HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.38

株式会社 日立システムズ

Human * IT

Hitachi Systems security Journal VOL.38

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

機械学習を
サイバーセキュリティに生かす！

新井悠 インタビュー

今回話を伺う新井悠氏が情報セキュリティ業界でキャリアをスタートしたのが 2000 年。以来、数々の職種を経験する中で、ぜい弱性調査・マルウェア解析・機械学習といった分野の技術力を磨いてきたという。そうした知見を踏まえ、これからのセキュリティエンジニアに求められるスキルや、ウィズ・コロナ時代のサイバーセキュリティといったテーマで語っていただいた。なお、インタビューはオンラインで行なった。

取材・文 = 斉藤健一　写真提供 =NTT データ

就活時代に目にした新聞記事が セキュリティ業界に進むきっかけに

斉藤（以下 S ）新井さんとはこれまできちんとお話しする機会がありませんでした。これまでの経歴から簡単に伺いたいと思います。大学では何を専攻されたのですか。

新井（以下 A ）情報学です。研究室では離散数学を学び、C 言語でプログラミングなどもしていました。学生時代から情報セキュリティに興味を持っていたわけではありません。

S 興味を持つきっかけは何だったのですか。

A 私が就活生だった頃、求人倍率は 1 を下回り、戦後最低だと言われていました。多くの企業で希望する職種に採用枠がないという状況でした。

S まさに就職氷河期の真っ只中だったのですね。

A そんな中、就活のために購読していた日本経済新聞で、情報セキュリティに関する記事を読みました。インターネットの新たな側面が見え、興味を持ったのです。そこで記事に掲載されていた企業に応募し、採用されることとなりました。

S その企業というのは。

A ラックです。当時は不況の最中でしたが、会社は情報セキュリティ事業を伸展させようと意欲的でした。

S 2000 年当時、官公庁の Web サイトが次々と改ざんされる事件が発生しましたね。

A この年には九州・沖縄サミットやインパク（インターネット博覧会）も実施されました。

S 懐かしいですね。当時の森首相が IT 革命を「イット革命」と言って失笑を買っていました。

A こうしたサミットやインパクの Web サイトなどを守る目的で作られたのが SOC（セキュリティ・オペレーション・センター）で、私も立ち上げから携わることとなりました。

S 人員はどの程度でしたか。

A 6 ～ 7 名ほどです。当時は監視しているサイトの数も多くはありませんでしたから、深夜などトラフィックがない隙間時間を利用して、ソフトウェアのぜい弱性を探していました。上司からの指導もあり、主に Windows を対象としました。

S 2000 年代初頭、Windows はセキュリティが充分に考慮されておらず、数多くのぜい弱性が発見されました。マイクロソフトがセキュリティに力を入れはじめたのもこの頃からでしたね。

米国駐在時代に価値観を揺さぶられた Code Red と 9.11

A その後、米国事業所へ移動となりました。

S 場所はどちらに。

A ワシントン DC にもほど近いバージニア州ペンタゴンシティです。

S 米国の IT 産業というと、シリコンバレーなど西海岸ベイエリアをイメージするのですが、東海岸に事業所を構えた理由は何でしょうか。

A 軍関係者や学術分野の人たちとつながりを持ちたいと考えたからです。

●新井悠（あらい・ゆう）

2000 年に情報セキュリティ業界に飛び込み、株式会社ラックにて SOC 事業の立ち上げや米国事務所勤務などを経験。その後情報セキュリティの研究者として Windows や Internet Explorer といった著名なソフトウェアに数々のぜい弱性を発見する。
ネットワークワームの跳梁跋扈という時代の変化から研究対象をマルウェアへ照準を移行させ、著作や研究成果を発表した。
2013 年 8 月からトレンドマイクロ株式会社で標的型マルウェアへの対応などを担当。
2019 年 7 月、NTT データの Executive Security Analyst に就任。近年は数理モデルや機械学習を使用したセキュリティ対策の研究を行なっている。
2017 年より大阪大学非常勤講師。著書・監修・翻訳書に『サイバーセキュリティプログラミング』や『アナライジング・マルウェア』がある。経済産業省情報セキュリティ対策専門官。CISSP。

