HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.43

株式会社 日立システムズ

Human * IT

Hitachi Systems security Jounral VOL.43

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

本誌読者の方であれば、日々の情報収集の過程で、サイバー犯罪やサイバー攻撃に関する数々のニュースに触れているはずだ。また、近年、その事案が増加していることにも気づいているだろう。その背景には、犯罪集団による営利目的の攻撃の急増や、国家の支援を受けた攻撃主体の台頭などが挙げられる。

世界情勢が大きく変化する中で、サイバーセキュリティについての理解を深めるには、技術だけではなく、国際政治・経済・安全保障といった分野の知識も必要となる。

今回、インタビューに登場いただくのは、慶應義塾大学の土屋大洋教授だ。国際政治の視点からサイバーセキュリティを研究しており、昨年末には「サイバーグレートゲーム」を上梓された。書名のとおり、サイバー空間における大国同士の覇権争いの実相に迫る一作となっている。

この「グレートゲーム」を軸にしてサイバーセキュリティの世界を見直してみると、それまでは個別の点として認識していた事案同士につながりが見え、線として捉えられるようになる。

インタビューが行なわれたのは本年６月上旬だが、その後も米中関係は悪化の一途をたどっている。こうした時代だからこそ、視点の軸となるものを養っていきたい。

取材・撮影・文＝斉藤健一

米中の対立と警視庁によるアトリビューション

斉藤（以下 S）：本誌では主にエンジニアを読者対象に誌面作りをしています。ですが、現在のサイバーセキュリティには、技術だけではなく、国際政治・経済・安全保障など、さまざまな要素が影響を与えています。そこで、今回は国際政治の視点からサイバーセキュリティを研究されている土屋先生に話を伺いたいと思います。

早速ですが、本年 4 月に菅総理大臣が渡米し、バイデン大統領との首脳会談を行ないました。会談後の共同声明では、「台湾海峡の平和と安定」について言及されています。実に数十年ぶりのこととあって注目が集まりました。また、5 月には先進 7 カ国（G7）外相会合が行なわれましたが、こちらでも中国をけん制する内容が共同声明に盛り込まれています。

一方、国内に目を向けると、4 月には警察庁が中国の攻撃者グループ “Tick” に協力した中国人（当時は留学生）を書類送検すると発表しました。Tick は JAXA（宇宙航空研究開発機構）などへサイバー攻撃を行なったとされ、中国人民解放軍とのつながりも指摘されています。

ただ、一連の攻撃が行なわれたのは 2016 年のことです。警察庁はなぜ、今、このタイミングで発表に踏み切ったのか疑問に感じています。ともすれば、日米同盟を忖度（そんたく）した結果なのかとも思えてしまいます。先生はどのようにお考えですか。

土屋（以下 T）：まず、警察庁の話をします。私自身もメンバーだったのですが「サイバーセキュリティ政策会議」という懇談会があります。警察庁のサイバーセキュリティ・情報化審議官が私的に主催しているもので、法学・技術系学者、弁護士、IT ベンダー、JC3（日本サイバー犯罪対策センター）などからさまざまな分野の識者が集まり、サイバー脅威への対処を検討しています。

令和 2 年度は昨年 10 月から本年 3 月まで 5 回開催されており、Web サイトでは発言の要旨や報告書などが公開されています※1。

●土屋大洋（つちや・もとひろ）

慶應義塾大学大学院政策・メディア研究科兼総合政策学部教授、博士（政策・メディア）1970 年生まれ。1994 年慶應義塾大学法学部卒業。1996 年同大学大学院法学研究科政治学専攻修士課程修了、1999 年同大学大学院政策・メディア研究科後期博士課程修了。国際大学グローバル・コミュニケーション・センター（GLOCOM）主任研究員などを経て、2011 年から現職。慶應義塾大学グローバルリサーチインスティテュート（KGRI）副所長。GLOCOM 上席客員研究員、国際社会経済研究所客員研究員を兼任。

この会議の中で、私はアトリビューション（攻撃主体の特定）体制の強化を提言しました。これまで警察はアトリビューションに積極的とは言えませんでした。というのも、攻撃主体を特定したとしても、外国からの攻撃の場合、その国の法執行機関から協力が得られないことも多いからです。

