HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.27

株式会社 日立システムズ

Human * IT

Hitachi Systems security Jounral VOL.27

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

KOSEN セキュリティ・コンテスト 2017 レポート

取材・文・撮影＝斉藤健一

高専生が競う CTF 大会

2017 年 10 月 20 日（金）～ 22 日（日）に木更津高専において、KOSEN セキュリティ・コンテスト 2017 が開催された。2016 年 11 月に高知高専で行なわれた初回に続く第 2 回目であり、今回はジェパディ（クイズ）形式の競技となった。初日に参加者交流会が開かれ、2 日目から競技が行なわれるスケジュールとなっている。会場に集まった 10 チームに加えオンラインからも 25 チームが参加した。　優勝チームには SECCON 2017 国内決勝大会への出場権が与えられる。大会期間中、関東地方には台風 21 号が接近・上陸し、荒れ模様の天候となったが、サイバー空間でも高専生による熱く激しい戦いが繰り広げられた。

競技開始前には講演も

開会の挨拶に立った木更津高専校長の前野一夫氏は、IT・IoT は今後の社会において欠くことができない技術であり、参加者がそれぞれの分野で活躍できるエンジニアになれるよう、こうしたコンテストを通じて研鑽に励んでほしいとエールを贈った。

開会式の後には 2 つの講演が行なわれた。1 つは高知高専客員准教授の竹迫良範氏による「情報セキュリティと倫理について」。竹迫氏は講演冒頭、CTF とは IT 技術の総合格闘技であり、あらゆる分野の知識・スキルが要求されると説明。さらに、エンジニアの能力を客観的に評価できる CTF の意義や、高専での人財育成の取り組み・教材などが紹介された。また終盤では、ハッカーになるための心構えや技術を悪用しない倫理観なども説かれた。

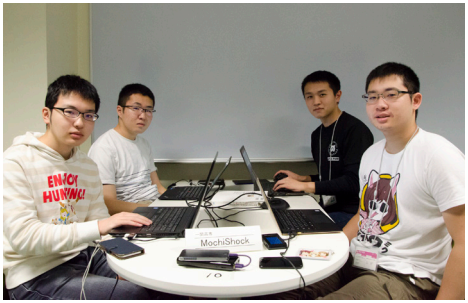
木更津高専校長の前野一夫氏

高知高専客員准教授の竹迫良範氏

そしてもう 1 つは PwC サイバーサービスの村上純一氏による「高専 OB としてのセキュリティ人財キャリア」だ。村上氏は木更津高専の出身であり、自らの経験を通じて高専生にキャリアを考えるためのアドバイスを授ける。村上氏は卒業後にラックへ就職、その後スタートアップの FFRI を経て、コンサルティング企業の現職へと転身したが、キャリアについては安定志向ではなく、常にチャレンジできる環境に身を置くようにしてきたという。


PwC サイバーサービスの村上純一氏


会場の様子。参加者は壁際のテーブルに着席している



MochiShock（一関高専）

M0x1（秋田高専）

講演後には登壇者 2 人のトークセッションが行なわれ、会場からは「高専生の強みとは何か ?」といった具体的な質問も寄せられた。竹迫氏は、高専生は年齢が若い時から進路を意識することになるが、これは大学生などと比べて大きな時間的アドバンテージだと述べた。一方、村上氏は、高専出身者を「左利き」に例え、世間がいかに「右利き」（学士・修士などの多数派）のためにできているかを知ることができ、その人たちとは違った視点で社会や物事を捉えられるようになると、高専 OB ならではの意見を述べた。

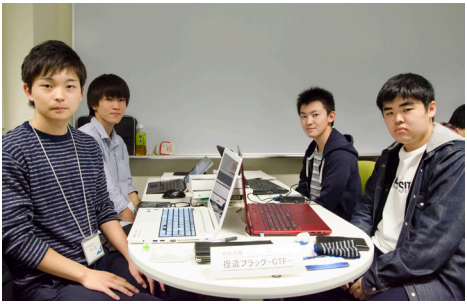
白熱の前半戦

2 日目午後、いよいよ CTF 競技が開始された。参加者を待ち受けるのは、Web・ネットワーク・バイナリ・暗号・その他のジャンルから出題される 21 問のクイズだ。すべての問題は隠されたフラグ（文字列）を見つけるものとなっている。例えば暗号の問題であれば復号した平文がフラグとなっていたり、ネットワークの問題では pcap(キャプチャー) ファイルの中にフラグが入っていたりする。各チームはこれらの問題を解き、得られたフラグをスコアサーバーに登録することで、問題の難易度に応じたポイントを得る。

