HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.35

株式会社 日立システムズ

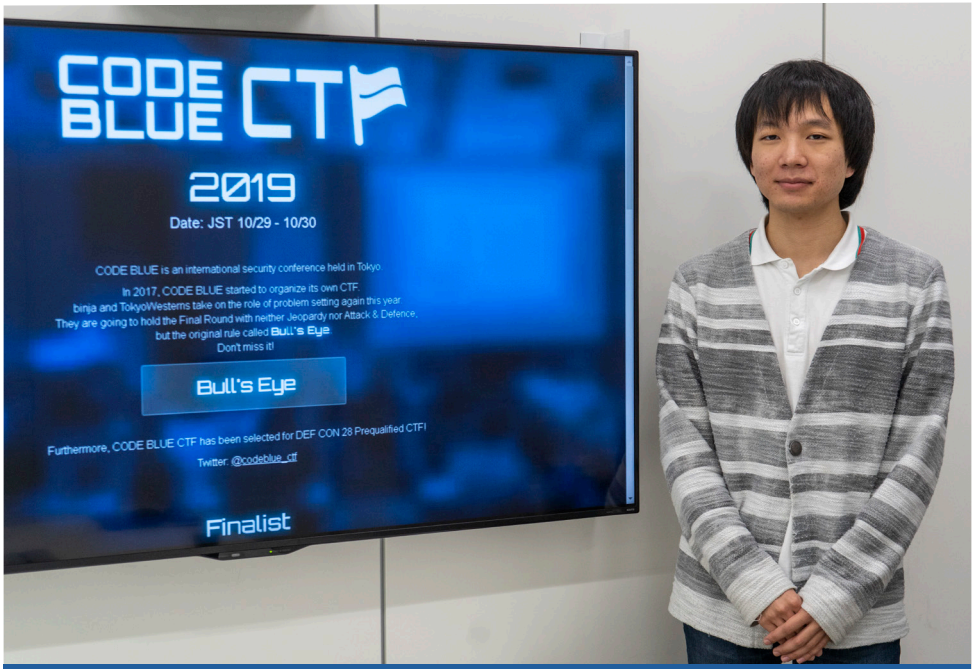
Human * IT

Hitachi Systems security Journal VOL.35

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



日本を代表する CTF チームの 1 つ TokyoWesterns のリーダー

市川 遼 インタビュー

CTF（Capture The Flag）とはサイバー攻撃を模したゲームのこと。日本国内で普及しはじめた当初は「単なる遊び」と揶揄されることもあったが、現在においては人材育成における有効性が認められ、さまざまな組織で実施されるようになってきた。
セキュリティカンファレンス CODE BLUE においても 2017 年から CTF 大会が併催されている。今回はこの大会の運営を担当するチームの 1 つ、TokyoWesterns の市川遼氏にご登場いただいた。
CODE BLUE CTF の競技形式である Bull's Eye をはじめ、CTF プレイヤーとしてのエピソードも伺った。

取材・文・撮影 = 斉藤健一

CODE BLUE CTF と Bull's Eye

斉藤（以下 S ）：当初は、CODE BLUE CTF（以下 CB CTF）を運営する TokyoWesterns（以下 TW）と binja、それぞれのチームの方にお越しいただき、話を伺いたいと考えていました。ですが、binja の小池さんのスケジュールが合わないとのことで市川さんお一人に話を伺うこととなりました。本日はよろしくお願いします。
市川（以下 I ）：こちらこそ。よろしくお願いします。
S 最初に CB CTF をはじめたきっかけについて教えていただけますか。
I もともと、binja の小池君は、世界に通用するオンサイト（会場で競技を行なう）の CTF 大会を自分たちで開催したいと考えていました。また、コンテスト形式についても、新たなアイデアを

持っていました。僕の方も彼のアイデアの実現に協力を申し出ました。これがきっかけとなっています。

S アイデアというのは、Bull's Eye（ブルズ・アイ）のことですね。これについては後ほど伺いたいと思います。以前、CODE BLUE 主催の篠田佳奈さんから、CB CTF の開催はお二人からの提案だったと聞いたことがあります。