しかし、アトリビューションは攻撃の抑制につながります。警察庁の考え方もこのように変わってきたのです。これが、先ほどの Tick 協力者の書類送検へとつながっています。日本が独自にアトリビューションした初の事例です。その意味ではとても興味深いと思います。

S なるほど。書類送検にはそういった背景があったのですね。

T 次に米中台の関係ですが、こちらは、2016 年 12 月、選挙に勝利したトランプ次期大統領（当時）が台湾・蔡英文総督からの祝意の電話に対応したことが大きな転換点だったと思います。というの

※1 **サイバーセキュリティ政策会議**　https://www.npa.go.jp/bureau/cyber/what-we-do/csmeeting.html

も、米国は台湾との国交がありませんから、対応すれば中国からの反発は必至の状況でした。

この時のトランプ氏の考えは知るよしもありませんが、米中関係において台湾が重要なカードになることは認識したと思います。

その後、中国との関係が悪化していく中で、米国は台湾を重視するようになりました。新型コロナ禍の 2020 年 8 月には米国の厚生長官が台湾を訪問し、蔡英文総統と会談を行なっています。

ここ数十年で最上位の閣僚を台湾に派遣したわけです。そして、2021 年にバイデン政権が誕生しました。民主党政権はこれまで中国に対して比較的寛容な態度を取ってきましたから、バイデン政権も同様のスタンスを取ることが予想されていました。ところが、フタを開けてみればトランプ政権時代の政策を維持・強化する方向へと進んだのです。

S 米国にとって中国は重要な貿易相手国でもあります。中国に制裁を科すことは米国にとっても経済的な打撃となるはずです。それでも中国に対して強硬な姿勢を貫くことにはどのような理由があるのでしょうか。

T 端的に言えば、ワシントン DC の中で対中国の認識が本質的に変化したのだと思います。もちろん、急にそうなったというわけではなく、徐々にコンセンサスが形成されたのだと思います。

2015 年の発売当時、日本でもベストセラーになった「China 2049」という書籍があります。2049 年は中国が建国 100 年を迎える年であり、中国はこの年までに米国を出し抜き、世界覇権を握るために策略をめぐらせている、というのがその内容です。著者は元 CIA の中国担当アナリストであり「中国は信頼に値する国家ではない」、「中国はわれわれが期待する民主化への道を進むことはない」と警鐘を鳴らしています。

現在の状況を見ると、これは明らかなことだと思いますが、当時のワシントン DC の中には疑念を抱く人たちがいました。ですが、その後サイバー空間での中国の画策が次々に明らかになるなど、中国の本質が見えてきたのです。

この認識は欧州にも波及しています。ウェビナーなどで欧州の研究者らと議論するのですが、新疆ウイグル自治区の弾圧などは、人権侵害に敏感な彼らの神経を逆なでしています。こうした認識がサイバーセキュリティの分野にも反映されているのだと思います。

サイバーグレートゲーム
: 政治・経済・技術とデータをめぐる地政学

不安定なグローバル・ガバナンス、サプライチェーン・リスク、選挙介入とフェイク・ニュース…　日本が直面しようとしている新たな「グレートゲーム」の実相に迫る。
土屋大洋・著／千倉書房・刊／ 3740 円（税込）

「サイバー戦争」というキーワード

S 引き続き「サイバー戦争」という言葉について伺います。さまざまな立場の人がこの言葉を使っていますが、その意味合いは千差万別です。「受験戦争」や「交通戦争」と同様の比喩表現として「サイバー戦争」が使われることもあれば、国際法上の戦争の定義にのっとり「サイバー戦争は起きていない」という人たちもいます。一方で、戦争の行為自体がこれまでと比べて大きく変化していることから、これを「見えない戦争」と呼ぶ人たちもいます。

サイバーセキュリティをめぐる報道や議論に接する上で、この「戦争」というキーワードへの理解は深めておいた方がよいと思うのですが、先生の意見をお聞かせください。

T「戦争」は国際法上禁止されている行為です。仮に行なうとしても「宣戦布告」が必要など国際法上のルールが存在します。また「サイバー攻撃」

というときの「攻撃」も国際法上は、物理的な破壊を伴うものや、人命に危害が及ぶものなどを指します。ですから、ランサムウェアやシステムからの情報窃取などは、国際法上では攻撃とは言えませんし、武力の行使でもありません。その意味でいえば、メディアで使われる「サイバー攻撃」も国際法上は「攻撃」ではないのです。ほとんどは「犯罪」であり、そのうちのある程度の割合が「諜報活動」、インテリジェンスの世界なのです。

