HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.47

株式会社 日立システムズ

Human * IT

Hitachi Systems security Journal VOL.47

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

アジアのメンバーと共にチームを組み 国際 CTF 大会の舞台へ

ICC 2022
International Cybersecurity Challenge
参加者インタビュー

取材・文＝斉藤健一

EU が主催する国際 CTF 大会で アジアチームが準優勝

2022 年 6 月 14 日から 17 日までの 4 日間、ギリシャ・アテネにて ICC（International Cybersecurity Challenge）が開催された。発起人は欧州ネットワーク・情報セキュリティ機関である ENISA（European Network and Information Security Agency）。ENISA では、これまでも欧州内のサイバーセキュリティ演習の支援などを行なってきた。ICC は欧州の枠を超えたグローバルな CTF 大会であり、初の試みになるという。世界各地の参加加盟国で構成された実行委員会によって企画・運営が行なわれる。

ICC の目的は、若い才能（18 歳〜 26 歳）を惹きつけ、サイバーセキュリティの分野で必要とされる教育やスキルについて、世界中のコミュニティの認識を高めることだという。

競技の予選は各国や地域ごとに行なわれ、64 を超える国と地域から総勢 4000 名もの若者が参加。予選を勝ち抜いたプレイヤーは、アジア・アフリカ・カナダ・ヨーロッパ・ラテンアメリカ・オセアニア・米国の 7 チームで競技に取り組む。各チームのメンバーは最大で 15 名だ。

競技は 6 月 15 日と 16 日の 2 日間で行なわれた。1 日目は Jeopardy（ジョパディもしくはジェパディ）と呼ばれるクイズ形式、2 日目は Attack & Defense（攻防戦）形式で行なわれた。日本人 3 名を含むアジアチームは、ヨーロッパチームに次ぐ総合第 2 位という好成績を収めた。

本稿では、運営でアジアの窓口となった篠田佳奈氏へのインタビューや、アジア代表メンバーとして参加した日本人プレイヤー 3 名へのグループインタビューなどを交えながら ICC をご紹介したい。

ICC 開催までの道のり

まずは、ICC 開催までの経緯について、セキュリティ・キャンプ協議会の篠田佳奈氏に話を伺った。篠田氏は ICC の構想段階からアジア地域の窓口として深く関わっている。

篠田氏の元に ICC への協力要請の打診が来たのは 2019 年 10 月、日本のセキュリティ企業に在籍する外国のエンジニアを通じたものだった。ICC 立ち上げでアジア代表チームを組織できる人物を探しているとのこと。その後 ENISA 担当者と打ち合わせを行ない、2020 年に ENISA 内で ICC の企画が採択された時点で、EU から日本政府への正式ルートで協力要請を受け、セキュリティ・キャンプ協議会が窓口となり活動を開始。篠田氏は ICC ステアリング・コミッティのメンバーとして議論の輪に加わることとなった。

並行してアジア地域の代表を選考する ACSC（Asian Cyber Security Challenge）の開催準備に取りかかる。日本の CTF チームである binja と TokyoWesterns に、韓国・台湾のメンバーを加えた国際チームを編制して運営に当たったという。

ACSC は 2021 年 9 月に個人戦のオンライン CTF として開催され、約 1000 名が参加。成績上位のプレイヤーの中から国籍・ジェンダーといった多様性も考慮し、15 名の代表が決定した。メンバーは、インド 2 名・日本 3 名・マレーシア 1 名・シンガポール 2 名・韓国 2 名・台湾 1 名・タイ 1 名・ベトナム 3 名という構成になった。

篠田氏に運営で苦労した点について伺ったとこ

ろ、大きく 2 点を挙げた。1 つは、代表メンバーを決める選考ポリシーに関わるもので、議論に議論を重ねたそうだ。参加各国から少なくとも 1 名を代表入りさせること、各国の最大参加人数を 3 名とすること、男性以外のジェンダー（自身の性自認に基づく申告を含む）も代表に含めることなどを決定した。前述のチーム構成はこうした苦労の産物だったと篠田氏は語る。

もう 1 つは、新型コロナウイルスのパンデミックにより、国際的な人の往来が可能か否か見通せなくなったことだという。当初は、2021 年 12 月から 2022 年 1 月に開催を予定していたが延期を余儀なくされ、最終的に 2022 年 6 月まで開催がずれ込んだのだという。