S 何名ほどの組織だったのですか。
A 組織上は 5 名ですが、責任者は日本にいますから、実質は 4 名です。米国駐在時には印象深い出来事が 2 つありました。
S それは何でしょう。
A 1 つは 2001 年 7 月に猛威を振るったインターネットワームの Code Red です。CNN など主要ニュース局で大々的に報じられました。ワームの発見者である eEye Digital Security のマーク・マイフレット氏が番組に出演して解説していました。それまで日本に住んでいて、インターネットワームがニュース番組で報じられることなどなかったので、これには驚きました。
S eEye Digital Security は、鵜飼裕司氏が 2003 年に渡米・入社した企業ですね。2007 年に帰国して FFRI を設立する以前の話です。
A 当時は米国に移り住んで間もない時期でした。スーパーマーケットの棚に並ぶ色鮮やかなドリンクボトルを目にして、日本人の感覚で「誰が飲むのだろう」といぶかしがっていたのですが、そのドリンクの名がワーム名になったことにも驚きました。
S 当時のワームやウイルスは発見者が独自に命名していましたね。
A もう 1 つの出来事が 2001 年 9 月 11 日に起きた同時多発テロです。事業所はペンタゴンシティにあり、文字通りペンタゴンの建物とは目と鼻の先の距離です。そこに旅客機が突っ込んできたのです。
S 今でこそ冷静に話せると思いますが、当時は恐ろしかったのでしょうね。
A 事件が発生したのは朝でした。オフィスで TV を観ながら動向を見守っていました。ニューヨークのツインタワーに 2 機目の旅客機が衝突するのを目の当たりにしました。報道によればハイジャックされた十数機の旅客機が今もなお行方不明とのこと。さらに、ペンタゴン近くに墜落・炎上した旅客機の黒い煙が事務所の居室内に入ってきたのです。パニックとなり体が震えるのを感じました。言葉も出ませんでした。
S 凄まじい体験です。
A その後はビジネスどころではありませんでした。アルカイダが犯行声明を出していましたから、中東アラブ系の人々はひどい差別に遭っていました。アジア系であっても攻撃される危険がありました。そんなとき、近所に住む親切な方から、その方はインド系でしたが、米国国旗を手渡されたのです。これを持っていれば、あなたは米国国民であり愛国者であると思われるはずだから、と彼は言ったのです。
S 日本に住んでいると、国家や国民を意識することはありませんから、得がたい経験ですね。
A 身の安全が脅かされたとき、人々はこんなにも変わってしまうものなのかとがく然としました。とにかく、敵か味方かに分けたかったのだと思います。
S 確かにビジネスどころではありませんね。
A その後、事業所を閉鎖して日本に帰国することとなりました。現在、コロナ禍で、空港がガランとしていますが、当時も空港に人影はありませんでした。飛行機の乗客もまばらで、ジャンボ機なのに乗客が十数名という状態でした。エコノミー中央 4 人掛けの席を横一列に使って寝そべって帰国したのを覚えています。

東日本大震災とキャリアの方向性

A 米国での体験を通じて、自分にできることは何か、を考えるようになりました。国や政府の取り組みについて、もっと知りたいと思っていたところ、JNSA の脅威を持続的に研究する WG のメンバーの方々と出会いました。また、それまではソフトウェアのぜい弱性の研究をしてきましたが、Code Red のようにぜい弱性を悪用するワームやコンピューターウイルスが勢いを増してきたこともあり、研究の軸足をぜい弱性からマルウェア解析へと移していきました。
S その成果が解説書の上梓へとつながるのですね。
A 当時は毎日のようにマルウェアを解析していて、面白い結果が出たものなどをブログなどで紹介していました。そんな中、知人からマルウェア解析の本を出すべきだと強く勧められたのです。その知人も共著者の 1 人となり、2010 年に「アナライジング・マルウェア」という解説書を上梓することができました。
S 出版物のほとんどが翻訳というオライリージャパンの中で、日本オリジナルの企画は珍しかったと記憶しています。
A この本を書き終えた翌年に東日本大震災が起こりました。今でも覚えているのですが、震災が起こった 1 週間後に「放射線量に関する情報」と題する標的型攻撃メールが流れたのです。解析すると、

APT10 による犯行の疑いが色濃く表れました。人々が困っている最中、それに乗じて悪事をする輩がいる。これを知ったとき、私は激しい怒りを感じました。その一方で、自分にできることはマルウェアの解析のみ。もっと別の形で誰かの役に立ちたいという思いが強くなりました。

ビッグデータをセキュリティに生かす

A 自らのキャリアを見つめ直し、さまざまな人に相談しました。その中で興味深かったのが、トレンドマイクロでした。ウイルス対策ソフトやベンダーの仕事に興味を持ちました。移籍したのは 2013 年のことです。当時、ほとんどの PC にはウイルス対策ソフトがインストールされている状況で、ベンダーには日々膨大な情報が集まってきました。まさにビッグデータの世界です。それまでは検体を 1 つずつ見ていましたから、大量のデータを目の前にしてどのように解析を進めていけばよいか、当初は悩みました。

S 深く掘り下げていたところ、新たに量も求められるようになったということですね。

A ただ、この頃にはコードを積極的に書くようになっていましたから、すぐに機械学習を使いデータをうまく処理できるようになりました。そして社内でこの技術を広めていきました。一概には言えませんが、セキュリティ業界内であってもプログラムを書かない人が少なからずいます。ツールをつなぎあわせたり、シェルスクリプトを上手に組み合わせたりしています。私自身もプログラムを書くのは面倒だと思っています。バグも出ますし、メンテナンスも必要ですから。

S 業界の方のバックグラウンドもさまざまですから、プログラムを書かない人がいるのも納得です。

A 自分が知っていることを他の人にやってもらったり、覚えてもらったりするのに、プログラムを書くことは有効で、普遍的に教えられる手段だと思っています。

新たな時代のエンジニアを育成する

S 教育に関心を持ちはじめたのもこの頃からですか。

A 米国から戻りマルウェア解析をはじめた頃から人材育成に関心はありました。ただ、リバースエンジニアリングなどは経験や勘に左右される要素もありますから、簡単ではないとも承知していました。