S 発言する人の立ち位置によって、言葉の定義や解釈は異なりますね。

T 先日、参加した学会で「ハイブリッド戦」が話題となりました。ハイブリッド戦とは、軍事戦略の1つで、軍事と非軍事、サイバー戦や情報戦などを組み合わせる手法です。2014年のウクライナ危機では、国家の記章が付いていない軍服を着用し、ロシア軍の武器を装備したリトル・グリーン・メンと呼ばれる覆面兵士が、議会や空港、軍事基地などを制圧していきました。これは国際法上明らかな違反です。

一方、ウクライナ側では、状況を把握しようとドローンを飛ばしても、電子戦による妨害電波で墜落させられてしまう。また、携帯電話による通信もサイバー戦により遮断されてしまいました。

ハイブリッド戦ではこうした事態が起こります。果たしてこれは戦争なのか否か、学会で議論を重ねたのです。1つの見方は「技術の進化」です。技術の進化により戦争のあり方が変化したという技術決定論的なものです。

もう1つの見方は、国際秩序の進化により、戦争を正面から認めることができなくなっているという考えです。それ故にこれまでとは違うやり方で相手の動きや武力を封じようとする、いわゆるグレーゾーンへ入り込んでいるというものです。

ハイブリッドとは何かという定義の問題もありますが、死傷者が出たり破壊行為があったりすれば、それは戦争であり、そういった形のものはすでに起きています。そして、サイバー空間だけで完結する戦争は、定義上おそらくないと考えています。

日本を標的にした情報戦の可能性は？

S ハイブリッド戦に関連して情報戦についても伺います。2016年の米国大統領選や、同年のEU離脱を問う英国国民投票では、SNSなどを通じてロシアが世論を操作して選挙介入を行なったとされています。

インフルエンス・オペレーションなどとも呼ばれていますが、現在の日本に対して、中国やロシアが情報戦を仕掛けてきている可能性はあるでしょうか。

T インフルエンス・オペレーションについて、手法としてインターネットやSNSを使うという点からすれば新しいものですが、プロパガンダは昔からありますし、さまざまな形での情報操作も以前から存在しています。そういった意味では、決して目新しいものではないと考えています。

私自身もプロジェクトを組み、3年間にわたって情報戦について調査を行ないましたが、明確な形での結論は出ませんでした。2018年の沖縄県知事選では、インフルエンス・オペレーションが行なわれたのではないかと言われていますが、情報をたどってみてもソースは国内のものばかりで、外国からの介入を示す証拠は見つかりませんでした。

また、2020年1月に行なわれた台湾の総統選挙では現地に赴き調査を行ないました。話を聞いてみると、確かにインフルエンス・オペレーションの痕跡はありました。SNSでは台湾在住と言いながらも、中国大陸から発信されているものなどです。しかし、こうした情報が市民に対してどれほどの影響を与えているのか、正直なところ不明です。

蔡英文総統が「中国はわれわれに情報戦を仕掛けている」と言い続けていましたから、市民も身構えて慎重に行動したのだと思います。

今後、外国による選挙介入が日本で起きたとしても不思議ではありません。ただ、そうした介入によって重大な結果がもたらされるかどうかは不明です。あわせて、外国の勢力が選挙に介入することによって得られる利益についても考えておく必要があると思います。

S 確かに、外国の勢力がどのようなことを望むか

によってシナリオは変わってくると思います。そこがインフルエンス・オペレーションの特定を難しくする要因でもあると思います。

ロシアの言論統制

S ここで、視点を変えて、中国やロシアの情報戦対策について伺います。中国にはグレートファイアウォール（金盾）がありますから、ネットワークの監視・検閲も可能だと思いますが、ロシアではどのような方法がとられているのでしょうか。

T 最も有効な対策は言論統制でしょう。これにはいくつかの方法があります。1 つは反政府的な言論を徹底的に弾圧するというものです。プーチン大統領への批判を続ける政治活動家のナワリヌイ氏などは刑務所に収監されてしまいました。反政府的な記事を掲載する媒体そのものも規制されるのでビジネスが成り立たなくなってしまいます。

