SHIELD Security Research Center

Hisys Journal

VOL.34

HITACHI
Inspire the Next

日立システムズ

Hisys Journal VOL.34

TABLE OF CONTENTS

サイバーセキュリティの学びのハードルを下げたい
林 憲明 インタビュー …… 3

DEFCON 27 OpenCTF 2019 参戦レポート …… 8

●はじめに

本文書は、株式会社日立システムズ セキュリティリサーチセンタが運営するセキュリティ情報サイト、S.S.R.C.(Shield Security Research Center) の公開資料です。本サイトでは、本文書のバックナンバーをはじめ、S.S.R.C. によるリサーチ結果などを随時公開しています。
S.S.R.C. http://www.shield.ne.jp/ssrc/

●ご利用条件

本文書内の文章等すべての情報掲載に当たりまして、株式会社日立システムズ（以下、「当社」といいます。）と致しましても細心の注意を払っておりますが、その内容に誤りや欠陥があった場合にも、いかなる保証もするものではありません。本文書をご利用いただいたことにより生じた損害につきましても、当社は一切責任を負いかねます。
本文書に記載した会社名・製品名は各社の商標または登録商標です。
本文書に掲載されている情報は、掲載した時点のものです。掲載した時点以降に変更される場合もありますので、あらかじめご了承ください。
本文書の一部または全部を著作権法が定める範囲を超えて複製・転載することを禁じます。

© Hitachi Systems, Ltd. 2019. All rights reserved.

サイバーセキュリティの学びのハードルを下げたい！
林憲明 インタビュー

林憲明氏はセキュリティ対策ソフトウェアベンダーに在籍し活躍する一方、社外のさまざまな組織においてもサイバーセキュリティ人材育成のために尽力している。その成果は、サイバー犯罪捜査の知識体系からカードゲームにいたるまで幅広い。精力的に活動する林氏のモチベーションはどこにあるのか話を伺うこととした。

取材・文・撮影＝斉藤健一

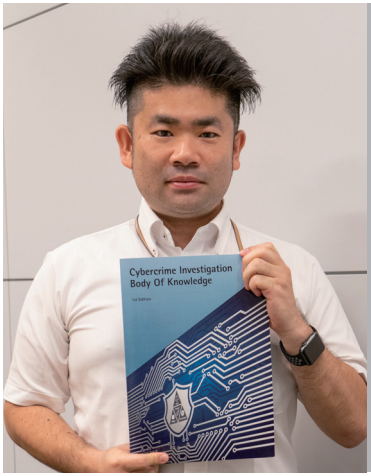
サイバー犯罪捜査の知識体系（CIBOK）とは

斉藤（以下 S ）：林さんはトレンドマイクロ社で活躍される一方、フィッシング対策協議会※1やJC3（日本サイバー犯罪対策センター）※2などでも活動されています。冒頭から個人的な話題で恐縮ですが、林さんとは以前から某 SNS で友達として繋がっています。本年 7 月くらいでしょうか、林さんのタイムラインを見ていて、とある投稿が気になりました。それは、林さんがサイバー犯罪捜査に関連する CIBOK（シーボック）という書籍の執筆者の 1 人であり、書籍のダイジェスト版を配布しているというものでした。早速送っていただき読んでみると、技術的な知見というより、むしろ犯罪捜査手法全般を俯瞰的に捉えた内容で、とても新鮮に感じました。今回のインタビューでは、最初に CIBOK について伺いたいと思います。よろしくお願いします。

林（以下 H ）：こちらこそ、よろしくお願いします。

S 単刀直入にお聞きしますが、この CIBOK とその発行元である CIKF という団体について簡単に

※1 **フィッシング対策協議会** https://www.antiphishing.jp/
※2 **JC3（日本サイバー犯罪対策センター）** https://www.jc3.or.jp/



