミュニティの扉を開いている。

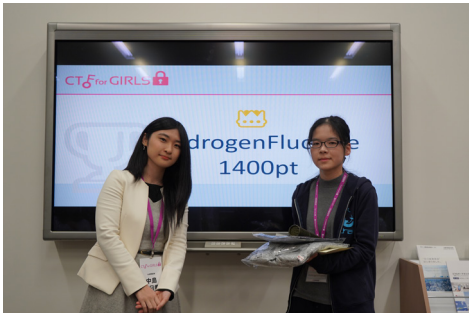
中島氏は CTF for GIRLS の目標に「持続可能な組織を作る」「コミュニティの輪を広げる」「レベルの高い人材を輩出する」の 3 つを掲げている。それぞれの達成度を尋ねたところ、先の 2 つについては「まずまず」で 50% ほどの達成度だが、最後の目標は「まだまだ」これからなのだという。究極の目標は「女性限定」という区分そのものが必要のない社会になることだというが、彼女自身もその時が来るのは何十年も先のことになると予想している。

●中島明日香（なかじま・あすか）

14 歳の時、女子高生ハッカーが活躍する小説「Project SEVEN」と出会いハッカーを志す。慶應義塾大学環境情報学部に入学 4 日目にして武田圭史教授の研究室の扉を叩く。在学中は情報セキュリティの勉強に明け暮れる。大学卒業後、NTT セキュアプラットフォーム研究所に入社。2014 年に CTF for Girls を立ちあげる。2019 年「サイバーセキュリティに関する総務大臣奨励賞」を受賞。

競技会場の様子

競技終了直前のスコアボード



今大会で優勝したHydrogen fluorideさん(右)。ハンドル名はフッ化水素の意味。大学のサークルではCTFの他にもゲームの制作や競技プログラミングなどを行なっているという

水面下で繰り広げられた熱い戦い

4-Girls CTF 2019は4回目のCTF大会となる。アニメ作品「攻殻機動隊」とのコラボ企画であった過去3大会と比較すると参加応募者は多かったという。

大会は個人戦で、バイナリ・フォレンジック・ネットワーク・暗号・Webの5ジャンルから、それぞれ初級・中級・上級の計15問が出題される。競技時間は11時30分から16時30分までの5時間。参加者は各自で休憩を挟みながら問題に取り組む。

個人戦ということもあり競技会場内は至って静かだったが、ノートPCのディスプレイを見つめる参加者の眼差しは真剣そのものだ。競技中にはタイムアタックという特定の時間帯だけ表示・解答できる問題もあり、参加者の集中力もより一層に高まる。

5時間にわたる競技の結果、優勝を飾ったのは1400ポイントを獲得したHydrogen fluorideさんだった。東京工業大学の2年生でコンピューター系のサークルに所属。SECCON BeginersやSECCON CTFの予選にも参加した経験があるそうだ。

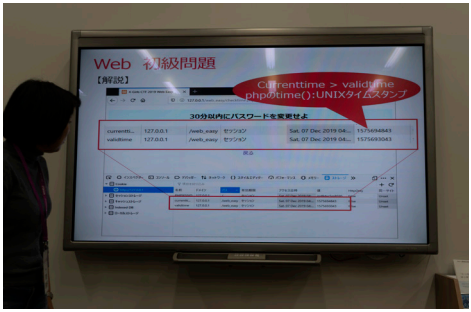
また、3位に入賞したyukiさんの活躍も印象に残った。過去の大会でも上位入賞の実績を持つという彼女だが、今大会は体調不良により途中からの参加となった。その状況でも、わずか2時間で1000ポイントを獲得したというのは見事というほかない。

競技後には参加者同士の交流も

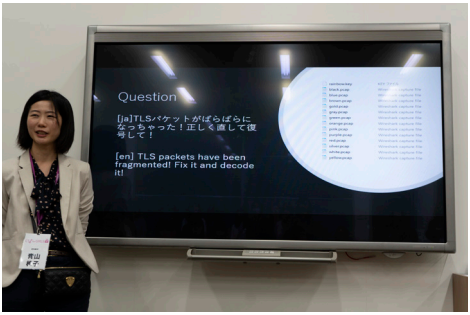
競技終了後は運営側による問題の答え合わせが行なわれたので、ここでいくつか紹介しよう。Web初級の問題は「30分以内にパスワードを変更せよ」というものだった。通信内容を見るとCookieに現在の時刻（currenttime）と有効時間（validtime）がUNIXTIMEを用いてセットされていることが分かる。問題では現在時刻の値の方が有効時間の値よりも大きくなっている（時間として進んでいる）ので、この値を編集・送信することによってフラグを得ることができる。