数年前にロシアに行なったときの話です。ロシアにもサイバーセキュリティの技術研究をしている人は数多くいます。ですが、私のように国際政治の視点から研究している人はいませんでした。疑問に感じて彼らに尋ねたことがありました。すると、研究はビジネスだと言われたのです。理解できず、どういう意味なのか訪ねると、ロシアでは研究資金は政府が提供しているために、政府が好まないテーマに資金が提供されることはないというのです。このように、記事を掲載する媒体や資金の流れを絞ることによって規制をかけています。

他にも、国内に多数の代替メディアを作ることが挙げられます。日本ではほとんど知られていませんが、フコンタクテ（VKontakte) という SNS サービスがあります。英語の “keep in touch（連絡を取る）” の意味で、ロシア版 Facebook とでもいうべき存在です。他にもヤンデックス（Yandex）という国内で人気の検索エンジンがあります。中国も同様の政策をとっていますが、自国民が米国のサービスに触れる機会を抑えようとしているのです。とはいいつつも、多くのロシア人が Facebook を使っているそうです。

米国の情報戦対策

S 米国はロシアからのインフルエンス・オペレーションに対して、どのような対策をとっているのでしょうか。

T 結論を先に言えば、有効な対策はとられていません。話が少しそれますが、一連の情報戦をロシア側から見ると、最初に仕掛けてきたのは米国だと認識しているのです。パナマ文書によって明らかとなったプーチン大統領側近の不透明な資金運用にしても、オリンピック選手団の組織的なドーピング不正問題にしても、すべては米国 CIA が仕掛けた情報戦だというわけです。

米国が、ロシアにはメディアの自由がないと主張するならば、反対に米国にはメディアに嘘を流す自由もあるはずだ、というのがロシア側の論理です。そして、フェイクニュースを流しました。場合によってマスコミが本当のことを論じたとしても、今度は米国大統領がそれをフェイクニュースだと騒ぎ立ててくれる。危機感を持った米国議会は、Facebook や Google に事態の収拾を求めますが、これは検閲につながります。米国がこれを行なってしまうと、中国やロシアと同じになってしまうのです。ですから、現在のところ、効果的な対策は打てていないということになります。強いて言えば、暴力行為を扇動したとして、トランプ大統領（当時）の Twitter アカウントを永久凍結しましたが、それが精一杯なのだろうと思います。

S 民主主義社会では対抗措置はとりづらいですね。

T 言論には言論で対抗せよ、ということになると思います。

2016 年以降の米国選挙とサイバーセキュリティ

T 2017 年 1 月、オバマ大統領が退任する直前ですが、選挙に関する大統領令に署名をしています。その内容は、選挙を米国の法律に基づく重要インフラの 1 つに指定し、セキュリティ対策の強化をはかるというものです。

米国の法律では 16 の重要インフラがあります。

その中の政府施設のサブセクターとして選挙が組み入れられました。これにどのような意味があるかと言えば、サイバー軍が選挙インフラを守れるようになったのです。

2018年に行なわれた中間選挙では、米国のサイバー軍が、ロシアによる選挙介入の中核組織であるIRA（Internet Research Agency）からのインターネットアクセスを切断しました。

サイバー軍を指揮するポール・ナカソネ司令官によれば、2020年の選挙防衛はサイバー軍の最優先事項であり、「執拗な関与（Persistent Engagement）」という言葉を用いて、ロシアが干渉を試みるたび徹底的にそれを阻止すべく行動したと述べています。

とはいえ、ロシアの狡猾なところは、選挙に介入すると見せかけて、IT企業のソーラーウインズに攻撃を仕掛けたことです。選挙介入に積極的だったのはロシアではなくイランだったと言われています。ロシアからすれば、トランプ大統領がいるだけで選挙は混乱し、民主主義そのものへの信頼も損なわれるので、必要以上に選挙介入にこだわる必要はないという判断をしたのだと思います。

サイバー空間での大国間の対立を収束させることは可能か

S これまで話を伺って、民主主義・専制主義、どちらの陣営も、サイバー空間で思うがままに諜報活動を行なっていることがわかりました。ただ、このまま進めば、大国間の対立の溝はさらに深まるばかりです。現実世界には核兵器による抑止力がありますが、サイバー空間では、各国が協調して事態を収束させられるのか疑問に感じています。国際協調の動きなどあれば教えてください。