●林 憲明（はやし・のりあき）
一般社団法人 サイバー犯罪捜査・調査ナレッジフォーラム
CIBOK 執筆者
2002 年にトレンドマイクロ株式会社に入社。1 年間の米国勤務から帰国後、国内専門のマルウェア解析機関を経て、先端脅威研究組織へ。現在は、日本におけるサイバー犯罪対策、特にオンライン詐欺を専門とした調査・分析業務を担当。また、研究諸機関や法執行機関における窓口として、情報共有や共同研究なども実施している。
これら業務の一環として、法執行機関や国際刑事警察機構（INTERPOL）でのトレーニング講師の実績あり。CIBOK 編集委員会（Editorial Committee）へ 3 ヵ国、12 人からなる執筆者の 1 人として参画。2017 年 4 月、『サイバー犯罪捜査知識体系ガイド（CIBOK：Cybercrime Investigation Body Of Knowledge）、シーボック』第 1 版（1st Edition）のリリースを行っている。CIBOK の編纂にあたり、国内外の警察組織に対するヒアリングを実施。「Job Task Analysis（職務分析）」も担当している。
フィッシング対策協議会 運営委員
情報処理技術者試験委員 及び 情報処理安全確保支援士試験委員
NPO 日本ネットワークセキュリティ協会 教育部会

説明していただけますか。

H CIBOK とは、Cybercrime Investigation Body of Knowledge（サイバー犯罪捜査知識体系）の略称で、CIKF（Cybercrime Investigation Knowledge Forum）はその管理団体であり、トレンドマイクロ社が発起人となっています※3※4。

S 林さんが参加された理由の一端がわかりました。

H 2013 年ごろだったと思いますが、国内外の法執行機関からトレンドマイクロ社に人材育成に関する協力要請がありました。当初は試行錯誤しながらもマルウェア解析、リバースエンジニアリング、ペネトレーションテスト、デジタルフォレンジックなどの知識や技能をトレーニングとして提供していました。

S セキュリティ対策ソフトウェアベンダーの強みを活かしたトレーニングですね。

H ただ、こうした活動を進める中で違和感を持つようになったのです。感覚的に言えば、土台のないところにさまざまなものを積み上げているようなものです。トレーニングを終えた直後の満足度は高いのですが、参加者それぞれが自組織に戻った時に、得た知識や技能が活かせるかというと、必ずしもそうではないと感じていたのです。そこで土台となるものを提供しようと考えました。コンピューターに例えれば「OS」のようなものです。リバースエンジニアリングやデジタルフォレンジックなどは「アプリ」という位置付けです。

S これが CIBOK 発刊・編集の動機になったというわけですね。

H そのとおりです。CIBOK とは、サイバー犯罪捜査を体系化したもので、知識や技能の前提となる「心得」のようなものです。もう少し具体的に言えば、サイバー犯罪捜査を実行するフレームワークです。捜査は大きく 3 つの階層に分けることができます。サイバー犯罪の種類などを知る「準備的な行動」、証拠の収集や分析といった「事件解決に向けた行動」、さらに他の組織と協力するための「犯罪情報の共有」などです。

S リバースエンジニアリングやデジタルフォレンジックといった技術は「事件解決に向けた行動」の中に含まれるのですね。

H はい。CIBOK ではサイバー犯罪捜査における実行フレーム以外にも、捜査チームのマネージメントにも触れています。

S ダイジェスト版を拝見させていただいた時、捜査チームのマネージメントについては、法執行機関に限らず CSIRT 運営にも役立つ部分があるのではないかと思いました。

H そのとおりです。CSIRT 運営に関するニーズはありましたから、CIBOK の中に積極的に取り込み・

※3 **CIBOK** https://www.cibok.org/ja/
※4 **Trend Micro Sponsors First Ever Guide for Cybercriminal Investigations**
https://newsroom.trendmicro.com/press-release/alliances/trend-micro-sponsors-first-ever-guide-cybercriminal-investigations

拾い上げるようにしました。

S CIBOK には他にどんな特長がありますか。他の教育プログラムとの違いなどがあれば教えてください。

H サイバー犯罪領域に関する体系化というのはほとんど存在しないので単純な比較はできません。近いものとしては、英国ブリストル大学の CyBOK（Cyber Security Body of Knowledge）が挙げられます※5。他にも JNSA の教育部会がまとめている SecBoK も考え方としては近いと思います※6。ただ、どちらも知識・技能領域に力を入れているという印象です。CIBOK では知識・技能領域については軽く触れる程度です。別の言い方をすれば知識・技能については他の教材などに任せています。あえて言うとすれば、この点が特長なのかもしれません。