S 昨年、セキュリティキャンプで講師を務められました。

A 実のところ、講師の依頼は過去に何度もいただいていて、その度にお断りしてきました。ですが、昨年、根負けしてついに引き受けることとなったのです。

S 断ってきた理由は何でしょう。

A 私以上にセキュリティに通じており、かつ熱意を持った方がたくさんいらっしゃるので、出る幕ではないだろうと思っていたのです。ですが、引き受けてみると自分自身にも得るものが多かったと感じています。面白かったのは、講義を受ける生徒よりも見学に来た人数の方がはるかに多かったことです。

S 企業の方が見学に来られることも多いですね。有名エンジニアの講義が聴けることもスポンサー・メリットの 1 つになっているのだと思います。

A セキュリティキャンプはいわばスキルの頂点をめざすトップ人材を育成する場です。もちろん、これは大切なことです。ですが、1 日に数万、年にすれば数億ものマルウェアが新たに生み出されているという現状もあります。これらの検体を処理できる人材、つまり実務をスマートにこなせる人材の育成も重要だと考えています。

S おっしゃるとおりです。大学での講義もその一環ですか。

A 大阪大学で学部生向けに Python を使った機械学習を教えています。コロナ禍以前から遠隔からも受講可能な授業となっています。東北大学・慶應義塾大学など複数の大学にも配信されています。

S 文部科学省が高度 IT 人材の育成を目的とした enPiT※1 ですね。

A 2015 年に JAIST（北陸先端科学技術大学院大学）で教壇に立ったのがきっかけでした。その後、JAIST の先生が大阪大学に異動になり、私の授業も異動することとなりました。

S 教育機関の方々と話をすると、セキュリティを教えるには大学院生になってからの方がよいと聞きま

※ 1 **enPIT**　http://www.enpit.jp/

すが、学部生向けのコースはいかがでしょうか。
A セキュリティを学ぶには基礎となるコンピューターサイエンスの知識が不可欠ですから、大学院生の方が望ましいのは確かです。授業では元々大学院生向けだった教材を手直しして使っています。難しくならないように、数式などもあまり使わないようにして、コードを書けばできるという形にしています。授業は興味を持つきっかけくらいで良いと考えています。ステップアップは各自で勉強すればいいわけですから。

新たな挑戦が原動力に

S NTT データに移籍された経緯は。
A きっかけは新しいことにチャレンジしてみたかったからです。日々、マルウェアの解析を続けてきたのですが、このままでいいのか、と疑問に感じていました。そこで、何かを変えたくて IDA Pro をアンインストールして、機械学習用の Anaconda という環境を導入しました。
S 勇気のいる決断でしたね。
A 自分が楽しいと思うことは何か、常に考えるようにしています。これまではぜい弱性探しだったり、マルウェア解析だったりしたわけですが、それが機械学習へと変化したのだと思います。結局、新しいことに挑戦するのが、自分にとって大切なのだと感じました。
S 新たな挑戦が原動力になっているハッカーは多いです。
A それからというもの、1 日中 GPU フル稼働でファンを〝シュワンシュワン〟させながら計算するのが日常になりました。そういうことを続けているうちに、機械学習には不可欠のデータセットに関心が移ってきました。また、情報セキュリティ以外のシステムがどのように動いているのか、もう一度学んでおく必要があるとも感じるようになりました。そのような時期に NTT データから誘いがあったのです。
S NTT データでの仕事内容は。
A 大きく 3 つあります。1 つは今回のインタビューのようなメディア対応。あとは執筆やエバンジェリストのような活動です。2 つ目は人材育成です。NTT データの CIRT メンバーを対象としています。人事異動によって組織の能力を下げてしまうことは許されません。そして、3 つ目がインシデント対応です。実際のところ、私が手を動かすわけではなく、指揮を担当しています。

CODE BLUE のレビューボード

S CODE BLUE のレビューボードを務められています。
A 代表の篠田佳奈さんの熱意に押されて引き受けました。
S ここ数年、CFP（Call for Papers：講演者募集）の数も格段に増えたと聞いています。
A ここ 2 ～ 3 年の応募総数は 300 ～ 400 ほどになっています。
S 増えた要因は何でしょう。
A あくまで個人の意見ですが 2 つあると考えています。1 つはこれまでの実績です。篠田佳奈さんは海外カンファレンスへ頻繁に足を運び、現地のコミュニティと積極的に交流しています。また、CODE BLUE カンファレンス自体も回を重ねて、広く認知されるようになりました。これらの積み重ねによって講演者や参加者が集まってきたのだと思います。
S なるほど。
A もう 1 つは、ジェネラル（一般）のセッションを設けたことです。専門家受けが良い最先端の技術情報でなくてもオーケーとしてハードルを下げたのです。私はこれに関して慎重派でしたが、蓋を開けてみれば、数多くの講演者・参加者が集まりました。もはやセキュリティは専門家だけの問題ではなくなったのでしょう。それこそ、私が Code Red 感染拡大のニュースを米国の CNN で観たように、日本でもセキュリティの話題が当たり前になっているのだと思います。
S 企業に対するサイバー攻撃が全国紙の一面を飾ることも珍しくなくなりました。
A ジェネラル・セッションも含め、全体の応募数が増えましたから、ペーパーを審査するレビューボードの負担も増すこととなりました。コロナ禍の影響で 2020 年はオンラインでの開催となりました。今までの形とは異なりますが、対応できる土壌はできていると思います。
S ジェネラル以外ではどのようなテーマが増えましたか。
A 機械学習に関するものは大幅に増えました。し