T 協調の動きはいくつかありますが、まずは国連の取り組みが挙げられます。国連政府専門家会合（GGE：the Group of Governmental Experts）の場でサイバーセキュリティに関する議論が行なわれています。25カ国（常任理事国の5カ国含む）の専門家がメンバーとなっています。日本もこの会合に加わり議論を重ねてきました。

本年5月末には、第6会期（2019年～2021年）の最終会合が開催され報告書が採択されました。報告書は、サイバー空間における脅威認識、規範、国際法の具体的適用、信頼醸成、能力構築などについての共通認識を示すもので、本年の国連総会に提出される予定です。先日、この話題について、外務省の方から連絡をいただきました。

前回の第5会期（2016年～2017年）では、報告書の提出までにはいたりませんでしたから、第4会期（2014年～2015年）以来の合意となります。

当然、この会合にはロシアも中国も参加しています。特にロシアは、サイバー空間における国際法の適用について、一定の合意を得るために積極的だったそうです。これは何を意味するのかと言えば、新たな条約を作って米国の動きを止めたいのです。

また、官民協力の取り組みを挙げると、GCSC（Global Commission on the Stability of Cyberspace）という組織があります※2。複数国の政府や省庁をはじめ、IT企業、教育・研究機関といったさまざまな組織によって構成されています。サイバー空間の規範を作り、6つの提言を行なっています。

サイバーグレートゲーム

S 先生が上梓された『サイバーグレートゲーム』を拝読しました。世界の関心事であるサイバーセキュリティの問題を、国際政治の視点から「選挙介入とフェイクニュース」、「サイバーインテリジェンス」、「サイバー防衛」といった形で分類し、一般読者にも理解しやすいように執筆されていると感じました。各テーマは独立しており、読者は自分の興味や関心に沿って読み進められます。

先生がご自身で世界各地に取材へ行き、現地の人の声を聞き、自らが撮影した写真を掲載する。こうして作られた紙面にはリアリティがあります。また、長目に書かれた序文にも、ある種のストーリーが感じられて好印象を持ちました。

T ありがとうございます。プーチン大統領の写真を撮って掲載していますからね（笑）。ただ、残

※2 **Global Commission on the Stability of Cyberspace** https://cyberstability.org/

念なことに、現在はコロナ禍で渡航できなくなりました。

S まったくそのとおりです。コロナ禍で移動ができない中、情報収集や意見交換はどのようにされていますか。

T オンラインでは限りがあります。話をしていても、みなポジショントークに終始していて、裏話や本音を語るところまでには発展しません。

S 情報収集に SNS を利用されますか。

T SNS はほとんど見ていません。もちろん、有用な情報を発信しているアカウントはあると思っています。情報収集では、なるべく 1 次文書には目を通すようにしています。

S 最後に、今後の活動や目標について教えてください。

T 私自身は研究者ですので、今後も研究を続けていきます。直近でいえば、選挙介入をテーマとした書籍に共著として携わっていて、先日脱稿したところです。もう 1 つ、個人的に海底ケーブルに関心を持っていて、これをテーマに執筆したいと考えています。執筆の構想から 5 年ほどたちますが、なかなか執筆に取りかかれないという状況です。

S どちらの書籍にも期待しています。今回のインタビューで先生のお話を伺って、これまでは個別の事案だと認識していたものの間につながりが見えるようになりました。今後は、国家間の対立を視点の軸にサイバーセキュリティについて見ていきたいと思います。本日はありがとうございました。

夭逝のセキュリティ・リサーチャーを偲ぶ
日本のセキュリティ業界関係者から寄せられたコメント

追悼 ダン・カミンスキー

構成・斉藤健一

本年 4 月 23 日、世界的に有名なセキュリティ・リサーチャーのダン・カミンスキー氏が逝去した。42 歳という若さだった。長年患っていた糖尿病による急性代謝性合併症（ケトアシドーシス）が原因だと伝えられる。このニュースは瞬く間にインターネット中に広がり、Twitter をはじめとする SNS では多くの人々が、彼の早すぎる死を悼んだ。その訃報は、テック系ニュースメディアにとどまらず、ニューヨークタイムズなど一般メディアによっても伝えられている※ 1。これは生前の功績の大きさや影響力の高さを示すものだ。