S 他の教材やトレーニングベンダーなどと互いに補完するということですね。ダイジェスト日本語版は 30 ページほどの分量ですが、CIBOK 本体は何ページくらいあるのでしょうか。

H 英語版・日本語版ともに 320 ～ 330 ページほどの分量です。

S 相当の分量ですね。ダイジェスト版を制作された経緯を教えてください。

H 2018 年にサイバー防衛に関する CYDEF という国際会議で講演する機会がありました※7。この時、主催側から予稿集の提出を求められ、Capability of supporting human resources development cyber crime Unit という名でまとめたのです。評判がたいへん良かったので、これをベースにダイジェスト版を制作することにしました。

S 確かに 300 ページ超の書籍だと簡単には手を出せませんが、ダイジェスト版なら読んでみたいという気になります。読んだ方の反応を具体的に教えていただけますか。

H 知識・技能系の書籍だと思っていたけれど、実際に読んでみたら違っていた。知識・技能系に重きをおかない内容は意外だったけれど共感できた。最初に知識体系を明確にしてから学びはじめる方法もありだと思った。などの声をいただいています。

S ダイジェスト版を CIKF の Web サイトで公開するといった計画はありますか。

H 現在のところありませんが、今後要望が多ければ検討したいと思います。その前にダイジェスト版の存在が余り知られていませんので、そこをクリアすることが課題だと感じています。

職人的な学び方から知識体系へ

S 林さんご自身、この CIBOK を使ったトレーニングで講師を務めることもあるかと思います。参加者の感想はいかがですか。

H 私が対応したのは日本国内の参加者を対象としたものになります。その反応は両極端です。知識体系よりも明日から使えるデジタルフォレンジックの講義をしてほしいという意見もありました。指導者に師事して技を盗むような職人の世界を好む人には BoK（知識体系）という考え方はフィットしにくいのかもしれません。一方で BoK に賛同してくれる人もいます。トレーニングではケーススタディのような演習を何度も行いますからそこでの学びが大きかったという声も聞きます。

S 学ぶスタイルは人それぞれですね。自分の得意な分野から知識や技術の習得を始めた人でも、いつか全体像の中での自分の立ち位置や自分に足りないものが見えてくる、もしくは知りたくなる時期が来るはずです。その意味でも早い段階で全体像（知識体系）を得ておくことは重要だと思います。

サイバーセキュリティの学びのハードルを下げるために

S CIBOK に携わるようになった経緯を教えてください。

H 以前はグローバルのリサーチ部門に在籍していましたが、個人的には日本国内で貢献できることをしたいと感じるようになりました。その時に CIBOK の話をいただき、プロジェクトに参加するようになりました。

S 再び SNS からの話題で恐縮ですが、林さんがセキュリティに関連したボードゲームやカードゲームの開発にも携われていることを知りまし

※5 **CyBOK** https://www.cybok.org/
※6 **SecBoK** https://www.jnsa.org/result/2018/skillmap/
※7 **CYDEF** http://www.cydef-web.jp/index.html

た。CIBOK も同様だと思うのですが、こちらも人材教育の一環として携われたのでしょうか。

H そのとおりです。セキュリティを学ぶハードルを下げたいという思いからでした。現在でも CTF は人気ですが、挑戦したくてもハードルが高いという層が一定数いて、そういう声に応えるためにどうしたらよいかと試行錯誤していましたが、その結果がボードゲームやカードゲームの開発でした。

S どのようなゲームか簡単に教えていただけますか。

H 1 つは「インシデント対応ボードゲーム」というもので、トレンドマイクロ社のコンテンツとなっています※ 8。それぞれのプレイヤーは企業の経営責任者・情報システム責任者・システム管理者・広報担当などに扮して組織で発生したセキュリティインシデントに対応していきます。サイバーセキュリティ机上演習（TTX：Table Top Exercise）にも似ていますが、ゲーム的な要素を増やしたものとなっています。

S 以前、このゲームの競技の模様を取材したことがあります。プレイヤー同士がコミュニケーションを通じて多くのことに気づく様子を目にしました。もう 1 つ、「セキュ狼」がありましたが、こちらはどういったものになりますか。

