HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.24

株式会社 日立システムズ

Human * IT

Hitachi Systems security Journal VOL.24

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

マシンによる防御の自動化、国家によるネット監視とプライバシー、アップル対FBIなど
イベント主催者が語る米国セキュリティ業界のトピック

Jeff Moss a.k.a Dark Tangent

ジェフ・モス　インタビュー

米国ラスベガスで毎年夏に行なわれる BlckHat や DEFCON は、セキュリティ業界の動向を知る上で欠くことができないイベントだ。今年の DEFCON ではマシン同士が競い合う CTF である DARPA Cyber Grand Challege が盛大に開催され、業界に防御の自動化という新たな潮流をもたらすこととなった。今回は DEFCON の主催者であり BlackHat の創設者でもあるダーク・タンジェントことジェフ・モス氏に、米国セキュリティ業界のトピックなどについて話を伺った。

●インタビュー＝笠原利香（Rika Kasahara）
●写真＋構成＝斉藤健一（Ken-ichi Saito）

セキュリティ自動化時代の幕開けを告げるCGC

笠原利香（以下 R ）：今回の DEFCON で開催された CGC（Cyber Grand Challenge）※1 には、スケールの大きさやショーアップなどいろいろな面で驚きました。

ジェフ・モス（以下 J ）：3 年間で 5500 万ドル（約 55 億円）の予算が投じられていますからね。

R 競技中にみごとな解説をしていたのは、kenshoto（見性戸）の…

J VISI ですね。元々別の人が解説を担当する予定だったのですが、トラブルがあって、VISI が急きょピンチヒッターで解説を担当することになったのです。

R CGC はどのようなコンセプトで始まったのでしょうか。

J DARPA のディレクターであるマイク・ウォーカー（Mike Walker）氏のプロジェクトです。彼は DARPA に在籍する前から DEFCON CTF の運営にも携わっていて、次世代の CTF についても考えていました。そして、DARPA のプロジェクトマネージャー就任を期に、防御の自動化をめざした CGC に着手しました。DARPA のプロジェクトマネージャーの任期は 3 年で、この間に自分のビジョンを実現するのです。前任のピーター・ザッコ（Peiter Zatko）氏も同様ですね。彼はサイバー・セキュリティの分野の優れた研究に対して、少額ではあるけれど、スピーディに予算を交付するプロジェクトを立ちあげました。

R DEFCON 24 のテーマは “Rise of The Machines（マシンの台頭）” です。これは映画「ターミネーター 3」のサブタイトルでもあるのですが、どういう意味が込められているのですか。

J 背景には CGC の開催がありますが、セキュリティ業界において、マシンによる自動化という新たな時代の幕開けになるのではないかと考えたからです。攻撃者がマシンを使えば敵になりますし、防御に使えば味方にもなってくれます。もちろん、ターミネーターも意識はしていて、半分ジョーク・半分本気のネーミングなのです。

●ジェフ・モス（Jeff Moss）

DEFCON 主催者であり BlackHat の創設者。ダーク・タンジェント（Dark Tangent）のハンドルとしても知られている。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おり、DHS（米国国土安全保障省）諮問委員会のアドバイザー、CFR（米国外交問題評議会）のメンバーなどの任にも就いている。

R なるほど。

J つけ加えると、CGC で優勝した Mayhem は、従来の DEFCON CTF 決勝戦にマシン単体で出場しています。また、3 位の Shellphish は、マシン＋人間というチーム構成で出場しています。マシンだけでどこまで戦えるか、マシン＋人間ではどうなのか、今回の DEFCON CTF はいろいろな意味で興味深いと思います（編注：2016 年 9 月 1 日時点で全チームの順位は公表されていませんが、競技 2 日目を終えた時点で Meyhem が 15 チーム中 15 位、Shellphish が 12 位）。

R 確かにおっしゃるとおりですね。IT 業界のキーワードの 1 つに “AI（人工知能）” があります。しかし、AI の飛躍的な進歩は人類にとって危険ではないかという批判の声もあります。この点に関して何か意見はありますか。

