SSRC SHIELD Security Reserch Center

Hisys Journal

VOL.02

HITACHI
Inspire the Next

株式会社 日立システムズ

プロフィール：本名はジェフ・モス（Jeff Moss）。DEFCON 主催者であり Black Hat の創設者。米国国土安全保障省の諮問委員や ICANN のチーフ・セキュリティ・オフィサーなどを歴任。長年にわたりハッカーコミュニティと政府機関との橋渡し役を務めている。

ダーク・タンジェント インタビュー

●インタビュー＝笠原利香　●写真＋構成＝斉藤健一

NSA をはじめとする国家によるネットワーク監視の発覚、SSL の信頼性を根幹から揺るがす Heartbleed 脆弱性、米国を執拗に攻撃する中国人ハッカーなど、この 1 年間で報じられたセキュリティに関する事件は数知れず、これらの脅威に世界中の人々が不安を感じている。そんな状況の中、各国のセキュリティ専門家が一堂に会する DEFCON22 が開催され、例年を上回る参加者があったという。今回は主催者であるダーク・タンジェント氏に今年の DEFCON について話を伺った。

Q1 中国人ハッカーに手を焼く米国政府がセキュリティ・カンファレンスに出席する中国人に対してビザを発行しないのではないかという噂が流れました。DEFCON ではどうでしたか？

A1 実際のところ、DEFCON には多くの中国人が来てくれましたし、中国の CTF チームも参加してくれました。僕自身、この噂について調べてみましたが、出所はわかりません。もしかすると中国人に対する政治的な警告だったのかもしれません。

1 つ、面白いエピソードがあります。とある中国人が DEFCON 参加のため米国大使館へ行きビザの申請をしたそうです。大使館職員が確認のため DEFCON の Web ページにアクセスしたのですが、その日はたまたま音楽イベントの出演アーティストを告知するニュースがトップに掲載されていたのです。それを見た大使館職員は「これはコンピューターのカンファレンスではない、音楽イベントだ」といって、ビザを発行しなかったそうです（笑）。Web ページをもっと詳細に見るべきでしたね。

Q2 今年は会場がかなり混雑しているように感じました。参加者数は昨年と比べてどの程度増えたのでしょうか？

A2 正確な数字は把握していませんが、確実にいえるのは昨年より 1500 人以上増えているということです（編注：昨年開催した DEFCON21 の参加人数はおよそ 1 万 5000 人）。DEFCON は木曜日から日曜日にかけて開催されます。例年だと参加登録は木曜日から土曜日にかけて均等にあるのですが、今年はなぜか木曜日の午前中に集中してしまい、長蛇の列ができました。理由はわかりませんが「ドットコムバブル」が起きた 2000 年当時をほうふつとさせました。

Q3 来年以降、Rio All Suite から他のホテルへと開催地を変更することは検討していないのですか？

2011 年から DEFCON 会場となった Rio All Suite も今年で最後。来年からは Paris と Bally's の 2 つのホテルで開催される

A3 今年はこれまで以上に各種ビレッジ（ハンズオンセミナー）を増やしています。プライバシーや暗号、ICS（産業制御システム）などです。小さなグループであっても特定の目的を持つ人たちが交流できる場所を提供したいと考えたからです。

しかし、現状の会場規模では限界に達したので、来年は変更する予定です。3 時間後に行われる閉会式で正式に発表しますので、それまで待ってください（笑）（編注：閉会式にて Paris と Bally's が来年の会場になると発表されました）。

Q4 今回の DEFCON ではローガン・ラム（Logan Lamb）氏によるホーム・セキュリティ製品に関する講演がキャンセルとなりました。この理由は何でしょうか？

A4 彼は数社の製品の調査結果を発表する予定でしたが、それらの製造メーカーが彼が勤める会社に対して発表を取りやめるよう圧力をかけてきたことが理由のようです。

Q5 日本のセキュリティ研究者は周囲からの圧力を気にして、ホーム・セキュリティ製品など PC 製品でないものを研究対象にすることを避ける傾向がありますが、米国の研究者はどうでしょうか？

A5 米国ではセキュリティ研究はある種、社会へのサービスだと考えられています。

製造メーカーに製品の欠陥を指摘することで、より良い製品作りにつながります。また、情報を広く公開することで、消費者が製品選びの際に参考にできる「インフォームド・チョイス」にも役立ちます。短期的には問題も起こるでしょうし、不便が生じるかもしれませんが、長期的に見れば必ず良い方向に向かうと思います。