H 正式名称を「セキュリティ専門家 人狼」といいます※ 9。JNSA 教育部会のワーキンググループで制作しました。全く知らない方のために簡単に説明すると、人狼は多人数でプレイするカードゲームです。各人に配られたカードにしたがい、村人と人狼という 2 つの陣営に分かれてプレイします。村人は自分の役割しかわかりませんが、人狼は自分以外の誰が人狼なのかを知ることができます。ゲームの各ターンにおいて、村人は人狼とおぼしき人物を追放します。一方、人狼は村人の 1 人を襲い、消し去ることができます。人狼がゼロとなれば村人の勝利となり、村人と人狼の人数が同じになれば人狼側の勝利となります。ゲームはプレイヤー同士の会話が中心の心理戦です。セキュ狼ではゲームの舞台が企業の CSIRT となり、

狼の役割が内部で不正を働く汚職者やブラックハットハッカーに置き換わっています。

S 最近、セキュ狼がモバイルゲームアプリになったという記事も見かけました※ 10。

H 岩崎学園情報科学専門学校の学生有志と協同で開発しました。現在、Android 版が Google Play で公開されています。アナログ版ではさまざまな判定を行う審判が必要ですが、モバイル版なら審判不要で全員がプレイできます。

S セキュ狼ではゲームを通じてどんなことが得られると思いますか。

H プレイヤー同士の人的交流はもちろんのこと、ゲームの中で起こる内部不正の恐ろしさを知ることができると思います。日本人は人を疑うのが苦手ですから、せめてゲームの中で疑似体験としてでも学べることは、良い機会だと思います。

S サイバーセキュリティ領域では監査法人のプレゼンスが高まっているように感じますが、これは内部不正が行われるケースが増えていることの証左なのかもしれませんね。

文系と理系の垣根を取り払う

S 先ほどの話と関連しますが、学びのハードルはどんな点にあると思われますか。

※ 8 **インシデント対応ボードゲーム**
https://resources.trendmicro.com/jp-docdownload-form-m057-web-incidentboardgamestandard.html

※ 9 **セキュリティ専門家 人狼** https://www.jnsa.org/edu/secgame/secwerewolf/secwerewolf.html

※ 10 **JNSA と情報科学専門学校、ゲームで内部不正を学べるスマートフォンアプリ『セキュリティ専門家 人狼』を共同開発**
https://www.jnsa.org/press/2019/190724.pdf

H 主に 2 つあると考えています。1 つはとっつきにくい外国語の用語がたくさんある点です。もう 1 つ、これは最初のハードルとある意味で近いのかもしれませんが、サイバーセキュリティ領域の中で最先端の情報を得るには英語が必要になるという点です。最前線にいる専門家にとっては当たり前の状況ですが、自然科学の領域などではノーベル賞級の研究であっても母国語である日本語で学ぶことができます。

S 確かに日本語の情報が増えれば学ぶ人も増えると思います。最近ではセキュリティエンジニアが高収入だと話題になることもありますから、経済的な理由でエンジニアを目指す人が増えるかもしれません。どちらかの状況が好転すれば、もう一方も良い方向に動き出しそうですね。

H コンピューターサイエンスの外側にいる人たちにもサイバーセキュリティの世界に入ってきてほしいと思っています。米国では、政治学・犯罪学・心理学などの専門家がサイバーセキュリティ領域に入ってきています。例えば、公共政策の研究者がリバースエンジニアリングについても学ぶといったイメージです。

S 日本だと考えられない状況ですね。

H 日本では理系と文系を区別して垣根を作ってしまうことも多いですよね。こういった状況は変えていきたいと考え、私自身も社会人大学院で著作権法を学び修士号を取得しました。

S 修士論文のテーマはどのようなものだったのですか。

H「著作権法から見るリバースエンジニアリング」です。フェアユースがテーマです。ソフトウェアや IoT 機器（当時は組込機器と呼んでいました）のユーザーによるリバースエンジニアリングの是非を問うものでした。

S 確かに。現実世界において、技術と社会は密接に関係していますから、双方の分野を学ぶことも不思議なことではありませんね。

4 つの「助」に与する

S 林さんご自身のキャリアの中で、今後取り組みたいことがあれば教えてください。

H 私自身が活動するフィッシング対策協議会の中でも言っていることなのですが、4 つの助けを実践していきたいと思っています。

S 4 つの助けとは何を指しますか。

H まず自分自身で行う「自助」です。また、1 人でできることには限界がありますから、共に助け合う「共助」。次に共に資金を供出する「互助」、これはいわば業界団体のようなものです。さらに公を巻き込んで行う「公助」へと発展していきます。私自身はこの輪の中で「プロボノ」として活動していきたいと考えています。