I そのとおりです。世界各国の名だたるセキュリティカンファレンスでは CTF が開催されています。そこで CODE BLUE でもぜひ CTF を開催したかったのです。そういった経緯もあり、運営は小池君が率いる binja と、僕がリーダーを務めている TW で行なっています。

S いつ頃のことになりますか。

I 2017 年のことです。ただ、この年に開催した 1 回目の大会は準備不足で Bull's Eye を実施するまでにはいたりませんでした。予選・決勝戦ともに binja が CTF 大会を開催する予定でストックしていた問題を使った Jeopardy 形式の大会となりました。そして、翌年 2018 年の決勝戦において Bull's Eye のシステムをお披露目しました。プロトタイプのようなもので、完成度は高くありませんでしたが、自分たちがやりたかったことは達成できたと思っています。

S では Bull's Eye について伺います。これはどういうシステムなのでしょうか。

I 端的に言うと、サイバー攻撃の精度を競うシステムです。攻撃の精度が高いほど得点につながります。なぜ、こういうシステムにしたかと言うと、CTF は基本的に運営側が用意した環境の中で競技が行なわれます。Jeopardy などでは機密情報に見立てたフラグを取りに行きます。見方を変えればフラグさえ取れればいいわけです。ですからその過程で何度システムを落としても、運営側に環境の再起動をお願いすればよいのです。

S ゲームならではの考え方ですね。

I 従来の競技では攻撃そのものにあまり気を使う必要がなかったのです。しかし、現実世界は違います。攻撃で対象のシステムを落としたからといって、管理者に再起動をお願いすることはできません。

S むしろ管理者側にアラートが上がってしまいますね w

I ですから、精度も攻撃の重要なパラメーターなのだと思っています。

S 攻撃の精度を測るというと、攻撃の試行回数と成功回数の割合を見るということになるのですか。

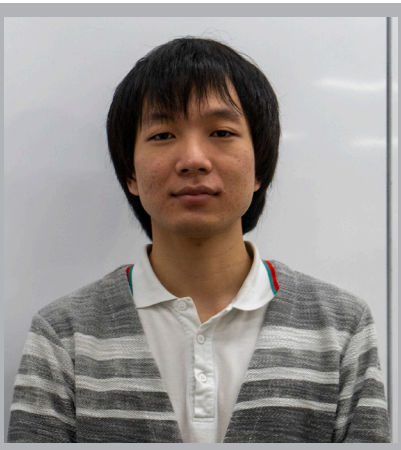
I スコアの計算方法としてはそのとおりです。攻撃する瞬間の環境を何回も再現できるようにしています。例えば攻撃を 1000 回行なったとして、そのうち何回が成功したかを計測することになります。

S 攻撃を何千回も試行させるとなると、問題の作成は従来とは全く違う特殊なものになりますね。同様の形式を採用している大会はありますか？

I 僕らが知るかぎりではありません。

S Bull's Eye に参加したプレイヤーからはどんな反響がありましたか。

I 先ほども言ったとおり、Bull's Eye は 2018 年のファイナルで一度実施しただけです。はじめての試みだったため、いろいろと失敗もしています。プレイヤーからのフィードバックの数としてはまだまだ少ないのですが、概ね好評価を得ています。はじめてのチャレンジを労う意味も込められてい



●市川遼（いちかわ・りょう）

東京農工大学・工学部・情報工学科・修士 2 年生。CTF チーム TokyoWesterns（TW）のリーダーを務める。発足当初は、東京農工大学（小金井・府中）、電気通信大学（調布）、東京高専（八王子）の学生で構成されていた。どの学校も東京西部に位置していることがチーム名の由来。TW はその後、DEFCON CTF を含め海外の CTF 大会において数々の功績を残している。また、2017 年より CODE BLUE CTF をチーム binja と共に開催・運営している。