一方、運営に携わる中で興味深かった点として、プレイヤーの心境の変化を挙げている。ICC では母国語も文化も違う人たちとチームを組み、問題を解くために英語でコミュニケーションをとって、協力・団結しなくてはならない。この環境によってプレイヤー同士にどのような化学反応が起きるのか、注視してきたとも語っている。

ICC に参加した日本人プレイヤーにインタビュー

引き続き、ICC に参加した日本人プレイヤー 3 名に話を伺った。各人のプロフィールは以下のとおり。なお、インタビューは 2022 年 7 月に行なっており、年齢・CTF 歴・所属組織などはその当時のものとなっている。

• st98（エスティー 98）さん

CTF 歴 8 年、2014 年から活動を開始。CTF に興味を持つきっかけは Web の開発から。セキュリティ・キャンプ参加者の記事を読み、その中にあった CTF に関する記述から興味を持つことに。大学では情報学を専攻し、情報セキュリティ関連の研究室に在籍。研究のテーマは Web セキュリティ。CTF の得意分野ももちろん Web セキュリティ。現在はセキュリティ企業に在籍。zer0pts という CTF チームに所属している。

• Dronex（ドローネックス）さん

CTF 歴 3 年、2019 年から活動を開始。大学生。CTF を始めるきっかけは高校時代の友人からの誘いでチームを組んだこと。現在は ./Vespiary というチームに所属している。得意分野は Pwn だが、チーム内に低レイヤーを担当する人間がいないということもあり、リバーシングなどにも手を出している。暗号にも取り組んだ時期もあるが現在は休止中。インタビュー当時は 25 歳で、ICC2023 にも挑戦する予定とのこと。

• れっくすさん

CTF 歴はまもなく 10 年を迎える。2012 年、高校 2 年生のときにセキュリティ・キャンプに参加。当時、CTF はマイナーな存在で日本国内で開催される大会もわずかだったそう。2014 年に大学に入学、そこから本格的に活動を開始。所属チームは dodododo だが、大会規模に応じて他チームに合流することも。暗号を好む。セキュリティ企業に在籍する一方で、2020 年から SECCON メンバーとしても活動しており、2022 年は CTF のリーダーも務める。

st98 さん、れっくすさんはそれぞれ所属企業のブログにて、ICC に参戦したレポート記事を書かれている（記事の最後に参考資料として URL を掲載）。問題の解法など技術的な情報はそちらをご覧いただくとして、本稿では、Jeopardy 形式の難易度、作問者の国籍による傾向、ICC に参加した感想などを中心に話を伺った。

斉藤（以下 K）：ICC 初日の Jeopardy について、皆さんが担当した問題のジャンルやその難易度について教えて下さい。

Dronex（以下 D）：Pwn を中心に見ていました。すべての問題を詳細に見たわけではありませんが、それほど難しいという印象は持ちませんでした。ですが、競技時間が午前 9 時から午後 5 時までと短かったことを考慮すると適切な分量だったと思います。

れっくす（以下 R）：主に暗号を見ていました。出題が 6 問あり、そのうち 2 問は解けたのですが、残り 4 問は超難問でした。8 時間という競技

時間では歯が立ちませんでした。仮に、世界トップレベルのCTF大会で出題されたとしても、解答できるチームはわずかだったと思います。

st98（以下 S）：Webを主に見ていました。簡単な問題と難問が混在しており、難易度にバラツキがありました。

K チームの各メンバーはどのようにして解く問題を分担していたのですか。

S ICCでは競技開始の時点ですべての問題文が見られる状態になっていました。まずはすべての問題をざっと見て、解きやすそうな問題から手を付けることにしました。チーム内のWeb担当メンバーで手分けをして、Discordで情報共有しながら解くことにしました。

R 暗号では、まずすべての問題を開いて、どのような問題なのかをDiscordで共有するようにしました。例えば、この問題はRSA暗号が使われているとか、楕円曲線暗号が使われているといったコア技術に関するコメントをつけるところから始めました。暗号を担当するメンバーは総勢5名と多かったのです。ベトナムから3名の方が参加していましたが、3人とも暗号を担当していました。さらにこの方々は本当に優秀で、いろいろと助けられました。