S プロボノとは何でしょう。

H 各分野の専門家が職業上持っている知識やスキルを提供して社会貢献する考え方です。単にボランティアというと「誰でもいいので時間をください」ということになりますが、プロボノでは各自の専門性を活かして公共利益のために協力することになります。そして、この考え方がセキュリティ業界の中で、もっと広がってくれることを期待しています。

S そのとおりですね。

H この一連の活動がうまく機能している例が、フィッシング対策だと思っています。Twitter などでは、フィッシングメールやサイトの情報に関する投稿が盛んです。

S Twitter で「フィッシングサイト」などのワードで検索すると、一般ユーザーが注意を喚起する投稿なども見つかりますね。

H オンライン詐欺という課題に対して、皆が積極的に協力している。しかも目に見えやすい。さらにその結果はセキュリティ製品やサービス、フィッシング対策協議会のページなどにも反映されていきます。こうした輪がもっと広がっていくと、少しずつでも安全・安心なインターネットの実現に繋がっていくと思います。他にも JC3、デジタル・フォレンジック研究会[※11] 、JNSA といった組織においても「プロボノ」として活動していきたいと考えています。

S 本日は興味深い話を伺うことができました。ありがとうございます。

※ 11 **デジタル・フォレンジック研究会** https://digitalforensic.jp/

米国ラスベガスで開催されたハッカーの祭典！ オープン参加の CTF で腕試し !!

DEFCON 27 OpenCTF 2019 参戦レポート

文 = 林義徳
画像提供（一部）=tessy

Open CTF 2019 に参加した経緯

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。

OpenCTF 2019 には、技能五輪国際大会の訓練の一貫で、参加しました。 技能五輪国際大会とは、筆者が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た、2019 年 8 月 22 日～ 27 日にロシア連邦のカザンで開催された WorldSkills Kazan 2019 のことです。当該大会の競技内容に CTF が含まれていたため、その対策と海外での競技に慣れる目的で、DEFCON27 で開催された OpenCTF 2019 に参加したという経緯です。

OpenCTF とは

OpenCTF 2019 と は、Neg9(a.k.a Negative Nine Security, Neg9!) に よ っ て、2019 年 8 月 9 日 10:00(UTC) ～ 10 日 20:00(UTC) に、DEFCON27 内で開催された CTF コンテストです。世界的に有名な DEFCON CTF とは別物で、DEFCON に参加しているすべての人が参加できるイベントでした。問題には、DEFCON のネットワーク内のどこからでも取り組めるようになっており、ずっと席に座っている必要もなく、ふらっと別の会場を周ることもできるような形式でした。 後述の hardware というジャンルの問題に取り組む際には、会場に戻って課題の機材を借りる必要があったようです。

CTF の形式は Jeopardy 形式で、問題のジャンルは全部で 9 つあり、web、pwnable、hardware、trivia、misc、reversing、sanitycheck、recon、crypto と、幅広く出題されていました。 難易度についても、初心者から上級者まで楽しめるように、簡単なものから難しいものまで幅広く出題されていたようです。

問題の解説

どんな問題が出たのかという例として、Writeup（解答例）を紹介します。紹介するのは、文字数の都合上、2 問だけに絞りました。実際に出題された問題は、OpenCTF 公式サイトで確認することができます。※ 1

なお、今回のコンテストで筆者が解けたのは、ほぼ " やるだけ " の問題だけでした。その点はご了承ください。

• [Web] Stylist 10pt

Decode a flag within an HTML page. という問題文とともに、図 1（次頁）のような stylist.html というファイルを与えられます。

まず、html>body>div#blocks 内のすべての要素 style 属性の値が ascii コードになっていることがわかります。 id が n00、n01、n02、n03 の要素の style 属性の値にあるカラーコードを ascii コードとみなして、それぞれ文字に変換すると、'flag' という文字列が出てくるので、残りも n05、n06、n07… と同じ作業を繰り返せば、flag が出てきそうです。 これを手作業でやるのは面倒なの