かし、この分野には多くの研究者がおり、大抵のことはやり尽くされているので、新規性に富むものはほとんどありません。そのようなペーパーは審査でバッサリと切っています。

S CODE BLUE では新井さんご自身も短時間のプレゼンテーションをされました。

A オープンソースのツールを発表する Blue box というコーナーで発表を行ないました。ダークウェブで違法物品を取引するサイトをラベリングしたデータセットがテーマです。このデータセットは GitHub で公開しています※ 2。

S どのように役立つのでしょう。

A 機械学習を使った対策開発に貢献します。違法物品を扱うサイトの早期発見の一手段となり得るので、法執行機関などには有効です。

S ダウンロード数はどれくらいですか。

A 公開当初に 100 ～ 200 程度のアクセスがありました。このデータセットは定期的にメンテナンスする必要がありますから、また別の機会に発表したいと考えています。

S メンテナンスが必要な理由は何でしょう。

A 違法物品を扱うサイトを例に考えると、データセットを作成した時点では最新であっても、時間の経過によって変化が生じます。具体的には従来のサイトが消滅したり、新たなサイトが出現したりという具合です。こういった変化によって機械学習モデルの予測精度が劣化してしまうのです。コンセプトドリフトと呼ばれ機械学習モデルの課題の 1 つです。

S なるほど。

A データセットが過去のものであっても、継続的にデータセットを更新しなくても精度を維持できるモデルを作るのが次のテーマです。他にも研究テーマのヒントはいろいろとあるのですが、時間が足りない状況です。

ウィズ・コロナ時代のサイバーセキュリティ

S ウィズ・コロナ時代のサイバー・セキュリティはどのようになると考えますか。

A コロナ禍で企業はテレワークを実施しています。一般的なセキュリティ対策で言えば、SaaS を積極的に導入することです。やはり手元の端末でアプリケーションを動かすことがリスクになります。ファイルのダウンロード・実行をやめる、これだけでも大きく変わるはずです。

S 組織の規模に関わらずできる対策ですね。

A テレワークの導入で会社と家の区別、つまりネットワークの境界があいまいになってきます。その中でセキュリティをどのように担保していくか、まさにゼロトラストネットワークの世界になってきます。

S 最近、注目されるキーワードですね。

A 先ほども言ったとおり、SaaS を積極的に利用しますから、セキュリティ対策も必然的にクラウド側になります。ですが、クラウドはある種のブラックボックスです。当然ログは端末側ではなくクラウド側に残り、その量も膨大になります。

S おっしゃるとおりです。

A セキュリティエンジニアにこれから求められるのは、膨大なログを効率よく処理して、怪しい通信を見つける技術力です。クラウド対応の SIEM（Security Information and Event Management）も提供されていますが、ベンダー任せにはせず、検出結果からその原因を推測できる勘を養うことも大切だと思います。言い方を変えれば、攻撃者の視点を持つということです。

S なるほど。

A このことは NTT データに移籍して、より強く感じるようになりました。今回のコロナ騒動がきっかけとなり、取引先企業のクラウドへの移行に拍車がかかっています。そうなると監視するべきポイントがクラウドに移ります。多くの組織が自前で SIEM フレームワークを用意してログを管理するようになりました。

※ 2 **DDIR** https://github.com/nenaiko-dareda/DDIR

サイバー犯罪でもギグワーク !?

S サイバー犯罪に傾向の変化などはありますか。

A ランサムウェアで稼いでいるグループに変化があります。コロナ禍の影響で医療機関を攻撃対象にしないグループが現れた一方で、引き続き医療機関も攻撃するグループもいます。

S 医療機関を攻撃しないグループは自らの良心の呵責に耐えかねたのかもしれませんが、犯行は続けていますから、全く共感できません。

A サイバー犯罪者グループも、各自が在宅で攻撃をするような状況になっています。一昔前ならば、犯罪者グループの拠点に当局の強制捜査が入ってテイクダウン（制圧）というケースもありましたが、現在ではそれもできません。

S 都市がロックダウンしても犯罪者は攻撃を続けているのですね。

A 彼らがどのように活動しているかというと、アンダーグラウンドコミュニティで仲間を募集しているのです。

S 情報交換に使うのはダークウェブですか。

A ダークウェブは違法薬物目的の人たちが 9 割以上です。多くの犯罪者はメンバー制のロシアのアンダーグラウンドサイトを利用しています。興味深いのはその募集が役割ごとに細分化している点です。