K ベトナムのメンバーがみな暗号を担当したという話を伺い、新たな疑問が出てきました。国によってプレイヤーが好きなジャンルや問題などは存在するのでしょうか。

D 話の方向性は少し異なりますが、国によって作問に傾向があると、プレイヤー同士で話題になることはあります。確固としたエビデンスがあるわけではなく、あくまでイメージの話です。例えば日本人による作問はパズル的な要素があるものが多いと、海外のプレイヤーから言われます。逆に日本人から見ると、海外の問題は、Pwnの問題なのにリバーシングが必要だったり、解答するプレイヤーが推測しなくてはならない要素を入れ込んだりするなど、手間をかけさせる傾向があると思います。

見事に準優勝を果たしたアジア代表チームのメンバー（写真提供：セキュリティ・キャンプ協議会）

S Dronexさんに同意します。国ごとに問題を作る特徴があります。

K 今回の記事の取材でセキュリティ・キャンプ協議会の篠田佳奈さんに話を伺う機会があり、そのときも話題になったのですが、例えばアジアで開催されたCTF大会ではアジアのチームが強いとか、北米の大会だと北米のチームが強いという話になりました。自国や自地域の開催であれば、時差ボケに悩まされることはありません。しかし、他にも要因があるのではないかと考えていたのですが、今回ったように、作問者と解答者の思考が近く、文化的な背景も共有しているからということも考えられると思うのですが、いかがでしょう。

D 確かに。日本のCTF大会だと問題を解いていて楽しいですし、面白いと感じることも多いです。

R 文化的な背景の共有というのもあるかもしれません。他にもCTFの作問ではその地域で流行している攻撃手法が取り入れられることも多いので、そういった状況も背景にあると思います。

K プレイヤーの方の率直な感想をいただくことができました。次に話題を変えてICCに参加した感想などをいただきたいと思います。

D 海外のメンバーとチームを組みプレイするということは、問題を解くために英語でコミュニケーションを取らざるを得ない状況に自分を追い込むということです。そこがとても面白いと感じまし

た。話すためには自分の中にある英語が苦手だというためらいを吹っ飛ばす必要がありましたが、今回の ICC でそれができたことがとても良かったと思っています。

S 英語でのコミュニケーションには戸惑った部分もありました。それでも、アジアのメンバーに知り合いができたことは大きな収穫でした。特に韓国のメンバーでお互いに名前は知っていて、ネット上の付き合いがある人物がいたのですが、ICC で実際に会うことができました。ここ数年、コロナ禍で移動もままならない状況だったので、本当に貴重な機会でした。

R お二人と同様、これまで英語でコミュニケーションする機会はほとんどありませんでした。今回、意を決して頑張ったところ、面白いと感じることができ、結果としてアジア圏の知り合いが増えました。

K 引き続き今後の目標などあれば教えてください。CTF プレイヤーとしての目標でも、仕事上のものなどでも構いません。

R SECCON の運営にも携わっていて、ICC で知り合った人たちに、次回の SECCON は対面開催なので、ぜひ参加してほしいと声をかけていました。これが実現できるよう、自分にできることを頑張りたいと思っています。あわせて、CTF プレイヤーの裾野を広げる活動にも注力してきました。これまでも SECCON Beginners の運営や、CTF に関する書籍の執筆などに関わってきましたが、今後も続けたいと考えています。

D 今回 ACSC で上位入賞を果たし、ICC に参加する機会をいただきましたが、自分の実力を客観視すると、まだまだ中堅レベルだという実感があります。Pwn のスキルアップをめざしていますが、次々に新たな技術などが登場しており、その流れについていくことの大変さも自分の中で認識していて、CTF の分野では長期的な目標は立てにくいと感じています。

K 目の前のことを 1 つずつこなしていくことが長期的な目標を達成するためのいちばんの近道だと言われています。今後のご活躍に期待しています。

S 一言でいえば精進を続けるということだと思います。自分の得意分野は Web セキュリティですが、Google CTF のようなトップレベルの大会だと、いまだ手も足も出ないような問題に出会うことがあります。自分の得意ジャンルを伸ばすと同時に、得意でないジャンルについても知識を積み上げていきたいと考えています。