※ 1 **OpenCTF 公式サイト** https://scoreboard.openctf.cat/challenges
問題を確認するためにはプレイヤー登録が必要

で、図 2 のようなワンライナーを使って解くことができます。

実際に実行して得られた flag が、flag{the_rabbit_got_a_hare_cut} です。

- **[misc] TaeandMe 84pt**

問題文は以下のとおりです。

Haha, let's chat!
challenges.openctf.cat:9009

サーバーに接続したときの応答は図 3 のとおりです。何かチャットのようなプログラムが動いていることがわかります。

接続直後のメッセージで指定されたハッシュの

```
<!DOCTYPE html>
<html>
  ⋮
  <body>
    <div id="blocks">
      <div id="n11" style="background: #000062;"></div>
      <div id="n29" style="background: #000074;"></div>
      <div id="n26" style="background: #00005f;"></div>
      <div id="n17" style="background: #00006f;"></div>
      <div id="n08" style="background: #00005f;"></div>
      <div id="n20" style="background: #000061;"></div>
      <div id="n06" style="background: #000068;"></div>
      <div id="n09" style="background: #000072;"></div>
      <div id="n14" style="background: #000074;"></div>
      <div id="n04" style="background: #00007b;"></div>
      <div id="n27" style="background: #000063;"></div>
      <div id="n24" style="background: #000072;"></div>
      <div id="n23" style="background: #000061;"></div>
      <div id="n10" style="background: #000061;"></div>
      <div id="n15" style="background: #00005f;"></div>
      <div id="n01" style="background: #00006c;"></div>
      <div id="n16" style="background: #000067;"></div>
      <div id="n03" style="background: #000067;"></div>
      <div id="n13" style="background: #000069;"></div>
      <div id="n00" style="background: #000066;"></div>
      <div id="n02" style="background: #000061;"></div>
      <div id="n05" style="background: #000074;"></div>
      <div id="n12" style="background: #000062;"></div>
      <div id="n28" style="background: #000075;"></div>
      <div id="n19" style="background: #00005f;"></div>
      <div id="n22" style="background: #000068;"></div>
      <div id="n18" style="background: #000074;"></div>
      <div id="n30" style="background: #00007d;"></div>
      <div id="n21" style="background: #00005f;"></div>
      <div id="n07" style="background: #000065;"></div>
      <div id="n25" style="background: #000065;"></div>
    </div>
  </body>
</html>
```

図 1 [Web] Stylist で出題された HTML ファイル

```
$ cat stylist.html | grep '<div id=\"n' | sort | grep -o "#.*;" | awk
'{print substr($0, 6, 2)}' | tr '\n' ' ' | python3 -c "import sys; print(''.
join([chr(int(c, 16)) for c in sys.stdin.read().split()]));"
```

図 2 問題を解くためのワンライナー

ような文字列は、接続するたびに変わるのですが、その文字列をサーバー側のプログラムにしゃべらせる（表示させる）ことができれば、flag が得られるようです。 いろいろと試すうちに、自分が入力した文字を、サーバー側がそのまま返すことがあることがわかりました。 あとは、接続直後に与えられたハッシュのような文字列を何度も入力していけば良さそうです。 そこで図 4 の python スクリプトで自動化しました。
これを実行して、しばらく待つと、flag{1t_wuz_ma!d_up_:clap:} という flag が手に入りました。

競技中の様子

コンテスト中には、参加者同士が歓談している様子も見られ、CTF コンテストとして取り組んでいる人よりも、余興として楽しんでいる参加者の方が多かった印象を受けました。 競技中も DEFCON CTF の会場と比べると、賑やかで、空気もピリついた感じではありませんでした。

競技には DEFCON のネットワーク内からであれば、どこからでも取り組めるようになっていたため、2 日目は、競技会場として用意されていたスペースの人も減っていた気がします。　筆者も 2 日目は、ほとんど競技会場で席に座っていることはなく、他の会場を周りながら、行った先々で空いている席を探して、問題に取り組んだりしていました。

なお、競技の結果は以下のとおりです。

1 位 noproblem 2936pt
2 位 OpenToTall 2152pt
3 位 IE6 2040pt

筆者は、同行していただいた tessy さんとチーム（You like Stone IPA）を組んで参加しており、最終的に 134pt を獲得し、54 位という結果に終わりました。