るのかもしれませんが、ゲームも面白かったという声を聞いています。

今年の CB CTF は DEFCON CTF 2020 のシード権を争う大会に

S ところで、CB CTF 2019の決勝戦に出場するチームはすべて海外勢ですよね。

I 昨年は日本チームも出場していましたが、今年はすべて海外チームになりました。

S この状況の背景には何かありますか。

I いちばん大きな要因は今年の CB CTF 決勝戦の優勝チームには DEFCON CTF 2020 のシード権が与えられることになったからだと思います。オンライン予選の出場チーム数は例年 700 ～ 800 ほどで推移していましたが、今年に関しては 1000 チームを超えていました。シード権を求めて多くのチームが参加した結果です。

S ちなみに、DEFCON CTF のシード権はどういった経緯で舞い込んだのでしょうか。

I シード権の話は僕のところに来ました。2018 年から DEFCON CTF の運営はアリゾナ州立大学の教授が率いるチームが担当しています。実は、僕は昨年この大学で半年間、研究留学をしていたのです。その経緯もあってシード権を与えてくれたのだと思います。

S 大会運営の頑張りに期待しているのですね。

I そうだと思います。

S CB CTF で運営者としてプレイヤーと対峙することとなります。今の時点で意気込みなどあればお聞かせください。

I 現時点ではまだ大会の準備が追いついていませんから、大きな口は叩けません。「どうかお手柔らかにお願いします」といった気持ちですw

劇的だった DEFCON CTF 2019 出場までの道のり

S 引き続き CTF プレイヤーとしてお話を伺いたいと思います。TW が DEFCON CTF 2019 決勝戦に出場するまでの経緯は劇的でした。ご存じない読者のために簡単に説明すると、TW はオンライン予選で敗退し、一度は出場への道を断たれたにも関

2019 年 DEFCON CTF 決勝戦での TokyoWesterns 集合写真
（画像提供 tessy）

わらず、中国で行なわれた DEFCON CHINA の CTF で見事に優勝。シード権を獲得して DEFCON CTF 決勝戦への出場を果たしたというものです。順を追って伺いたいと思います。まずオンライン予選ですが、こちらは何位だったのですか。

I 14 位でした。DEFCON CTF 2019 決勝戦への出場チーム数は前年と比べて縮小し、シードを含めて全 16 チームになりました。予選通過のラインは 10 位までだったのです。2018 年では予選 16 位まで通過できたのですが…

S 本当にあと一歩のところだったのですね。次に DEFCON CHINA CTF について伺います。こちらはどのような経緯で出場することになったのですか。

I DEFCON CHINA CTF（Baidu CTF）は招待制でした。招待を受けた時点では DEFCON CTF のシード大会だとは知りませんでしたが、準備を進めていく中で知りました。

S チームでの参加だったのでしょうか。また競技の手応えはいかがでしたか。

I リモートでの参加も許されていましたのでチームで参加しています。現地に赴いたのは 4 名で、残りは日本からの参戦です。手応えはありました。競技中盤でトップに立ち、そのまま逃げ切ることができました。

S そして DEFCON CTF の決勝戦に出場することになりましたが、こちらはいかがでしたか。

I DEFCON CTF 決勝戦への出場は昨年に引き続き 2 度目になります。TW を結成した当初の目標は DEFCON CTF 決勝戦への出場でしたので、そ

の目標は達成できましたが、昨年も今年も決勝戦で良い成績を残すことはできませんでした。ですが、出場して分かったのは、技術的な側面においてDEFCON CTFは世界最高峰の大会ではないということでした。とはいえ、チームメンバーの層を厚くしないと勝てない大会だという認識も得ましたので、来年以降はTWにこだわらず他のチームとの連携も視野に入れていきたいと思います。

CODE BLUEでの講演について

S 市川さんは、CODE BLUE 2019において、CTFの運営以外に講演も行なう予定です。タイトルは「アンチウイルスをオラクルとしたWindows Defenderに対する新しい攻撃手法」。オラクルと言うと、神のお告げである「神託」や「神託を伝える人」という意味になります。この言葉からイメージするのは、Windows Defenderを「踏み台」としたアプリケーションへの攻撃となりますが、どうなのでしょうか。