S 役割とは。

A 例えば、ランサムウェアをばらまく人、すでに企業などの組織に侵入しておりバックドアを持っている人、企業と交渉を行なう人などです。連絡手段には匿名性の高いメッセージングアプリの Telegram が使われています。

S 働き方が多様化する中、プロジェクトごとに人が集まって仕事を進めるギグワークが注目されていますが、犯罪者の世界でもギグワークが進んでいるのですね。

A 従来のビジネスはマルウェアを作り、それを売るという形でした。ですが、現在はその場で即席チームを作り、攻撃して、身代金をせしめる成功報酬型になりました。また、犯罪者が狙うターゲットも変化しています。これまでのランサムウェアは個人をターゲットにしており、身代金も 1 件につき 200 ドル程度でした。ところが、最近話題になった米国の大手法律事務所の事例では 4200 万ドルもの身代金が要求され、支払いに応じなければ、大量の個人情報を暴露すると脅迫しています。

S 個人情報にはレディーガガ、マドンナといったセレブをはじめトランプ大統領の名も挙がっていました。

A 今後はこういう犯罪者グループと立ち向かわなくてはならなくなります。セキュリティ対策としては、パッチなどの修正プログラムを迅速に適用すること、エンドポイントのセキュリティ製品を使うなど、基本的なことを地道に続けるほかないと思います。

今後の目標

S 今後の目標などありますか。

A 現在、本の執筆をしています。セキュリティの分野で機械学習をどのように生かすかがテーマになっています。例えば、スパムやマルウェアの検知から、敵対的機械学習と呼ばれる AI をあざむくための機械学習なども取り上げるつもりです。

S 執筆はお 1 人ですか。

A 26 ～ 27 歳の共著者と共に作業を進めているのですが、大いに刺激を受けて自分自身も成長しているように感じます。知らないことを積極的に学んでいきたいという欲求を自分の中に持ち続けています。私自身のキャリアを振り返ると、セキュリティを主軸として専門性を高め、機械学習の分野が 2 本目の柱となりました。できれば、あと 2 ～ 3 本の柱を立てたいと考えています。

S 具体的な構想はありますか。

A 現時点ではありませんが、全く違う分野かもしれません。あるとき突然、財務の勉強などをはじめるかも（笑）。

S わかりました。本日はありがとうございました。

国際カンファレンスから草の根勉強会、さらには CTF 形式のハンズオン教材まで

自宅でできる情報セキュリティ・スキルアップ法

文＝斉藤健一

新型コロナ禍によりイベントの開催はリアルからオンラインへ

中国武漢市に端を発する新型コロナウイルス感染症（COVID－19）は、世界中を巻き込んだ歴史的な凶禍となった。2020 年 7 月中旬の段階での全世界の感染者は 1300 万人を超え、死者も 58 万人に上るという痛ましい事態となり、その勢いはいまだ衰えを知らない。

日本においても、TV・新聞等のマスコミが連日、国内の新規感染者数を報道する。5 月末の緊急事態宣言の解除後には、いったん沈静化すると見られていた事態だが、7 月に入ると首都圏を中心に再び新規感染者数が急増し、第 2 波を懸念する声が高まっている。

政府は新型コロナウイルス感染拡大を防ぐため、3 密（密閉・密集・密接）を避ける「新しい生活様式」の提言を行なった。ビジネスではテレワークや時差通勤の実施などを要請し、イベントの開催においても参加人数の制限や予防対策措置の徹底を求めている。

これに伴い、IT 分野に限らず、国際的なカンファレンスからユーザーグループ主催の小規模な勉強会にいたるまで、多くのイベントが開催の中止や延期、もしくはオンライン開催への移行を余儀なくされた。

オンライン開催イベントのメリット

しかしながら、不都合なことばかりではない。オンライン開催イベントには距離という制約から解放されるメリットがある。つまり、自宅にいながらにしてどんなイベントにも参加できるということだ。海外カンファレンスの場合、時差という制約は残るものの、渡航費用が不要になるというメリットは大きい。さらに、これまでは有料だったものがオンライン開催では無料になるケースもある。

そこで今回はオンライン開催イベントを紹介したい。セキュリティ業界内で知名度のある国内外のカンファレンスやシンポジウムなどの動向を調べてみた。また、草の根勉強会などを探すための情報源、さらに、実際に手を動かすハンズオン教材の情報などもあわせて紹介する。

国内外の代表的イベントの動向

ここでは主にオンラインに移行したイベントの概略を開催順にお伝えする。各イベントの詳細ついては次ページの表 1 を参照していただきたい。なお、P12 の表 2 では開催の中止・延期を決めたものや未定のものなどをまとめているので、あわせてご覧いただきたい。

・HITB（Hack In The Box）SINGAPORE 2020

15 年以上の歴史を持つセキュリティ・イベント。ここ数年はシンガポールとオランダで開催されてきた。トレーニングとカンファレンスで構成されている。今年はオランダでの開催が中止となり、シンガポールでのイベントはオンラインへと移行した。期間は 7 月 20 日～ 26 日（シンガポール時間）。25 日～ 26 日に行なわれるカンファレンスは HITB Lockdown と銘打ち、ストリーミング配信を無料で視聴することができる。