DNS ぜい弱性の発表で一躍時の人に

彼の名を一躍世界に知らしめたのは 2008 年に発表した DNS のぜい弱性を突く攻撃手法だ。DNS はインターネットの根幹をなす技術の 1 つであり、その安全性が脅かされることはネット社会の信頼性が揺らぐことにもなりかねない。

DNS では UDP が使われており、TCP に比べて通信データの偽造が容易なことから、キャッシュ DNS サーバーにニセの情報を送り記憶させドメイン名を乗っ取る「DNS キャッシュポイズニング」の危険性が以前から指摘されていた。とはいえ、攻撃を成功させるには、サーバーにデータがキャッシュされていない状態であることや、権威サーバーへの問い合わせに使用する ID と攻撃側が送信するニセ情報の ID が一致している、といった条件が必要だった。

しかし、カミンスキー氏が発表した手法では、同じドメイン内に存在しない名前を変化させながら連続で問い合わせることで、キャッシュが有効になることを回避した。また、DNS の ID は 16 ビット（65535 通り）と規定されており、元より総当たり攻撃に対する耐性は十分とは言えなかった。

この攻撃によって DNS キャッシュポイズニング成立の可能性が大幅に高まることとなった。同時に、そのインパクトの大きさから「カミンスキー・アタック」と名付けられた。さらに、この発表がきっかけとなり、その後の DNSSEC 導入の流れが活発となった。

セキュリティ業界きってのショーマン
人柄を褒めたたえる声も多数寄せられる

カミンスキー氏は非常に魅力的な人物だ。BlackHat や DEFCON といったカンファレンスで彼が話すと、会場は底抜けに明るく愉快な雰囲気へと一変する。まさに、セッションはショーと化し、彼はその MC となる。

彼が DEFCON でスピーチするようになったのは 2000 年代初頭のこと。当時の DEFCON はアレクシスパークという小さなホテルで開催されており、一部のセッションは屋外に設置したテントで行なわれていた。当然エアコンもなく、巨大な冷風機を使ってテント内に空気が送り込まれていたものの、40℃を超える真夏のラスベガスでは焼け石に水といった状態だった。そんな会場であっても彼のセッションには溢れんばかりの人が集まっていた。

当時は、有名ハッカーグループの cDc（Cult of the Dead Cow）が、Back Orifice（リモート・ア

※ 1 **Daniel Kaminsky, Internet Security Savior, Dies at 42**
https://www.nytimes.com/2021/04/27/technology/daniel-kaminsky-dead.html

クセス・ツール）や Camera/shy（ステガノグラフィ）といった新作ツールを DEFCON で発表していた。多くの聴衆が詰めかけ、会場はコンサートホールさながらの熱気に包まれていた。その様子を目の当たりにしたメディアが「ハッカーがロックスターと化した」と報じていた時代でもあった。

その後、cDc のようなハッカーグループの活動は沈静化していったが、カミンスキー氏は 20 年以上もセキュリティ業界の最前線で活躍を続けた。DNS のぜい弱性を発表した 2008 年には日本で開催された BlackHat Japan にも登壇している。

余談だが、DEFOCN では過去のセッション動画をアーカイブしているが、今回の訃報を受けカミンスキー氏の動画を集めたプレイリストを公開している※2。

また、インターネット上には彼を偲ぶコメントを寄せられているが、その多くが彼の人柄を褒めたたえるものとなっている。本誌でもカミンスキー氏とゆかりのある人々にコメントを依頼。以下にそれらを紹介させていただく（順不同・敬称略）。

国内セキュリティ業界関係者から寄せられた追悼コメント

●はせがわようすけ（セキュアスカイ・テクノロジー）

2008 年にセキュリティ業界に転職した私に、それまで趣味で行なっていた調査研究がこの業界に対してもきちんとインパクトを与えられるものだと自信を与えてくれたのがカミンスキー氏でした。

Black Hat Japan での私の講演を「おもしろい」と絶賛し、後のパーティーでも何度も繰り返し「本当に興味深い研究だ。もっと話したい」と肩を組んで気さくに声をかけてくれたことで、大きな舞台での初めての登壇に気後れしていた自分は大きく助けられました。

過去の実績や知名度で判断するのではなく、おもしろい講演に対しては素直におもしろいと伝えることもまた若手を育て業界を盛り上げる大きな要因だと気づかせてくれたのも氏の行動です。あの時のお礼を言う機会を失ってしまったことが残念でなりません。

●本川祐治（当社）

ダンの訃報を知った時、「また大切な人を失った」と悲しくなりました。ダンはいつも朗らかで、おばぁちゃんお手製のクッキーをタッパーに入れて持ち歩き「やぁ！クッキー食べない？」と声をかけてくれました。ビールを飲むと陽気だったのも素敵でした。研究者としてのダンは、誰もが気にしていたインターネット基盤の問題についてわかりやすく説明してくれました。特に DNS に関してはさまざまな角度から目の前で実証してくれました。

RIP, Dan.