I オラクルというのはセキュリティ業界内ではデータリークの文脈で使われることが多いと思います。「パディングオラクル攻撃」というのが有名です。講演の概要をざっくりとお伝えすると、アプリ内で秘密データとユーザーの入力を一緒に保存しているときに、Windows Defenderの動作によって秘密データがリークされてしまうというものです。

S リークを神託と見立てているわけですね。

I はい。元々、CTF問題を作っている過程で思いついたアイデアで、形にしてみたところかなり現実的に通用する手法であることが分かりました。

S 実際のCTFで出題できたのでしょうか。

I Qihoo360が主催するWCTFという大会で出題しました。ところが問題に致命的なバグがあり、出場した全チームに意図しない方法で解かれてしまいましたw

S それは残念です。今後、バグを修正したバージョンの出題などは予定されていますか。

I 実は、CB CTFの予選となったTW CTFで出題しました。手法については事前に告知していましたから、今回は意図した方法で解いてくれたチームが13ほどあって、うれしく思っています。

CTFの活動を通じて得た交流関係

S 先ほど米国で半年ほど留学されたという話が出てきましたが、これについても伺いたいと思います。やはり日本の環境とは違いますか。

I はい。まず資金面でまったく異なります。米国の方が潤沢にありますから、機材などは違いますね。

S それは企業との共同研究などを通じて研究室が独自に資金を得ているからということですか。

I 研究資金の調達にはいくつか方法があるようです。企業との共同研究もその1つですが、米国の大学はもともと学費が高額です。ですから大学自身が潤沢な資金を持っていることもあるようです。

S 留学の経緯はどのようなものだったのですか。

I こちらもCTFつながりでした。自分の中では大学単体で広がった交流関係よりもCTFを通じた交流関係の方が圧倒的に広くなっています。

S 今後のキャリアでもこの経験が活かされるでしょうね。ところで、市川さんは現在、大学院修士2年生ということですが、今後の進路は決まっているのですか。

I いまだに迷っていますが、アカデミックの世界に残るよりも、企業に就職する道を選ぶことになると思います。

S やはりセキュリティ業界へ進むのですか。

I セキュリティエンジニアも選択の1つです。僕自身、CTFがきっかけでコンピューターサイエンスを学ぶようになりました。ですから得た知識は体系的とは言えません。そういった意味では、ソフトウエアエンジニアとして、改めて学び直すのも良いとは考えています。

S 分かりました。今後の活躍にも期待しています。本日はどうもありがとうございました。

隔年開催の技能職種世界大会、本年よりサイバーセキュリティが新職種として採用！

技能五輪国際大会（WorldSkills Kazan 2019）出場レポート

文・写真＝林義徳

技能五輪国際大会に出場

岩崎学園・情報科学専門学校・情報セキュリティ学科・3年、林義徳です。インターネット上では、主に 8ayac というハンドルネームを使って活動しています。普段は Web セキュリティを中心に情報セキュリティの勉強をしながら、趣味でバグバウンティをやっています。

2019 年 8 月 22 日～ 27 日に、ロシア連邦のカザンで開催された第 45 回技能五輪国際大会に、サイバーセキュリティ職種の日本代表選手として出場してきました。

技能五輪国際大会とは、ワールド・スキルズ・インターナショナル (WSI: WorldSkills International) によって開催される、参加国の職業訓練の振興と、参加者の国際親善・交流を目的とした、技能労働者の技能を競う大会です。その正式名称は、国際技能競技大会 (WorldSkill Competition) であり、技能五輪国際大会 (Skills Olympics) とは通称となります。

競技職種は、溶接・配管・西洋料理・洋裁・自動車工など 50 種以上もあります。どのような職種があるのか、興味のある方はぜひ公式サイト※1にアクセスしてみてください。