J CGC では AI ではなく “CRS（Cyber Reasoning System：

※ 1 競技の模様は YouTube で視聴可能　https://www.youtube.com/watch?v=n0kn4mDXY6I

CGC 会場には各チームごとにカラーリングされたマシンがずらりと並ぶ

CGC 閉会式での一幕。上位 3 チームのメンバーが壇上に立つ。後ろのスクリーンにはコメントする DARPA プロジェクトマネージャーであるマイク・ウォーカー氏の姿が映し出される

サイバー推測システム）”という言葉を使っています。攻撃の検知、ぜい弱性の発見からパッチ作成や適用といった一連の流れには 16 ～ 18 のステップがあると言われています。CGC 以前にも CRS は存在していました。ただし、これらのステップを部分的に自動化するに留まっていたのです。CGC の画期的なところは、すべてのステップを自動化した CRS を作り出したところにあると思います。

ハッカーがクリントン候補を支援 !?

R 11 月の大統領選を前に、民主党のヒラリー・クリントン候補を支援する “Hackers for Hillary” という基金にあなたが協力したという記事を目にしました※ 2。これについて話を聞かせていただけますか。

※ 2 **Hackers for Hillary: event attendance 'through the roof' after Trump remarks**
https://www.theguardian.com/technology/2016/aug/04/hackers-for-hillary-attendance-black-hat-conference-trump

J “Hackers for Hillary” という名前については誰が付けたのかは分かりません。友人の中にクリントン候補を支援する基金を作りたいという人物がいて、協力したといっても、会合での講演を依頼されたというものです。私としては、基金の会員だけでなく誰もが聴講できることを条件に承諾しました。2 時間の講演のうち最初の 1 時間は会員限定で、後半の 1 時間は聴講自由という形で行なわれたのです。

R セキュリティ業界の人たちが政治に関心を持つことはこれまであったのですか。

J ネット上でのプライバシーを守ろうとする人たちの間では政治の話題が取り上げられることはありましたが、セキュリティ業界では初のことだと思います。

R 結果はどうだったのですか。

J 主催者は当初、20 名〜 30 名が参加し 1 万ドル（約 100 万円）が集まればよいと考えていたようですが、結果は 60 名ほどが参加し、約 3 万ドル（約 300 万円）の支援金が集まったと聞いています。

ネット監視とプライバシーの未来

R 話は変わりますが、米国の PLAYBOY 誌（2016 年 7/8 月号）に「デジタル世代の監視とプライバシー」[※3] という記事を寄稿されたと聞きました。残念ながらその記事をオンラインで読むことができないので、記事の概要を簡単に教えていただけませんか。

J はい。オンラインの監視というと多くの人が NSA（米国家安全保障局）に目を向けますが、私は少し別の見方をしています。現在、ユーザーの情報を最も集めているのは企業なのです。例えば、スマートフォン・アプリでは、アプリがアドレス帳や GPS 情報などを取得することに OK しないとインストールできないものもあります。一方、現実世界では、ショップ内の Wi-Fi に接続すれば、ユーザーの滞在時間、場合によっては売り場のどの場所にいたかという情報まで分かります。企業はあの手この手を使ってネットワークをマーケティングや広告の場に有効活用できないかと考えているのです。

R 確かに。

J 国家などによる監視とはすこし話はずれますが、こういった企業のマーケティング戦略により、ユーザーがネットから受け取っている情報は操作されたものであると言えます。

R なるほど。ユーザー自身は自分の好みで選んだ情報だと思っていても、実は企業の影響を受けている可能性があるということですね。

J そのとおりです。現在のサイバー空間では、一人ひとりのユーザーが読んでいるニュース、見ている広告、さらには聴いている音楽でさえ、企業によってカスタマイズされたものとなり、経験する現実もユーザーによって異なっているのです。例えるなら各ユーザーはシステムによって作り出された透明な球体（バブル：泡）の中にいて、他のユーザーとは仕切られた世界の中で暮らしているような状況なのです。