※2 **DEFCON の YouTube チャンネル、ダン・カミンスキー氏のセッションをまとめたプレイリスト**
https://www.youtube.com/playlist?list=PL9fPq3eQfaaC-2LgmH8MlMi41ryw8ty2l

参考資料 **JPRS トピックス＆コラム 新たなるＤＮＳキャッシュポイズニングの脅威 ～カミンスキー・アタックの出現～**
https://jprs.jp/related-info/009.pdf

●笠原利香（スイス在住）

最初に彼に出会ったのは 2003年のラスベガス。人懐っこく、話好きで、毎年会うのが楽しみなだった。2007年にばおばーちゃんの焼いたクッキー」を持参して、パケット・ケイレツのこと、日本でフグを食べたことなど、爆笑続きのインタビューを HackerJapanにしてくれた。

翌年のある日、「彼の名前をそのまま漢字にできる !!!」といきなり思いついた私が手作りしたのは、「仮眠好・男」というTシャツ。多忙と時差ボケで、ラスベガスでもうたた寝ばかりの彼にピッタリ。彼にプレゼントしてまたみんなで大爆笑だった。このTシャツ、私の一生に一度のコピーライトの大傑作だと思っている。気に入ってくれてありがとう。仮眠ばかりの生活は終わり。ゆっくり眠ってね、ダン。

●エル・ケンタロウ

ダン・カミンスキーと初めて会ったのはもう 10 年以上前のこと、彼が日本に講演に来た時だった。その頃、すでに彼の研究は世界中から注目されていた。講演後、彼に質問に来る参加者の通訳を務めたが、彼は誰に対しても、どんな質問に対しても真剣にかつユーモアを交えて答えていたことを思い出す。根っからのテクノロジー好きだったと言える。

その後、彼はどんどん注目されるようになり、ベガスでは発表すれば、会場に立ち見が出て入れないほどの人気だった。ダン・カミンスキーの功績はセキュリティに限らず、インターネット全体の進歩に多大な影響があったと言える。まさしくインターネットを守ったスーパーヒーローと呼んでいいと思う。

しかし、彼の訃報を受けて、彼を知る人の多くが彼の研究者としての功績よりも、人間としての魅力を思い出している。ダンは、本当に優しく、ユーモアに溢れた人間だった、太陽のように明るいというわけではなく、洞窟の奥でゆらゆらと揺れる蝋燭の炎のような、ほっとする明るさだった印象がある。研究者としては、超一流では片付けられないぐらいの才能を持ち合わせながら、誰よりも研究熱心で好奇心旺盛だった。確かに、人間として完成していないところもあったが、それがまた彼の魅力だったとも思う。

よく、カンファレンスを運営する仲間と会って話すと、みなダンに振り回された逸話を語る。惜しい人を亡くしたと思う反面、やっと彼がゆっくりできると思うと複雑な気持ちになる。

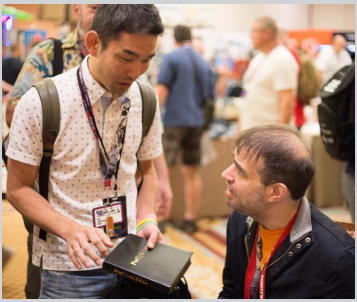
●寺島崇幸 a.k.a. tessy (AVTOKYO 代表)

AVTOKYO を初めて開催したのは 2008 年 10 月 11 日。それ以前は、米国ラスベガスの DEFCON や国内開催の BlackHat Japan といったイベント後に開催していた単なる飲み会だったのです。ところが、2007 年に BlackHat 主催者（当時）のジェフ・モスさんをはじめ何人かのスピーカーが飛び入り参加して盛り上がったことから、今につながる「AVTOKYO」へと変わったのです。