DEFCON27/OpenCTF 2019 に参加して

今回、OpenCTF 2019 に参加した目的は、技能五輪国際大会の訓練の一貫で、海外での競技や雰囲気に慣れるためでした。

結果的に、目的に対し有意義な経験ができ、技能五輪では、始終落ち着いて競技に臨むことがで

```
$ nc  challenges.openctf.cat 9009
If you can make me say 9059b24f0650c518c81298e471a37f086fd37b17 then I will
tell you the flag.
hoge
This is- this is kangaroo court!
fuga
if on Monday week this happens again you will not stay in the courtroom.
```

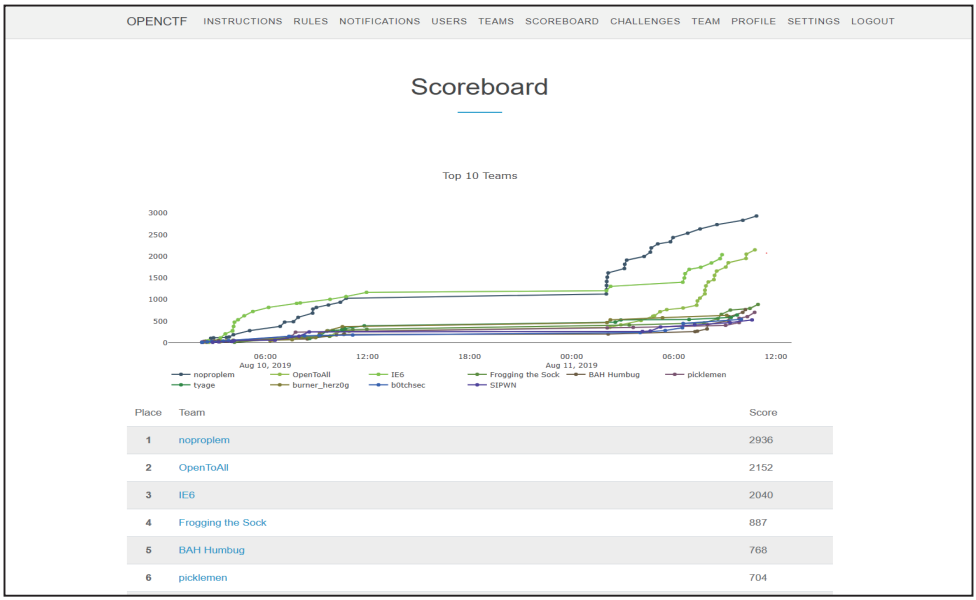
図 3 問題サーバーに接続、文字列を入力したときどんな出力になるか確認したところ

```
import re
from pwn import *

r = remote('challenges.openctf.cat', 9009)
s = r.recvline().split()[6]

for i in range(10000):
   r.sendline(s)
   resp = r.recv(2048)
   if "flag{" in resp:
       print(re.findall('flag{.*}', resp)[0])
       exit(0)
```

図 4 問題を解くために作成した python スクリプト



Place	Team	Score
1	noproplem	2936
2	OpenToAll	2152
3	IE6	2040
4	Frogging the Sock	887
5	BAH Humbug	768
6	picklemen	704

図 5 上位チームの得点推移を示すスコアボード

OpenCTF 会場の様子

問題に取り組む筆者。DEFCON 会場内であればどこからでも参戦できる（画像提供：tessy）

きました。

また、DEFCON27 に参加した数日間は、楽しく、非常に刺激的でした。

DEFCON の存在は、２年半前ぐらいから情報セキュリティの勉強を始めてから、だいぶ早い段階で知っていて、いつか行ってみたいと思っていたのですが、こんなにも早く参加できて嬉しかったです。

OpenCTF への参加はもちろんのこと、聴講や、Village/Contest エリアの見学などを通し、自身の技術力の未熟さも痛感させられました。

常に圧倒されっぱなしの DEFCON 初参加でしたが、全体を通して、非常に良い経験をさせてもらえたことに感謝しています。

最後に余談になりますが、本記事の序盤で軽く触れた、技能五輪国際大会の結果は敢闘賞（6 位）という結果でした。次号にて、当該大会の詳細や参加レポートを執筆予定です。