さらに KoH（King of Hill）と呼ばれる形式の問題も 2 つ用意された。キング・オブ・ヒルとは文字どおり「お山の大将」のことだが、これはサーバーの制圧を意味している。具体的には主催者が用意したサーバーに自チームの ID を書き込むなど、特定の条件を満たした状態を維持できれば、その間は定期的にポイントが得られる。一方、他チームは ID の上書きなどを試みてサーバーの新たな制圧を狙うというものだ。

競技時間は 2 日目の 13 時から 18 時、3 日目の 9 時から 12 時をあわせた 8 時間となる。問題には競技用ネットワークに接続していないと解けないものもあるが、中には会場から持ち帰り、宿舎で引き続きチャレンジできるものも含まれている。

多くの CTF 大会では会場内で大音量の音楽を流したり、パトランプを点灯させてポイント獲得を告げたりすることも多い。しかし、今回のコンテストではオンライン参加のチームも多く、会場の様子をネットで配信することもあり、前述のよう


捏造フラッグ -CTF-（福島高専）


DICE（豊田高専）

21 日のポイント獲得グラフと順位

最終的な順位と解答した問題

な派手な演出は行なわれなかった。時折、運営スタッフのコメントが入るものの、競技は終始落ち着いた雰囲気の中で進んでいった。

競技開始から 1 時間ほど経過した 14 時ごろには、insecure（奈良）、BiPhone（明石）、SandBox（金沢）、PwnPwnPain（都立）といったオンライン参加のチームが牽引する形で得点上位集団が形成される。さらに 1 時間が経過した 15 時ごろには BiPhone が連続で得点を重ね、集団から一歩抜け出すことに成功し、insecure がそれを追いかける。

しかし、17 時すぎに insecure が KoH の 1 つを攻略し、展開が大きく変化した。KoH 攻略によって得られるのは 10 分間ごとに 30 点。これにより insecure は BiPhone を徐々に引き離し、さらに 18 時近くにクイズを解いたポイントも加え 400 点近い差をつけてこの日の競技を終えた。

嵐を呼ぶ後半戦

大会 3 日目の 10 月 22 日は第 48 回衆議院選挙の投票日でもあったが、関東地方には台風 21 号が直撃し天候は朝から大荒れの様相だ。競技の方も開始直後の得点ラッシュで波乱が起こる。前日 2 位だった BiPhone が持ち帰った問題を攻略して得点を重ね首位に返り咲いたのだ。BiPhone としてはさらに得点を重ねたいところだが、残っているのは 1 問のクイズと 2 問の KoH という状況。一方、KoH の 1 つを攻略している insecure には時間ごとに一定のポイントが入るためジリジリとその差を詰め、さらにクイズ問題でも 1 問の正解を加えて、再びトップに立ち、そのままフィニッシュを迎えた。

なお、SandBox も得点し BiPhone と同点となったが、解答時刻が早かった BiPhone が 2 位となった。

話題はそれるが、今回の大会で筆者が興味深いと思ったのは上位チーム以外の得点状況だ。競技後半になると下位チームの得点に動きがなくなってしまう大会は多い。メンバーに初心者が多いとお手上げ状態になってしまうのだ。

ところが、今回の大会では時間が経過しても下位チームが着実にポイントを獲得していた。運営スタッフに聞くと、問題のレビューを徹底し CTF 初心者でも 1000 点程度は獲得できるよう難易度を調整したとのことで、見事に功を奏していた。