K 最後の質問です。ICC は次回も開催されるとのことで、チャレンジされる方へのメッセージをお願いします。まだ参加できる年齢の方はライバルへのメッセージということにもなると思いますが。

D ICC は間違いなく貴重な経験になると思います。ぜひチャレンジしてください。不安な要素があるかもしれませんが、CTF が好きな者同士が集まっているので、何とかなります。頑張ってください。

S ICC は楽しく貴重な経験でした。自分自身もまだ参加資格があるので、チャレンジしたいと思います。これから、どんどん強いプレイヤーが出てくると思うので、ぜひ一緒に ICC に行きましょう。私も頑張ります。

R 今後は年齢的に参加できなくなるので残念です。海外で対面で開催される CTF に出場できるのは、日本国内でも一部の強豪チームに限られると思います。一方、ACSC や ICC は個人戦で年齢制限もあり上位を狙える可能性がより高いと言えます。海外で CTF をやってみたいと考えている人には、この機会を逃してほしくありません。今回は渡航費も含めてフルサポートで海外に行くことができました。次回以降は不確定な部分もありますが、ACSC の事務局は日本にあり、チャレンジしやすい環境だと思います。

K 本日はありがとうございました。

さいごに

セキュリティ人材育成を背景に、国内でも CTF 大会が注目を集めている。そのような中でも、国を超えたチーム編成で競技に挑む ICC は特別な大会だったといえる。話を伺った参加者たちは皆、国際的なコミュニケーションの壁を乗り越え、アジア各国の友人ができたと、嬉しそうに語ってくれた。

本誌では今後も、セキュリティ人材育成にさまざまな角度から焦点を当てたレポートを紹介していくつもりだ。

参考資料

●公式サイト

・International Cybersecurity Challenge　https://ecsc.eu/icc

・Asian Cyber Security Challenge　https://acsc.asia/

● ICC 攻防戦の競技に使われたサービスのアーカイブ

・CybersecNatLab/ICC2022-AD-CTF　https://github.com/CybersecNatLab/ICC2022-AD-CTF

●関連記事

・セキュリティ・キャンプ ブログ「ICC (International Cybersecurity Challenge) 出場者インタビュー」
https://blog.security-camp.or.jp/posts/icc-2022-interview/

・セキュリティ・キャンプブログ「ICC (International Cybersecurity Challenge) 2022 が開催されました」
https://blog.security-camp.or.jp/posts/icc-2022-report/

・SecurityNEXT「若手国際 CTF で日本人含むアジアチームが好成績 - 言葉や準備不足乗り越え奮闘」
https://www.security-next.com/137706

●プレイヤーが所属する企業のブログ

・DARK MATTER（サイバーディフェンス研究所）「国際地域対抗 CTF の ICC2022 に参加しました」
https://io.cyberdefense.jp/entry/2022/06/27/%E5%9B%BD%E9%9A%9B%E5%9C%B0%E5%9F%9F%E5%AF%BE%E6%8A%97CTF%E3%81%AEICC2022%E3%81%AB%E5%8F%82%E5%8A%A0%E3%81%97%E3%81%BE%E3%81%97%E3%81%9F/

・LAC Watch（ラック）
若手向け国際 CTF 大会「ICC 2022」に出場し 2 位に！奮闘の様子をレポート
https://www.lac.co.jp/lacwatch/people/20220711_003039.html

社会のさまざまな動向を把握し、リスクの変化に対応したセキュリティ体制を構築

Hitachi Systems CSI（Cyber Security Intelligence）Watch 2023.02

文＝日立システムズ

ソフトウェアサプライチェーン攻撃対策に向けた管理の動向

【概要】

ソフトウェアサプライチェーン攻撃から組織を守るために様々な取り組みがあるが、その中でもソフトウェアの構成要素のぜい弱性管理が重要である。その中の仕組みの１つとして SBOM（Software Bill of Materials）があり、以前から一部業界では活用が進められていたが、米国の統合歳出法案（H.R.2617）が可決され、特定のケースにおいて医療機器に関する SBOM の提出が義務化された。日本や他業界へのソフトウェアサプライチェーンマネジメントが加速すると考えられるため、関連する法規および管理技術を注視していく必要がある。