表 1 2020 年 国内外の有名カンファレンスの開催動向

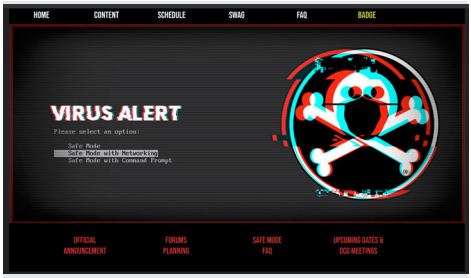
カンファレンス名 URL	開催方法	日程	費用
HITB SINGAPORE 2020 https://conference.hitb.org/	オンライン	7 月 20 日 ~26 日 （GMT +8:00）	1899 ドル～（トレーニング）、無料（トークス）
BlackHat USA 2020 https://www.blackhat.com/us-20/	オンライン	8 月 1 日～ 6 日 （GMT - 8:00）	3100 ドル～（トレーニング）、995 ドル～（ブリーフィング）
DEFCON safe mode https://www.defcon.org/html/defcon-safemode/dc-safemode-index.html	オンライン	8 月 7 日～ 9 日 （GMT - 8:00）	無料
第 24 回 サイバー犯罪に関する白浜シンポジウム http://www.riis.or.jp/symposium24/	オンライン	8 月 27 日～ 28 日	1 万 5000 円（チケット購入締め切り：7 月末日）
HITCON 2020 https://hacker.org.tw/index.html	オンサイト・ オンライン併催	9 月 11 日～ 12 日 （GMT+8:00）	700 ～ 1500 台湾ドル（オンライン）オンサイトの料金は Web サイトを参照
サイバーセキュリティシンポジウム道後 2020 https://www.sec-dogo.jp/	オンライン	9 月 17 日～ 18 日	2 月開催のシンポジウムに参加申し込みを行なった人が対象。追加の募集については後日発表予定
BlackHat Asia 2020 https://www.blackhat.com/asia-20/	オンライン	9 月 29 日～ 10 月 2 日 （GMT+8:00）	3000 ドル～（トレーニング）、750 ドル～（ブリーフィング）
コンピュータセキュリティシンポジウム 2020 https://www.iwsec.org/css/	オンライン	10 月 26 日～ 29 日	無料～ 1 万 9000 円（会員種別・登録時期により異なる）詳細は Web サイトを参照
CODE BLUE 2020 https://archive.codeblue.jp/2020/	オンライン	10 月 29 日～ 30 日	無料

• BlackHat USA 2020

米国ラスベガスで毎年夏に開催されるセキュリティ・カンファレンスで、DEFCON と共に業界内での知名度は高い。23 回目を迎える本年はオンラインでの開催となった。開催期間は 8 月 1 日～ 6 日（太平洋標準時）で、トレーニングとブリーフィングが行なわれる。費用は前者が 3100 ドルからと例年並みだが、後者は通常時開催の約半額となる 995 ドルからとなっている。また、スポンサーのセッションやオープンソース・ツールを紹介するコーナーも従来通り行なわれる。なお、基調講演は「民主主義のストレステスト：世界的パンデミック下での選挙の完全性」や「世論ハッキング」といった時勢を反映したものとなっている。なお、9 月末から 10 月上旬にかけて、Black Hat Asia 2020 も開催される予定だ。

• DEFCON Safe Mode

前述の Black Hat がビジネス寄りなのに対し、コミュニティ色が強いのが DEFCON だ。参加費も BlackHat に比べてはるかに安価なため、例年、世界各地から多くの人が集まっていたが、本年は無料のオンライン開催という大英断を下した。Safe Mode と銘打たれ、マスクをつけた DEFCON キャラクターと VIRUS ALERT という文字が印象的なデザインとなっている。開催は 8 月 7 日～ 9 日。あらかじめ収録されたプレゼンテーション動画が開催期間中に公開され、タイムテーブルにあわせて質疑応答の時間が設けられる。また、DEFCON CTF をはじめとする各種コンテストもオンラインで開催される予定だ。



DEFCON Safe Mode の Web ページ

• 第 24 回 サイバー犯罪に関する白浜シンポジウム

例年、5 月に行なわれているシンポジウムが新型コロナ禍の影響で、時期を移しオンラインでの開催となった。開催は 8 月 27 日～ 28 日。「ＡＩはサイバーセキュリティの夢を見るか？」をテーマに、各界のサイバーセキュリティ関係者がそれ