R バブルとは言い得て妙ですね。

J 今後、AI を活用したビッグデータ解析などが進めば、今よりはるかに効果的な広告戦略が登場するかもしれません。企業によるユーザー情報の収集は今後さらに加速していくに違いありません。そして、このとき政府が企業に対してユーザーの個人情報の提供を求めたらどうなるでしょう。政府は自ら国民の情報を集めなくても、企業が集めたものを提供してもらえればよいのです。現在、さまざまな企業がユーザーに対してフリーで使えるサービスを提供していますが、将来的にこのような状況になることを想定すると、本当のフリーとは何なのか、いま改めて考える必要があると思います。

R かなり現実味を帯びていますね。話を聞くと、企業が収集した個人情報を政府が使うことに対して規制を設けるべきだという意見も出てきそうですが、これに対して何か意見はありますか。

J 個人的には使い方によるのではないかと思います。例としてユーザーの位置情報を記録するスマートフォン・アプリで考えてみます。仮にどこかでひき逃げ事件などが発生したとします。警察が広域のスマートフォン・ユーザーの位置情報履歴に

※ 3 **Playboy Magazine Releases "The Freedom Issue"**
http://www.prnewswire.com/news-releases/playboy-magazine-releases-the-freedom-issue-300289874.html

アクセスできるとしたら、事件発生の前後に現場付近を通った目撃者を探すことに役立ち、事件解決につながるかもしれません。ただし、警察といえども行きすぎた情報利用には規制を課すべきでしょう。また、悪意を持つ人間による利用も危険です。例えば、水面下で提携を進める企業同士のトップ会談や潜入捜査を行なう警察官などの場合、位置情報の特定は死活問題だと言えます。ですから、今後 4 ～ 5 年の間に政府は規制に関して何らかの方向性を打ち出すべきだと考えています。

R なるほど。

J スマートフォンのアプリでは他の問題も抱えています。米国にはコンピューター犯罪を取り締まる法律として CFAA（Computer Fraud and Abuse Act）があります。この法律が制定されたのはアナログモデムを使ったダイヤルアップ接続が主流の 1980 年代です。この法律における不正アクセスの判断基準は「同意」であり、ユーザーやネットワーク管理者の同意を得ない接続は「不正」とされていたわけです。

R 懐かしい時代でした。

J スマートフォンの SNS 連携アプリなどでは、ユーザーの同意なしにさまざまなサービスに接続していて、法律の基準にそぐわなくなっているのです。他にも一部の企業が CFAA を盾にセキュリティ研究者の調査を拒むケースが出てきているそうです。

R そうなると研究者は慎重にならざるを得ないですね。

J そのとおりです。調査が困難になると、セキュリティ業界の発展にも影響を与えかねません。カナダにも同様の法律がありますが、調査などの結果が公共の利益になると判断されれば例外として認められます。米国もカナダを見習ってほしいと思います。

R おっしゃるとおりですね。

Apple 対 FBI の争点とは？

R 最後の質問です。今年米国では iPhone のロック解除をめぐり、Apple 社と FBI が対立し、一時は裁判所までを巻き込む闘争にまで発展しました。これについて何か意見はありますか。

J 難しい質問ですね。この対立を突き詰めて考えると、2 つの争点があると思います。1 つは米国国内においてセキュアな製品を作る権利があるかどうかという点です。FBI は Apple 社に対して犯罪者が使用した iPhone のロック解除とバックドアの設置を求めましたが、仮にこれが認められたとしたら、セキュアな製品を作る権利がないということになってしまいます。

R 非常に興味深い視点ですね。

J もう 1 つは、米国の憲法ではソフトウェアのコードは言論の自由として認められているという点です。FBI が Apple 社のソフトウェアに介入するということは、言論の自由の侵害とも言えるわけです。ただ、実際のところ、FBI は第三者の協力を得て iPhone のロック解除に成功し、訴えを取り下げましたから、この 2 つの争点に関する裁判所の判断は下されていません。

R ソフトウェアのコードが言論の自由として認められているというのは先進的であり、米国らしいと思います。

J 余談ですが、FBI と Apple 社の対立を別の視点からお話します。数学者や製品開発者からすると、暗号はセキュアであるか否かという二者択一的な考えしかありません。しかし、FBI 関係者が求めている暗号は「セキュア」と「インセキュア」の中間なのです（笑）。