本大会の参加資格は、一部の職種を除き、大会開催年に満 22 歳以下の者で、過去に同一職種で参加していない者と定められています。参加選手は、各国 1 職種につき 1 名または 1 組です。競技時間はおおむね 20 時間で、数日にわたって実施されます。

なお、技能五輪には国内大会も存在しますが、国際大会とは別物です。しかし、日本では、多くの職種で、国内大会が国際大会への出場権を競う予選会を兼ねているようです。

新規職種に採用された サイバーセキュリティ

サイバーセキュリティ職種は、今年初めて導入された新規職種です。そのため他の職種と比べ、特殊なこともいくつかあったようです。

・参加資格／選手人数

参加資格は、過去に同一職種で参加していない者という点では、他の職種と同様でした。しかし、年齢の制限は異なり、大会開催年に満 25 歳以下の者という少し緩めの制限になっていました。また、参加選手の人数は各国につき 2 名となっており、その 2 名でペアとなり競技に臨むような形式でした。

・代表選手の選考

サイバーセキュリティ職種では、代表選手の選考方法も特殊でした。

一般的には、国内大会で国際大会の代表選手を選考するのですが、サイバーセキュリティ職種では、その方式ではなく、書類選考と技能試験で選考されました。大会開催前年の 10 月頃に書類選考があり、その約 1 カ月後に技能試験がありました。

書類選考で提出すべき書類には、CTF コンテストや情報系コンテストでの入賞実績や、セキュリティの実務的な実績、取得しているセキュリティの国際資格、アウトプットの実績などを記入します。

技能試験では、基本的な情報セキュリティの知識を問う問題や、自由に BadUSB を作成する問題、与えられたログを解析してレポートを作成する問

※1 **WorldSkills International** https://worldskills.org/

題などが出題されました。 試験時間は 3 時間で、インターネットには接続できないという条件の下で行なわれました。 普段から CTF やその他のセキュリティ系のコンテストに参加しているような方からすれば、こういった状況での競技というのは、特殊に感じると思います。 しかし、技能五輪の IT 系職種では、一部の例外を除き、このレギュレーションは一般的なようです。

筆者の場合、学校の教諭の勧めもあり、募集要項の詳細も知らぬまま本大会の選考に応募しました。実をいえば、当時の筆者は書類選考に書ける事柄も多くはなかったですし、技能試験についても最後までやりきれないまま終了してしまいました。ですから、代表に選ばれたことに自分自身も驚いています。もしかすると、選抜には技術力以外の基準があったのかもしれません。

なお、選考は個人単位で行なわれました。大会ではもう 1 人の代表の方とペアを組み競技に臨むこととなります。

サイバーセキュリティ職種の競技

競技は 4 日間あり、各日程の課題のテーマは、以下のように分かれていました。

1 日目　DFIR（Digital Forensics and Incident Response）/Application Security
2 日目　Infrastructure Setup/Security Hardning
3 日目　Capture the flag - Attack
4 日目　Capture the flag - Defense

1 日目は、すでに攻撃された、さまざまなシステムのメモリダンプやイメージファイルなどを与えられて、それを解析する課題や、Web サーバーやファイルサーバーのぜい弱性を特定して修正する課題、コードレビューの課題などに取り組みました。

2 日目は、指定されたサーバやネットワーク機器のコンフィギュレーションを行なうインフラ構築の課題でした。 単に指定されたように構築するだけでなく、各サーバーやネットワーク機器に対し、セキュリティを向上させるといった追加設定の提案を行なうというセキュリティ要素も、この日の課題には含まれていました。

3 日目および 4 日目は、CTF の課題でした。 筆者の印象としては、一般的な CTF というよりも、サイバーレンジと CTF をかけ合わせたような競技だったように感じました。 3 日目と 4 日目は、それぞれ攻撃側と防御側という立場で競技に取り組みますが、基本的には、見つけた flag を submit して、正しければ得点となるというルールです。