表 2 その他のカンファレンス・シンポジウムの動向

カンファレンス名 URL	動向	備考
eCrime 2020 EU https://apwg.eu/	延期	当初は 4 月開催予定だったが、調整後の日程は公式サイトで発表予定
サイバー防衛シンポジウム熱海 http://5th-battlefield.com/	延期	当初は 6 月開催予定だったが、新型コロナ禍の影響により延期。調整後の日程は公式サイトで発表予定
BSides Tokyo 2020 https://bsides.tokyo/	開催（?）	公式サイトで　は 11 月 1 日に渋谷で開催される旨が記されている。詳細は不明
情報セキュリティワークショップ in 越後湯沢 http://www.anisec.jp/yuzawa/	不明	7 月中旬時点で公式サイトでのアナウンスは行なわれていない
AV Tokyo http://ja.avtokyo.org/	不明	7 月中旬時点で公式サイトでのアナウンスは行なわれていない
PacSec https://x.com/pacsecjp	オンライン	公式サイトでは 11 月 1 日～ 6 日にオンラインで開催される旨が記されている。詳細は不明

ぞれの研究成果や事例を持ち寄り議論が進められる。昼間の講演に加えて、夜間に車座が開かれるのが大きな特徴。車座とは講師・参加者の区別なく自由闊達に議論できる場のこと。オンライン開催でも BOF として開催予定だそうだ。なお、例年併催されている情報危機管理コンテスト決勝戦は 5 月末に開催済み。中継動画が公開されており、コンテストの Web ページから視聴することができる。※ 1

・HITCON 2020

台湾のセキュリティ・コミュニティのメンバーが中心となり立ちあげた国際カンファレンス。例年、CMT（8 月）と PACIFIC（12 月）に開催していたものを、本年は 1 つに統合した。開催は 9 月 11 日～ 12 日。当初はオンラインでの開催を予定していたそうだが、政府の迅速な初動対応で新型コロナウイルスの封じ込めに成功したことにより、国内参加者向けにオンサイト（会場に参加者を収容する従来の形式）での開催も決定したという。CFP（論文募集）の締め切りが 7 月末ということで、プレゼンテーションのラインナップなどは今後公開される予定だ。

・サイバーセキュリティシンポジウム道後 2020

例年、2 月に行なわれるシンポジウムが新型コロナ禍の影響で、時期を移しオンラインでの開催となった。開催は 9 月 17 日～ 18 日。当初は「東京オリンピック・パラリンピックとその後を見据えたサイバーセキュリティ」というテーマであったが、開催日の変更に伴い全面的にプログラムを見直すという。2 月開催のチケットを購入した人が参加できるが、追加募集も後日行なわれるという。

・コンピュータセキュリティシンポジウム 2020

情報処理学会コンピューターセキュリティ研究会が主催する学術シンポジウム、通称 CSS。コンピューターセキュリティの基礎となる理論や技術から応用事例、管理運用、心理学、社会科学的考察まで幅広い領域を対象としている。マルウェア解析技術を競う MWS Cup などが併催されることでも有名だ。本年は 10 月 26 日～ 29 日にオンラインで開催される。

・CODE BLUE 2020

例年、秋に開催されてきた国際的なサイバーセキュリティカンファレンス。今年は 10 月 29 日～ 30 日にオンラインで開催される。無料で参加できることが発表されており、大きな注目を集めている。CFP の締め切りは 8 月 15 日。

情報セキュリティ系勉強会の現状は？

2000 年代中盤より数々の情報セキュリティ系勉強会（以下勉強会）が開催されてきたが、新型コロナ禍でどのような影響があったのだろうか。その状況を簡単に調べてみた。勉強会や各サービスの情報は次ページの表 3 にまとめたので、あわ

※ 1 **第 15 回情報危機管理コンテスト** http://www.riis.or.jp/symposium24/crisismanagement/final/

表 3 IT 勉強会関連情報とイベント支援サービス

サイト・サービス名 URL	概要
情報セキュリティ勉強会ポータル https://sites.google.com/site/securityworkshop/	情報セキュリティ系勉強会をまとめたページ。リンク先は各勉強会のアーカイブになっており、開催状況などを調べることができる
Connpass https://connpass.com/	システム開発企業が運営。勉強会・セミナーに使用したプレゼンテーション資料をアーカイブ機能などを提供している
Doorkeeper https://www.doorkeeper.jp/	IT 系が中心の支援サービス。コミュニティの運営に注力している印象。有料イベントの支払いにも対応している
TECH PLAY https://techplay.jp/	運営母体は人材派遣・紹介の関連企業。勉強会・セミナーの情報の他、自社からも積極的に情報を発信している
こくちーずプロ https://www.kokuchpro.com/	IT 系に限らず幅広いジャンルに対応。SEO による集客など主催者側へのサービスを前面に押し出している
Peatix https://peatix.com/	さまざまな規模、幅広いジャンルのイベントを扱う支援サービス。チケット販売やイベント運営サポートも充実している

せてご覧いただきたい。

勉強会の情報は、「情報セキュリティ系勉強会ポータルサイト」を参考にした。話はそれるが、ここ数年、勉強会の主催者の間には萎縮ムードが漂っていた。2018 年に明るみに出た Wizard Bibble 事件※ 2 や、2019 年のアラートループ事件※ 3 での警察当局の対応から、勉強会の内容が不正指令電磁的記録に関する罪（通称ウイルス作成罪）に抵触するのではないかという不安が広がったのだ。ここに新型コロナウイルス感染拡大の脅威が加わることとなった。