チャーハン定食背脂多め（石川高専）

HDD 破壊部隊（有明高専）

KEMG（木更津高専）

raspberry（高知高専）

問題の解説

競技終了後にはいくつかの問題に対して解説が行なわれた。参加者が苦戦したのが暗号問題の 1 つと 2 問の KoH だ。暗号問題は「Homomorphic Encryption」。準同型暗号とも呼ばれ、暗号文のままでも計算できるという特長を持っている。問題作成者によれば、暗号の開発に日本人が関与している※ 1、日本語の文献がない、暗号方式を実装したプログラムが公開されていない、といった基準でこの方式を選んだという。英語の論文を読み、暗号方式を実装したプログラムが書ければ、この問題は攻略できたのだそうだ。

次に、insecure だけが攻略できた KoH だが、こちらはポートノッキングのスキルを問うもので、pcap ファイルに残された記録を理解し再現することでサーバーへ接続できるのだそうだ。さらに稼働しているプログラムを入手して解析すれば、外部からのコマンド実行も可能だったという。

また、KoH の残る 1 つはどのチームも解くことができなかったため、他の CTF 大会に流用することも考慮し、解説は省略された。

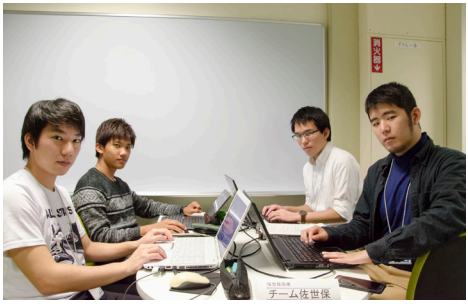
なお、他の問題については、参加者による解答例（Write Up）がブログなどで公開されている。詳細を知りたい方はそちらをご覧いただきたい※ 2 ※ 3。

おしまいに

現在、高専では 5 校の拠点校を中心に情報セキュリティ人財育成事業を行なっている※ 4。

木更津高専も拠点校の 1 つとなっており、2017 年 5 月に開かれた「第 21 回サイバー犯罪に関する白浜シンポジウム」の「情報危機管理コンテス

※ 1 **Okamoto-Uchiyama homomorphic encryption algorithm implementation in e-voting system**
http://ieeexplore.ieee.org/document/7905739/
※ 2 **KOSEN セキュリティコンテスト 2017 Write-Up - プロになりたい** http://jaganikuman.hatenablog.com/entry/2017/10/22/222230
※ 3 **KOSEN セキュリティコンテスト 2017 Write-Up - 絵のない技術書** http://tokunn.hateblo.jp/entry/2017/10/23/134637
※ 4 **（独）国立高等専門学校機構 情報セキュリティ人財育成事業**
https://www.nisc.go.jp/conference/cs/jinzai/wg2/dai03/pdf/03shiryou06.pdf



チーム佐世保（佐世保高専）

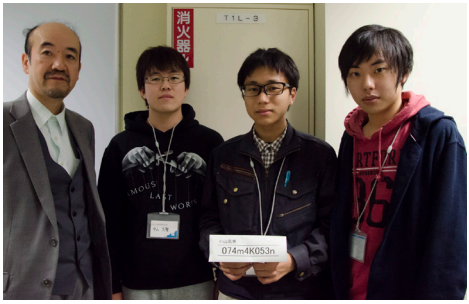

木更津高専・情報工学科・准教授の米村恵一氏

ト」決勝で同校のチームが優勝したことは記憶に新しい。このあたりについて情報工学科・准教授の米村恵一氏に話を伺った。

拠点校になったことによる変化でいちばん大きなものは米村氏自身の意識だったという。特別授業などで多くの人たちと接することで、生徒と共に自分自身もセキュリティを学びたいと決意したという。そして、こうした思いが生徒にも伝わり相乗効果となって情報危機管理コンテストの結果につながったのではないかと述べた。

大会のトークセッションで竹迫氏も語っているように、高専生のメリットは年齢の若い時点でエンジニアとしてのキャリアを意識できるところにある。セキュリティ人財の不足が叫ばれる中、高専の人財育成の取り組みも少しずつ成果が出ているように思われる。