【内容】

2020 年に SolarWinds 社の製品を起点とした攻撃がソフトウェアサプライチェーンに多大な影響を及ぼしたことが話題になった。複数のソフトウェアを組み込んだソフトウェアパッケージ製品は多く存在する。構成するソフトウェアにぜい弱性が見つかった場合、パッケージにも影響が及ぶことになる。このような脅威に対して、ソフトウェア製品の構成要素を含めたセキュリティ管理を行なうソフトウェアサプライチェーンマネージメントが重要視されている。その仕組みの１つに SBOM がある。

SBOM は、ソフトウェアに含まれるパッケージやファイルといったコンポーネントの一覧と、そのバージョン、ライセンス、依存関係などを記載したものである。SBOM は、サプライヤーが顧客に提供することでコンポーネントの詳細を明示

表 ソフトウェアサプライチェーン攻撃と関連動向

時期	発行機関	影響範囲	内容
2019 年 9 月	経産省	日本	「ソフトウェア管理手法等検討タスクフォース」を発足し、SBOM 活用について検討を開始した
2020 年 3 月	IMDRF	国際 / 医療	「医療機器サイバーセキュリティの原則および実施」（IMDRF ガイドライン）を発表し、顧客への SBOM 提供を推奨した
2020 年 6 月	WP29	国際 / 自動車	ソフトウェア管理を求める規則（UN-R-155/UN-R-156）を策定し、自動車業界で SBOM 活用について注目が高まった
2020 年 12 月	-	-	SolarWinds 社を発端とするサプライチェーン攻撃が発生した
2021 年 5 月	米国政府	米国	大統領令（EO14028）によって、米政府向けソフトウェアについて SBOM の提供が必要となった
2021 年 12 月	厚労省	日本 / 医療	IMDRF ガイドラインを周知に向け、ガイドラインに沿った「医療機器のサイバーセキュリティ導入に関する手引書」を公開した
2021 年 12 月	-	-	Log4j（ログ作成ライブラリ）のぜい弱性が発見された
2022 年 4 月	FDA	米国 / 医療	「医療機器サイバーセキュリティ：品質システムに関する考慮事項と市販前提出物の内容に関する草案」にて SBOM の活用・提供を推奨した
2022 年 9 月	欧州委員会	欧州	サイバーレジリエンス法案によって、ネットワーク接続される製品の SBOM 作成が必要となった
2023 年 1 月	米国政府	米国 / 医療	医療機器の SBOM 提出義務化が含まれた、統合歳出法案が可決された

し、透明性を確保することを期待して作られており、顧客にはソフトウェアに含まれるコンポーネントのぜい弱性を管理することが期待されている。医療業界は各業界の中でもソフトウェアサプライチェーンマネジメントが先行しており、IMDRF（国際医療機器規制当局フォーラム）ガイドラインやFDA（Food and Drug Administration）によるガイダンスにおいてSBOMの作成や活用が推奨されていたため、一部で導入が進められていた。今回H.R.2617が可決されたことで、米国では、米国で販売する医療機器がインターネットに接続する場合にFDAへのSBOM提供が義務付けられた。

一方、日本では厚生労働省の「医療機器のサイバーセキュリティ導入に関する手引書」において、ソフトウェアの組み合わせによって医療機器の不具合が生じる可能性を意識する必要があるとされている。医療機器導入の際に開示が求められる一例としてSBOMが挙げられているが提出は義務化されていない。

米国の大統領令に準拠するために必要なSBOMの最小要件が発表されている。この最小要件にはコンポーネント名やそのバージョンなど多数の項目が示されており、手動での生成は難しい。自動生成ツールの活用が期待されるものの、現時点では完全自動化は困難であると考える。マイクロソフトなどのベンダーが無償で提供しているツールを複数検証したが、大統領令の最小要件を満たすSBOMを生成することはできなかった。普及率が高い有償ツールでもSBOM生成の精度は6割程度であった。

日本では、サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースにおいて医療機器・自動車・ソフトウェアの分野別に実証が進められており、令和5年度以降、実証の結果を踏まえてSBOM導入ガイダンスなどのドキュメント整備・普及が検討されている。

【情報源】

https://insidecybersecurity.com/daily-news/omnibus-bill-sets-cyber-requirements-medical-devices-under-fda-review-including-sbom
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/index.html

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.47

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