3 日目の CTF は、攻撃者として、課題環境を攻撃して flag を探す競技でした。 具体的には、Linux や Windows 上に構築された Web サーバーやファイルサーバー、IRC サーバー、その他のサービスに対し、Kali Linux を用いて攻撃を行なう形式でした。 一般的な CTF のように、それぞれ独立した問題を解いて flag を得るというよりは、強いて言えば、ペネトレーションテスト的な内容でした。

4 日目の CTF は、Blue Team として振る舞い、自チームのサーバーに飛んでくる疑似攻撃を制御しつつ、ログ中から flag を探すといった競技でした。 具体的には、FortiGate や Splunk などを駆使しつつ、疑似攻撃を適切にフィルタリングしたり、ログ中から flag を探す形式でした。

競技内容は以上です。 これらの競技は、1 日 5 時間ずつ 4 日間にわたって、計 20 時間行なわれました。各課題ともに、チーム 2 名で取り組むことになりますので、お互いの協力が不可欠です。例えば、1 日目のコードレビューでは、Pwnable が得意なパートナーの方に C 言語の問題をお任せし、Web セキュリティを勉強している筆者が PHP の問題を担当していました。筆者がパートナーに迷惑をかけてしまう場面もありましたが、全体的に見れば、うまく分担・協力できたと思っています。

なお、予選会と同様に、競技中にインターネットに接続することは許されません。 スマホなどの電子機器も、その日の競技が終了するまでは、会場に用意されたロッカーに預けなければならないため、休憩中であっても、インターネット検索はできないという仕組みになっていました。

大会出場前には訓練に参加

技能五輪国際大会の代表選手は、競技のための訓練を行ないます。また、その費用は国費で賄われます。筆者は、訓練として、専門家によるトレー

ニングを受けたり、実際にコンテストに出場したりしました。

筆者は、もっぱら Web セキュリティを勉強していたため、専門家による DFIR やインフラ構築のトレーニングを受けられたことは幸いでしたし、勉強になりました。 また、海外の大会に参加できたことも、海外経験と競技経験のどちらも乏しい筆者にとっては、非常に幸運かつ貴重で有意義な経験でした。 具体的には、本文書の前号※2で執筆した、DEFCON 27 OpenCTF 以外にも、インドのチェンナイで開催された The International Cyber Security Challenge 2019 (World Skills India) というコンテストにも出場しました。

訓練として、費用を負担してもらいながら、貴重な経験や勉強をさせてもらえるというのは、学生の筆者にとっては大変幸運なことでした。

競技中の様子／競技者同士の交流

サイバーセキュリティ職種には、日本・アメリカ・イギリス・インド・オマーン・シンガポール・フィリピン・ブラジル・メキシコ・ロシア・中国の 11 カ国から 22 名の選手が参加していました。

競技が始まる前や終了した後には、彼らとの交流を十分に楽しむことができました。 特に、競技終了後に、各国がどのようなアプローチで課題をこなしたのかを、語り合うのは最上のひとときでした。

また、技能五輪国際大会の伝統的な文化でもあるピントレーディングも、良い思い出となりました。ピントレーディングとは、ピンバッジの交換を通じた交流方法です。 他国の選手と挨拶代わりに、ピンバッジを交換します。 この交流を想定して、日本の代表選手やエキスパートと呼ばれる役職の人物には、4 種類 100 個のピンバッジが事前に配られました。 技能五輪を見学していた一般参加者の方からもトレードを申し込まれることが多く、見境なくトレードしていれば、その 100 個は、あっという間に使い切ることができたと思います。 なお、筆者も気に入っている桜をモチーフにしたピンバッジが、外国の方からも人気だったことは印象的です。