R 確かに。それでは議論がかみ合わないは当然ですね（笑）。本日はさまざまな視点から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した。

ハッカーやセキュリティにまつわるニュースを独自の視点から捉える時事コラム

Threat Scope

#22 米国大統領選を標的としたサイバー攻撃の可能性

文＝エル・ケンタロウ

セキュリティ専門家の多くが米国大統領選へのサイバー脅威を懸念

米国大統領選挙は 11 月の本選を目前に控え選挙戦も本格化、共和・民主両党の競争も激化している。そんな最中、本年 7 月後半から 8 月にかけて、民主党に関連する情報漏えい事件が立て続けに起こっており、政府機関・メディア・セキュリティ業界関係者などから選挙そのものがハッキングされる可能性を危惧する声も聞こえ始めている。世界に大きな影響力を持つといわれる米国大統領を決める選挙は、はたしてハッキング可能なのだろうか。

セキュリティ企業の Tripwire 社は、8 月初旬にラスベガスで開催された BlackHat USA 2016 において「ハッカーが米国大統領選に影響を与える可能性」についてアンケート調査を行なった。対象はカンファレンス会場を訪れた 220 名のセキュリティ業界関係者。その結果、回答者の 63% が「可能性あり」と答えている。

調査自体がセキュリティカンファレンスの会場で行なわれたという特殊性を差し引いても、大統領選へのサイバー脅威の影響は無視できない状況であることは明らかと言えるだろう。

余談だが、BlackHat USA の直後に開催された DEFCON 24 では、サイバー攻撃による政府転覆の可能性を研究した講演も行なわれていた。

情報戦を制する者が大統領選を制する

これまでに行なわれた大統領選を振り返ってみると、現代的なマーケティング手法が選挙戦で有効に活用されたのは、民主党のクリントン氏が勝利した 1992 年の大統領選だと言われている。この時のクリントン陣営は当時最先端のマーケティング手法を取り入れ、民意の変化や状況などを的確に把握したり、注力すべき地域の特定などを行なったりしたとされる。

また、ソーシャルメディア黎明期の 2008 年に大統領選に挑んだ当時のオバマ候補はソーシャルメディアを巧みに使った草の根運動を展開。資金調達力ではるかに勝るヒラリー・クリントン候補を破り、民主党の代表候補となった。本選でも同様にソーシャルメディアを駆使して国民の支持を集め、大統領の座を射止めた。

同選挙では、米国統計学者のネイト・シルバー（Nate Silver）氏にも注目が集まった。シルバー氏は、過去のデータや世論調査の分析から投票結果を予測し、全米 50 州のうち 49 州でみごとに的中させた。この時から選挙戦におけるデータ分析がより重要視されるようになったことは言うまでもない。

このように、米国大統領選はその時代ごとの最先端の情報処理分析がさまざまな角度から使用されてきた。

大統領選を取り巻くサイバー脅威

今回の大統領選では、本年 3 月に Anonymous が共和党のトランプ候補を引き下ろすとして OpTrump を決行し、トランプ候補個人の電話番号をネット上で公開したがトランプ候補の選挙戦への影響はほぼなかった。一方、本年 4 月ごろからはクリントン候補の民主党を標的とする情報漏えい事件が連続して発生している。この漏えい事件の犯人像や背景に関してはさまざまな憶測が流れているが、この事態を重く見た民主党はサイバーセキュリティに関する顧問会議を設立した。

また、共和党は本選挙のマニフェストにおいて、サイバー空間がもたらす米国への危険性について多岐にわたって触れており、米国政府として早急

にサイバー空間における姿勢を明確にする必要があると主張している。

今回の一連の事件を受けて、大統領本選自体へのサイバー攻撃の可能性についてセキュリティ業界・メディア・政界などさまざまな方面から危惧する声が上がっている。

昨年、政治的サイバー攻撃の増加を予測したセキュリティ企業、Forcepoint 社のボブ・ハンスマン（Bob Hansmann）氏は、さまざまな攻撃主体が米国の選挙キャンペーンを標的にする危険性を示唆している。政治的背景のみならず、多くの個人情報が集まる選挙関連組織は攻撃者にとって格好のターゲットである、と同氏は警鐘を鳴らしている。