SECCON 2017 国内決勝大会へ出場する insecure チームの健闘を祈るとともに、高専の人財育成事業のさらなる発展に期待したい。



074m4K053n（小山高専）
会場参加の中で最上位のチーム。左から引率の石原学教諭・中山太智さん・鈴木雅人さん・林知秀さん。今回の大会にあわせて電気電子創造工学科の生徒で結成された。元々 4 人のチームだったそうだが、1 名が学校の都合で不参加。CTF 初参加のメンバーがいたり、宿舎に持ち帰った問題を解くのに朝 4 時まで起きていたりといった苦労話を聞かせくれた。

CYBER SEA Game 2017 レポート

文＋写真 =tessy（寺島崇幸：SECCON 実行委員会）

ASEAN10 カ国の代表が集う CTF 大会

2017 年 11 月、タイ・バンコクにて「Cyber SEA Game 2017」という CTF 大会が開催されました。Cyber SEA Game とは Cyber South East Asian Game の略で、ASEAN 地域におけるサイバーセキュリティ業務に携わる若者の育成と人的ネットワークの強化を目的としています。2015 年に第 1 回目が開催されましたが、このときはインドネシアの CSIRT である Id-SIRTII/CC※1 が主催し、日本政府が支援を行ないました。その後、この取り組みは、日 ASEAN 統合基金 2.0(JAIF) によるプロジェクト「日 ASEAN サイバーセキュリティ協力ハブ」の構成の 1 つとして位置付けられ※2、2017 年に第 2 回目が開催される運びとなりました。

筆者は SECCON 実行委員会有志の一員として、第 1 回目に続き今大会でも運営に携わる機会をいただきました。そこで、前回との違いなども交えながら、競技の模様を紹介したいと思います。

Cyber SEA Game を有り体に言えば、ASEAN 10 カ国の代表が一堂に会して競う統一戦です。ただ、第 1 回目が開催された 2015 年の時点では、CTF の経験がない、もしくは認知度が低いといった理由から、代表チームを決める国内予選の開催もままならない国がありました。そこで、私たち JNSA/SECCON 実行委員会有志は、ASEAN4 カ国（タイ・ミャンマー・ラオス・カンボジア）で、CTF 予選大会の現地運営支援を行ないました。

タイでは予選大会直前に政府系サイトがサイバー攻撃を受けたり、ミャンマーでは競技中に停電が起こったりするなどのハプニングもありましたが、最終的にインドネシア・ジャカルタにて 9 カ国 14 チームが参加した決勝大会が行なわれました（諸事情によりシンガポールが欠場、各国 2 チームまでの出場枠があった）。熱戦を制したのはベトナムチームで、彼らは日本で開催される SECCON CTF 決勝大会への切符を手に入れました。なお、この大会の模様は 2016 年 1 月公開の本誌 VOL.17 に掲載されています※3。

Cyber SEA Game 2017 は タイ・バンコクで開催

今回の主催はタイの CSIRT である ETDA※4 が行ない、日本からは NEC のスタッフと SECCON 実行委員有志が問題作成や現地での決勝戦開催支援を行ないました。事前の準備では、タイ側とメールやテレカンファレンスの他、LINE（タイでは生活インフラを担いつつある）なども活用してコミュニケーションをはかりました。

決勝戦開催直前の 10 月は、自国のオンライン予選開催やプミポン国王の火葬の儀などが重なり、タイ側のスタッフにとってはハードなスケジュールだったと思いますが、前回と比較して開催までの準備はスムーズにできたと感じています。

決勝戦は 11 月 22 日、バンコクのスイスホテル（Swissôtel）にて開催されました。ASEAN10 カ国の代表チームが参加、全 10 チームで勝敗が争わ

※1 **Id-SIRTII/CC** https://www.idsirtii.or.id/
※2 **総務省｜ ASEAN 向けサイバーセキュリティ演習の実施**
http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000132.html
※3 **Hitachi Systems Security Journal Vol.17** https://www.hitachi-systems.com/report/specialist/hj/
※4 **ThaiCERT（ETDA）** https://www.thaicert.or.th/en/homepage/