当日、HackerJapan の出版元である白夜書房に会場を提供していただきセミナー形式で 1 部を行ない、終了後は場所を移して 2 部の飲み会を開催。

そんな手作りな初開催イベントにダン・カミンスキーさんは顔を出してくれたのです。常に笑顔で気さくに周りの参加者と語っていた姿が記憶に残っています。コミュニティと人のつながりっていいなあと改めて思いました。当日のサイン T シャツは家宝として保存してあります。

・花田智洋（SECCON 実行委員長／ AVTOKYO スタッフ）



彼が飛び入り参加した AVTOKYO 2008 で初めて対面。急きょ開催された LT（ライトニングトーク）大会にうっかり勢いで手を挙げてしまい、聴衆の「英語でやれ」のヤジに乗っかり怪しい英語で「肉認証」（牛肉を使った静脈認証の登録）のプレゼンを披露。後に伝え聞くところによると、彼はスライドを見ながら手を叩いて喜んでくれていたとか。

それから数年が経った 2011 年頃、彼が突然思い出してくれたようで、プレゼン資料を公開するようにと篠田佳奈さんにメッセージを送ってくれて※ i、あわてて英語版を作り公開しました※ ii。

そしてプレゼンから 10 年後の 2017 年、DEFCON25 に参戦した際に書籍サイン会場で彼の姿を発見。tessy さん、園田道夫さんに「俺が日本で肉認証を披露した花田だ！」と言ってこいと焚きつけられ、話かけてみたら「お前誰？」的な塩対応（写真上）。

顔面蒼白のまま慌ててオンライン上にアップしておいたプレゼン資料を見せたところ、彼の記憶が蘇り「お前、あのクレイジーなやつじゃないか！」とサインを中断して立ち上がって肩を組んでもらったのが彼と僕のストーリー（写真下）。ご冥福をお祈りします。

※ i　https://x.com/dakami/status/1370556479120384000
※ ii https://www.slideshare.net/slideshow/avtokyo2008-after-party-ka-e-da-mabiometrics-authentication-hacks/10357665

●篠田佳奈（CODE BLUE 事務局代表）

ダン・カミンスキーの訃報。
「嘘でしょ？」
それが私の最初の言葉だった。
あんなに愛された人がこんなに早く？
いや愛されすぎたからなのか…
今日は 4 月 1 日のエイプリルフール？ いやもうゴールデンウィークは目の前だ。

忘れがちだけど死は誰しものそばにある。
形あるものは壊れ、自分を含めいつかはみな旅立つ。
でも早すぎる…
ダンは舞台の上ではハリウッドスターのように輝いていた。彼の講演はいつも大人気だった。舞台の上の彼は身振り手振りが大きいから写真はよくぶれた。でもそれが素敵だった。笑顔が満点で、彼が破顔するだけでそこにいる誰もが幸せになった。
2008 年には、結果として最後の開催となった BlackHat Japan に招へいできた。そしてこの年が初回の AVTOKYO にも参加してくれた。笠原利香さんが作った「仮眠好・男（カミンスキー・ダン）」と書かれた T シャツを最高だと喜んでくれた。花田智洋さんによるステーキ肉を使った認証デバイ

次頁に続く

スを騙す研究発表に腹をかかえて笑い、「最高のコンテンツだよ！ぜひ世界に発表すべきだ！」と花田さんを激励した。

10 年経ってラスベガスで 2 人が偶然 DEFCON で再会した時も「あの時の君か！」と破顔して大きなハグをしていた。
ダンはあんなに最高の人物だったからこんなに早く逝ったのかな。
まるで、もうこの世になんの未練もないみたいに、流れ星みたいにこんなに早く…
彼みたいな人に縁できたことを心から嬉しく、また誇りに思う。

写真は 2008 年の BlackHat USA。彼の最愛のおばあちゃんと。「おばあちゃんの作るクッキーは最高なんだぜ」と彼は私に 1 枚手渡してくれた。
彼の天国への道はエクスプレスチケットでフカフカのソファ席なんだろうけど、もし可能なら、またすぐに生まれてきてほしい。彼のいない世界はちょっとさみしい気がする。
最高にクレバーで最高にハッピーなダン・カミンスキー。
たくさんの思い出をありがとう！

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.43

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