またネットワーク上級は「TLSパケットがばらばらになった！正しく直して復号して！」という問題で、複数のpcapファイルとTLSを復号するための鍵ファイルが用意されている。解法としてはTCPパケットのシーケンス番号に着目してつなぎ合わせることができれば復号できるという。ちなみにこの問題を解答できたのは1名だけだったそうだ。

この答え合わせの時間は参加者同士の交流会も



競技会場の様子



競技会場の様子

台湾から参加した yuyu さん（左）と Lee さん（右）。yuyu さんは台湾の女性限定コミュニティである HITCON Girls のメンバーでもある

兼ねており、会場にはスイーツも用意され、くつろいだ雰囲気となった。ここで運営側より台湾から参加した yuyu さんと Lee さんが紹介された。共に台湾政府が主導する AIS3（Advanced Information Security Summer School）の受講者で今回の大会に参加することを楽しみにしていたそうだ。その後、希望者による懇親会も予定されていたが、筆者の取材はここまでとなった。

最後に余談だが、今大会を取材した筆者の感想を述べる。女性の中にポツンといる状況は、ある種の居心地の悪さを感じざるを得ない。しかし、これは男性社会の中にいる女性が常に感じていることなのかもしれない。中島氏が言うように女性限定という区分が必要なくなるには多くの時間が必要だが、その実現のためには男性側の意識が変わることも重要だろう。今回の取材はこのことが感じられるよい経験となった。

学術界と産業界、研究者と実務者を結ぶ交流の場

コンピュータセキュリティシンポジウム（CSS）2019 レポート

文 = 関谷信吾

CSS とは

2019 年 10 月 21 日～ 10 月 24 日にコンピュータセキュリティシンポジウム 2019(以下 CSS2019) が開催されました。

- 名称：コンピュータセキュリティシンポジウム
- 主催：情報処理学会コンピュータセキュリティ研究会
- 開催地：長崎県 ハウステンボス
- Web サイト：https://www.iwsec.org/css/2019/
- 併設ワークショップ：
  マルウェア対策研究人材育成ワークショップ
  プライバシーワークショップ
  ユーザブルセキュリティワークショップ
  OSS セキュリティ技術ワークショップ

CSS はコンピュータセキュリティに関連する研究成果を発表する場です。併設されているワークショップからも分かるとおり、マルウェアからプライバシーまでセキュリティに関連した幅広いテーマで論文が投稿されています。

今年はハウステンボス内の会議室 (図 1) で開催されました。シンポジウムが終わるころにはイルミネーションが点灯されていて、とても綺麗でした。

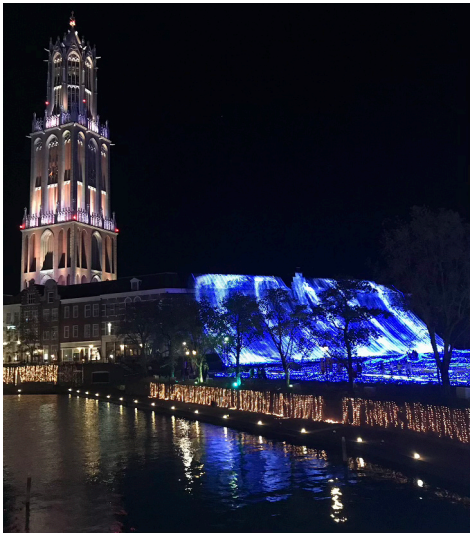


図 1 ドムトールン（高い塔）の会議室で開催

イベント紹介

CSS では論文のプレゼンテーション以外にも競技会や基調講演などが開催されています。

• 競技会

CSS で開催される競技会には、マルウェア解析技術を競う MWS Cup と、匿名加工したデータの安全性と有用性を競う PWS Cup の 2 つがあります。当社は複数大学の学生とチームを組み MWS Cup に参加しました。