ASEAN10 カ国の代表チームが競う CYBER SEA Game 2017

会場の様子

れます。参加者の中には前回も出場していた見覚えのある顔ぶれも多かったと思います。

競技は、ジェパディ（Jeopardy）形式で行なわれます。問題は、Web、フォレンジック、リバースエンジニアリング、ネットワーク、暗号、攻撃コード（Pwnable）、その他といった 7 つのカテゴリから 31 問が出題されます。競技時間は午前・午後をあわせた 6 時間。第 1 回目の経験から国ごとの実力差が大きいことが分かっていたので、難易度が低い問題を多めに用意することとしました。

勝敗の行方は？

競技が開始されると、今回が初出場となるシンガポールが得点を獲得して先頭に立ち、タイ、ベトナム、インドネシアが続きました。午前中は主にタイ ETDA 側で作成したものが出題されていましたが、正答するチームも少なく、競技が停滞する時間も続きました。実は問題レビュー時点で、内容や意図が分かりにくいという懸念を伝えていたのですが、開催直前ということもあり、簡単な対処しかできなかったことが悔やまれます。

午後には日本側が作成した問題も出題され、なおかつ簡単な問題も多くあったことから、得点が大きく動く展開となりました。

午前中はタイがリードする状況でしたが、午後に入るとベトナムが首位に立ち、しばらくその状態をキープします。聞くところによると、タイチームは、決勝戦前日にマレーシアで開催されたコンテストに参加しており、当日早朝のフライトで帰国・会場入りするという強行軍だったそうです。

競技が残り 1 時間となったところでスコアボードが隠され、参加者も私たちも得点の推移が分からない状況となりました。最終結果は、優勝がインドネシア、2 位シンガポール、3 位ベトナムとなりました。前回の優勝国で前評判の高かったベトナムチームは終盤にスコアが伸び悩み他チームの追い上げを許してしまいました。さらに、終了 5 秒前にインドネシアが得点し、シンガポールを逆転するという劇的な展開もありました。最終的にはボーナスポイントの 20 点が勝敗を分けたのだそうです。

優勝したインドネシアチームは本年 2 月に開催される SECCON 2017 国際決勝大会への招待参加が決まっています。彼らの顔を見かけたら是非声をかけてみてください。

大会を終えて

今回の私たちの役割は決勝大会の運営を支援するというものでしたが、大会全体の運営という視点から見ると、参加者同士の交流の場が少なかったように思います。もちろん、参加者同士が語らう場面もありましたが、さまざまな国から多くの人たちが集っているわけですから、競技終了後に交流できる時間があれば、さらに良かったのではないかと思います。

競技終了後に各チームの解答状況や参加者アンケートなどのフィードバックを見せてもらいましたが、おおむね好意的なコメントが多く安心しました。これらの情報から見えてくる参加者の傾向は、リバースエンジニアリングや攻撃コード（Pwnable）は苦手だけれども、Web や暗号のカテゴリに興味を持つ人が多く、実際にそれらの問

上位 3 チーム（左からインドネシア、シンガポール、ベトナム）

ASEAN10 カ国から集まった参加者たち

題は多く解かれていたというものになります。ちなみに、暗号問題が人気というのは日本とは異なる傾向です。もしかすると、参加者には情報系の学科を専攻する学生が多く、暗号に馴染みがあったのかもしれません。

また、問題作成にあたっては、前述のとおり国ごとの実力差を考慮したつもりでしたが、結果を見ると大きな得点差があり、いまだギャップは埋められていないと感じています。Cyber SEA Game の目的の 1 つに、ASEAN 内で自主的かつ継続的に運営できる能力を身につけるというものがあります。競技開催も 10 カ国の持ち回りでできれば良いのですが、現状では国ごとのバラツキもあり、今後の継続的な取り組みの中で対応していきたいと考えています。

取り組みはまだ始まったばかりですが、ミャンマーなどでは自主的に国内の CTF 大会を始めるようになったそうです。2 年前の大会がきっかけとなり、新しい取り組みへとつながったことは非常にうれしく思います。

前回のレポートでも書いたように、是非ともこの取り組みは継続をしていただいて ASEAN だけでなく、日本との関係をも深めていければと願っています。

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.27

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