集合写真（プライバシーを配慮しボカシ加工を行なっています）

他にも、印象的な出来事といえば、競技中の観衆との距離が近いことです。 サイバーセキュリティ職種の競技は、大きなホールの一角で行なわれていたのですが、目と鼻の先に観衆がいる状態で競技に取り組みました。 仕切りはあるものの、成人男性の腰の高さ程度しかなく、握手もできる距離感です。 競技中に、実際に声をかけられたときは、とても驚きました。 他の職種でも同様に観衆と競技者の距離は非常に近く、観ている側としては、間近でいろいろな競技を見ることができるので、非常に良い仕組みだなと感じました。 他の IT 系職種では、作業画面が、観衆側のモニターにも複製されているものがありましたが、サイバーセキュリティ職種では、そうではありませんでした。画面が複製されるのはとても恥ずかしいので、これは幸いでした。

なお、競技の最終結果は、以下のとおりです。この結果は、受賞国を抜粋したものですので、詳細は WorldSkills Kazan 2019 のアーカイブ※3 をご覧下さい。

金メダル ロシア
銀メダル 中国
銅メダル ブラジル、シンガポール
敢闘賞 インド、日本

日本チームの順位としては、6 位という結果で、敢闘賞（Medallion for Excellence）を獲得するこ

※ 2 **Hitachi Systems Security Journal** https://www.hitachi-systems.com/report/specialist/hj/
※ 3 **WorldSkills Kazan 2019 Results** https://worldskills2019.com/en/event/results#cyber-security


表彰式の様子



メダリオン・パスカード・交換したピンバッジ（左）桜のピンバッジ（右）

とができました。 表彰式は、カザン・アリーナという大きなスタジアムで大大的に行なわれましたが、惜しくも、表彰台に上がれるのは銅メダルまででした。

競技以外も充実

筆者としては、競技以外の行事にも、刺激的な体験は少なくありませんでした。

例えば、国内での表敬訪問です。 赤坂東邸にて皇嗣同妃両殿下に拝謁し、首相官邸では菅官房長官から激励を受けるなど、またとない経験をさせていただきました。

次に、開催国ロシアでのエクスカーション（体験型見学会）です。 カザンの伝統的な歌や踊りを体験したり、現地の学校でカザンの伝統料理をいただいたり、絵付けの体験をしました。 他にも、カザン・クレムリンや赤の広場などの有名な世界遺産を現地の方の案内の下、巡るような行事もありました。 現地は本大会を盛り上げようという活気に溢れており、歓迎ムードに包まれていたように思います。

また、カザン・アリーナで行なわれた開会式や閉会式も大規模で刺激的な経験でした。 花火が打ち上げられたり、さまざまな歌や踊りのパフォーマンスを観覧しているうちに、自分が競技をしに来たことを忘れてしまいそうになったほどです。

なお、開会式の様子は、WorldSkills Kazan 2019 のFacebookページ※4で視聴することができます。

技能五輪国際大会に参加して

今回、筆者は本大会にサイバーセキュリティ職種の代表選手として出場しましたが、それは単に競技を行なうだけの役割ではなかったように思います。 本大会の目的である、国際親善や交流のための役割も担っていることには、実を言えば、現地に着いてから気づきました。 結果的に、この目的をよく果たせているのだとすれば嬉しいかぎりです。

本大会のサイバーセキュリティ職種の競技については、今大会が初めてだったということもあり、不完全な部分があったことは理解できますが、正直なところ、納得できないこともありました。 しかし、学習の機会として、非常に良い経験が多く積めたので、総合的には満足しています。 例えば、自身では Web セキュリティのことばかり勉強してしまいがちなので、このような機会に他の分野の勉強をできたことは、有意義でした。 また、訓練や実際の競技中など、あらゆる場面で、自身の未熟さを痛感させられたのは、その後の学習のモチベーション向上に繋がった良い経験でした。

全体を振り返り、刺激に満ちた、貴重な経験の連続でした。 このような経験をさせていただけたこと、さまざまな人がサポートしてくれたことに感謝します。 皆さま、ありがとうございました。

※ 4 **WorldSkills Kazan 2019 Facebook** https://www.facebook.com/WorldSkills/videos/1657198351080425/

参考資料

https://ja.wikipedia.org/wiki/ 国際技能競技大会

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.35

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