MWS Cup 当日は動的・静的解析、DFIR の技術を問う問題が約 20 問出題され、午前 10 時から 13 時までの 3 時間の中で解析を行ないます。全 15 チームが黙々と与えられた課題に取り組んでいたのが印象的でした (図 2)。

上記の当日課題のみならず、事前課題として出題された「マルウェア解析に資するツールなどの作成」も評価の対象になります。

弊社が MWS Cup へ参加する目的の 1 つに学生の技術力向上があります。事前準備として、勉強会を開催して技術力向上を図りました。当日は声を掛け合い、チーム一丸となって取り組みました。学生と社会人、お互いの技術力を飛躍させる良い機会になりました。

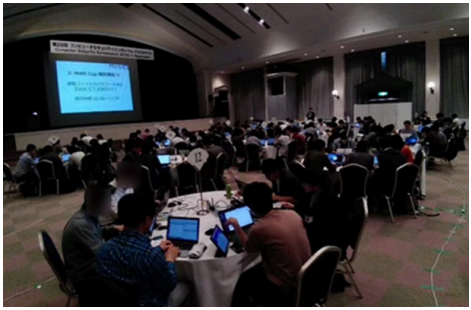


図 2 競技会の様子

図 3 懇親会の様子

• 基調講演

基調講演では、原田泳幸様から「デジタルマーケティングが創造するビジネスモデル」の講演がありました。会社を経営する立場から最新の革新的なサービスを紹介し、サービスにはセキュリティ対策が必須であることを説明されていました。

村山優子先生から「情報科学におけるトラストの研究課題」の講演がありました。安心とセキュア、トラストの考え方の違いを紹介し、リスクがある環境ではトラストが必要であると説明されていました。

両講演とも貴重なお話を伺うことができ、講演後には活発に質疑がなされました。

• 論文紹介

ここからは評価が高かった論文および個人的に注目した論文を紹介していきます。

① CSS2019 最優秀論文賞
「広域スキャンで収集した応答を用いた全ポート待受型 Web ハニーポット」
加藤誠也他 (横浜国立大学)

この論文ではハニーポットの観測能力の向上を目的として、アクセスへの応答を模倣する手法を提案していました。提案手法と既存手法を比較した結果、提案手法では HTTP リクエストが約 2 万 8000 件増加し、検体は約 7 倍に当たる 228 件の検体を取得できていました。

特定の応答のみ模倣することで、特定の業種に関連する検体のみ収集できないかと期待しています。

② CSS2019 学生論文賞
「クラウドサービス悪用攻撃の大規模実態調査」
福士直翼他 (早稲田大学)

この論文ではクラウドサービスを悪用したサイバー攻撃の実態を調査するため、クラウドサービスに割り当てられる IP アドレスのブラックリストを調査していました。クラウドサービスはサイバー攻撃に悪用される場合があり、悪用された IP アドレスが正規サービスに再割り当てされることが懸念されています。

調査の結果、1 日あたり、約 1 万件のクラウド事業者の IP アドレスがブラックリストに掲載されていると分かったとのことです。

③個人的に興味を持った論文
「SNS データを用いたセキュリティインシデント早期検知に関する実現可能性検証」
榊剛史他 (東京大学)

この論文では SNS 上のデータからセキュリティインシデントを早期検知するために、ユーザーをクラスタ化して反応を可視化する手法を提案していました。

paypay、7pay の不正アクセス事件で検証したところ、特定のクラスタのみが強い反応を示し、電子決済の不正利用に興味を持つユーザー群がいると推測していました。このようなユーザー群を監視することで、インシデントを早期検知できる可能性があるとのことです。

最後に

CSS はコンピュータセキュリティに関する最先端の研究と、学生によるフレッシュな発想に触れられるシンポジウムとなっています。懇親会 (図 3) では社会人、学生を問わず、さまざまな参加者と意見交換することができます。セキュリティに興味のある方は参加を検討されてはいかがでしょうか。弊社は来年も参加を予定していますので、会場でお会いしましょう。

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.36

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