例えば錠前メーカーを例にすると、かつての製品にはいくつもの欠陥がありましたが、研究者らの指摘によって改善が進みました。また、市場に新たに参入しようとするメーカーも、公開されている情報を利用すれば、一定水準以上の製品を最初から作ることができます。

Q6 製造メーカーが DEFCON に対して圧力をかけてくることはないのでしょうか？

A6 過去にはありましたが、現在ではありません。おそらく、われわれが圧力に屈することなく戦うということを製造メーカーが知ったからだと思います。先述のように矛先が講演者に向かうようになったのはこういった背景もあるのです。

もちろん、DEFCON では「責任あるディスクロージャー※1」を守るよう講演者に求めています。

ただ、研究者の中には、メーカーやベンダーに脆弱性を報告し、彼らの回答を待つ間に DEFCON の講演に応募する人もいます。こういった場合、DEFCON としては秘密を厳守し、講演のアナウンスを開催ぎりぎりまで行わないこともあります。その結果、メーカーやベンダーは慌てて対応を始めますが、講演までに間に合わなかったという例がありました。

Q7 いくつか一般的な質問をします。Anonymous のようなハクティビストについて意見を聞かせてください。彼らに賛同しますか？ それとも抗議は別の形で行うべきだと思いますか？

A7 彼らの活動を考えるには、マクロの視点とミクロの視点、その両方を持つ必要があります。問題を提起して人々の目を向けさせるというマクロの視点から見ると彼らは正しいと思います。しかしミクロの視点から見て、目的を遂行するための DoS 攻撃には賛同できません。というのも、攻撃は対象に限らず周囲のネットワークに対しても副次的な被害を及ぼすからです。

DoS 攻撃というと、以前は Web サーバーへの接続をあふれさせるものでしたが、最近ではアプリケーションサーバーを標的としたものも出てきています。バックエンドのデータベースに負荷をかけるクエリを送りつけるのです。これならトラフィック量は少なくて済みます。このように社会的に意識を持った攻撃に変わりつつありますが、個人的には別の方法で抗議すべきだと考えています。

※1 **責任あるディスクロージャー (responsible disclosure)**: コンピューター・セキュリティにおける脆弱性情報公開ポリシーの１つ。研究者が脆弱性を発見したときに、ベンダーへ報告し、パッチ作成など一定時間を経た上で一般に対して情報公開を行うもの。現在主流の考え方。

Q8 NSA はいまだにインターネットの監視を続けていますが、これに対して意見を聞かせてください。

A8 監視は、米国に限らずフランス・ドイツ・ロシア・中国など、さまざまな国で行われています（笑）。もはやインターネットの監視は日常のことと考えた方がよいかもしれません。それよりも監視に対してどのように対応していくかが次の課題となるでしょう。

インターネットの監視は何度となく取りざたされていましたが、確たる証拠もなく、これまでは誰も何もできませでした。しかし、監視の実態が明らかになったことで、インターネットのポリシーや製品も変化してきています。

IETF（インターネット技術タスクフォース※2）では、よりセキュアでプライバシーに配慮した将来のプロトコルについて議論が始まっています。こうした意味で、監視の発覚は重要なターニングポイントとなったのではないでしょうか。

Q9 スノーデン氏は過去 DEFCON に参加したことはあるのでしょうか？

A9 参加したことはないと思います（笑）。ただ、彼の方から今年の DEFCON でパネリストの一員としてディスカッションに参加したいという提案はありました。しかし、多くの人がパネリストとして登場しテーマも多方面にわたる予定だったことや、彼自身がすでに 7 月に開催された HOPE※3 にビデオ会議システムを使って参加しており、DEFCON で新たな話が出てくるかどうかなど不安な点が多かったため、彼の提案は受けませんでした。

笠原：来年の DEFCON も期待しています。ありがとうございました。

※2 **IETF（Internet Engineering Task Force）**：インターネットで利用される技術の標準化を推進する組織。（https://www.ietf.org/）

※3 **HOPE**：米国のハッカー雑誌 "2600" が主催するカンファレンス。1994 年に第 1 回が開催され今年で 10 回目を迎えた。（http://www.hope.net/）