また、著名なセキュリティ研究家のブルース・シュナイアー（Bruce Schneier）氏は、ハッカーによる大統領選関連の攻撃は民主主義そのものへの攻撃であり、米国政府は迅速な対応を求められる時期に来ていると指摘。シュナイアー氏を含めセキュリティ関係者の中には 11 月の投票時には電子投票システムそのものが標的となる可能性を示唆している。

電子投票システムに関しては過去数年来、ぜい弱性が指摘されており、実際州によっては電子投票から従来の紙での投票に切り替えているところも現れている。米国政府としても今回の大統領選を取り巻くサイバー脅威に関する危険性を認識しており、連邦捜査局（FBI）と国土安全保障省（DHS）もいく度にわたり警告を発している。

米国国家情報長官（Director of National Intelligence）のジェームス・クラッパー（James Clapper）氏は、超党派センターの公聴会において「われわれ政府情報機関もさまざまな攻撃主体が共和・民主党両党を標的とした攻撃を展開していることを把握している。今後このような行為は激化する可能性がある」との見解を示した。また、公聴会において同氏は、国家的な背景を持つ攻撃主体のみならず、ハクティビスト（政治活動のためにハッキングを行なうグループ）に加え、金銭目的の犯罪攻撃主体による攻撃キャンペーンが展開されていることを把握しており、両陣営に対して公平に情報開示を行なっていることも明らかにした。

このようにさまざまな脅威が大統領選を取り巻いているが、サイバー攻撃によって選挙結果そのものがひっくり返される事態にはならないだろうと予測する向きもある。というのも、米国における選挙は各地域で行なわれることから、システム全体を攻撃することは非現実的であり、一地域に絞ったところで選挙結果全体への影響は低いと考えられるからだ。

マギル（McGill）大学研究員のガブリエラ・コールマン（Gabriella Coleman）氏は、むしろ攻撃主体は選挙プロセスそのものに疑問をもたらすことが目的であり、結果的に社会不安を煽ることが目当ての可能性があると指摘している。

いずれにしろ、世界が注目する米国大統領選が日々変わり続けるサイバー脅威によってどのように影響を受けるか、セキュリティ関係者のみならず世界中が注目している状況下にあることは間違いない。結果が出た後でもさまざまな脅威による選挙戦への影響が分析されることになるのは否めないだろう。

●参考文献

Bruce I. Newman（1993）The Marketing of the President: Political Marketing as Campaign Strategy SAGE Publications

●参考 URL

Timeline of Guccifer 2.0's Democratic National Committee Hack.
https://m.reddit.com/r/dataisbeautiful/comments/4qmem6/timeline_of_guccifer_20s_democratic_national/
Hacking of DNC raises fears of cyber attack on US election
http://phys.org/news/2016-08-hacking-dnc-cyber-election.html
By November, Russian hackers could target voting machines
https://www.washingtonpost.com/posteverything/wp/2016/07/27/by-november-russian-hackers-could-target-voting-machines/
States ditch electronic voting machines
http://thehill.com/policy/cybersecurity/222470-states-ditch-electronic-voting-machines
Hackers target the campaigns of presidential contenders
http://securityaffairs.co/wordpress/47455/hacking/hackers-target-presidential-contenders.html

6 Modern Marketing Strategies From Barack Obama
http://time.com/20141/obama-on-between-two-ferns-zach-galifianakis/
Could the U.S. election be hacked? It's not so unlikely
http://www.cbc.ca/news/world/pringle-election-hacking-1.3713911
Experts say cybercriminals are trying to manipulate the US election
http://www.cnbc.com/2016/08/11/most-cybersecurity-experts-say-criminals-are-trying-to-manipulate-the-election.html
5 Reasons Why Hackers Can't Rig the U.S. Election
http://fortune.com/2016/08/09/voting-machines-hackers/

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.24

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