2020 年、従来の勉強会がいくつか開催されていたが、新型コロナ禍による緊急事態宣言後はオンラインへと移行した。オンライン勉強会を開催したコミュニティには「北海道情報セキュリティ勉強会」、「総関西サイバーセキュリティ LT 大会」、「OWASP Sendai」、「OWASP Japan」、「#ssmjp」、「Security-JAWS」があった。

現在、オンライン勉強会を主催するノウハウがネットを通じて広がっているので、今後の開催は増えていくと思われる。

勉強会やイベントを探すには

勉強会やイベントを探す最も手軽な方法は、イベント支援サイトを利用することだ。以前は有志が管理する勉強会カレンダーもあったが、勉強会の増加により、更新作業に負荷がかかったり、必要な情報が見つけにくくなったりしたことから、現在では休止、もしくは休止に近い状態のものばかりとなった。

イベント支援サイトの代表的なものとしては、**「Connpass」、「Doorkeeper」、「TECH PLAY」、「こくちーずプロ」「Peatix」**があり、それぞれが特長を持つ。

「Connpass」と「Doorkeeper」は、IT 技術系を対象としている。勉強会の他、主催するコミュニティも探せるので、興味ある分野をチェックすることをお勧めしたい。

「TECH PLAY」も IT 技術系を対象としている。東京・渋谷にイベントスペースを持ち、自社からも積極的に情報を発信しているのが特長だ。

「こくちーずプロ」と「Peatix」は、幅広いジャンルの意ベントを扱う。IT 系の勉強会やイベントを探すという意味では補助的な存在になるが、他のサイトには登録されていないものを見つけることができる。

もちろん、勉強会やイベントを探す方法は他にもある。支援サイトに次ぐものとしては Facebook や Twitter など SNS での検索だろう。

Facebook には、同じ興味を持つ人が集まり交流する「グループ」機能がある。検索できるのは、誰もが参加できる公開グループと、参加に管理者の承認が必要な非公開グループだ（検索でヒットしない秘密グループもある）。記事では具体的なグループについて言及することはしない

※ 2 **Wizard Bibble 事件** https://ja.wikipedia.org/wiki/Wizard_Bible%E4%BA%8B%E4%BB%B6

※ 3 **アラートループ事件**
https://ja.wikipedia.org/wiki/%E3%82%A2%E3%83%A9%E3%83%BC%E3%83%88%E3%83%AB%E3%83%BC%E3%83%97%E4%BA%8B%E4%BB%B6

表 4 CTF 形式のハンズオン教材

サイト名 URL	概要
Hack The Box https://www.hackthebox.eu/	ペネトレーションテストやサイバーセキュリティのスキルを磨くためのオンラインプラットフォーム。ユーザー登録の時点からハックが始まるのがユニーク
SANS Holiday Hack Challenge https://holidayhackchallenge.com/	米国 SANS が提供。2019 年のチャレンジは RPG をプレイする形式で進める。Web では過去のチャレンジもアーカイブされている
picoCTF https://picoctf.com/	カーネギーメロン大学が中高生向けの CTF 大会を主催、その問題が公開されている。リバースエンジニアリング、暗号解読など豊富な課題が用意されている
MNCTF http://mnctf.info/	マクニカネットワークス社が提供、問題文が日本語となっている。暗号・フォレンジック・マルウェア・ネットワークなどのジュアンから出題されいる

が、情報セキュリティ系で定期的に勉強会（オンライン含む）を開催しているグループもあるので、Facebook ユーザーで気になる方は是非ともチェックしていただきたい。

また、企業が開催するセミナーを探すには Twitter が適している。「ウェビナー（Webinar）」＋「セキュリティ」といったキーワードで簡単に見つけることができるはずだ。

公開されているハンズオン教材にチャレンジ

最後に実際にチャレンジできるハンズオン教材を紹介しよう（表 4）。カンファレンスや勉強会に参加する他に実際に自分の手を動かすこともスキル磨きには効果的だ。

ここではほよたか（@takahoyo）さんの「おうちで出来るセキュリティチャレンジ / cyber security challenge from home」※ 4 を使わせていただく。スライドでは**「Hack The Box」、「Hack The Box」、「SANS Holiday Hack Challenge」、「picoCTF」、「MNCTF」**が紹介されており、ほよたかさんの Twitter ではそれぞれについてコメントしている※ 5。

多くの教材は CTF 大会などのイベントで使われた素材が一般向けに公開されたものだ。WriteUp（他のユーザーが書いた解法）があるものも多いので、つまづいたら参考にしてみるといいだろう。

現実の世界において、「3 密」は避けなくてはならないが、オンライン・イベントに参加したり、教材に挑戦したりすれば、自宅にいながら「濃密」な時間を過ごすことができるはずだ。みなさんも是非とも試してみてほしい。

※ 4 **おうちで出来るセキュリティチャレンジ** https://speakerdeck.com/takahoyo/cyber-security-challenge-from-home
※ 5 **ほよたかさんのコメント** https://twitter.com/takahoyo/status/1254350860961767425

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.38

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