HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.26

株式会社 日立システムズ

Human * IT

Hitachi Systems security Journal VOL.26

TABLE OF CONTENTS

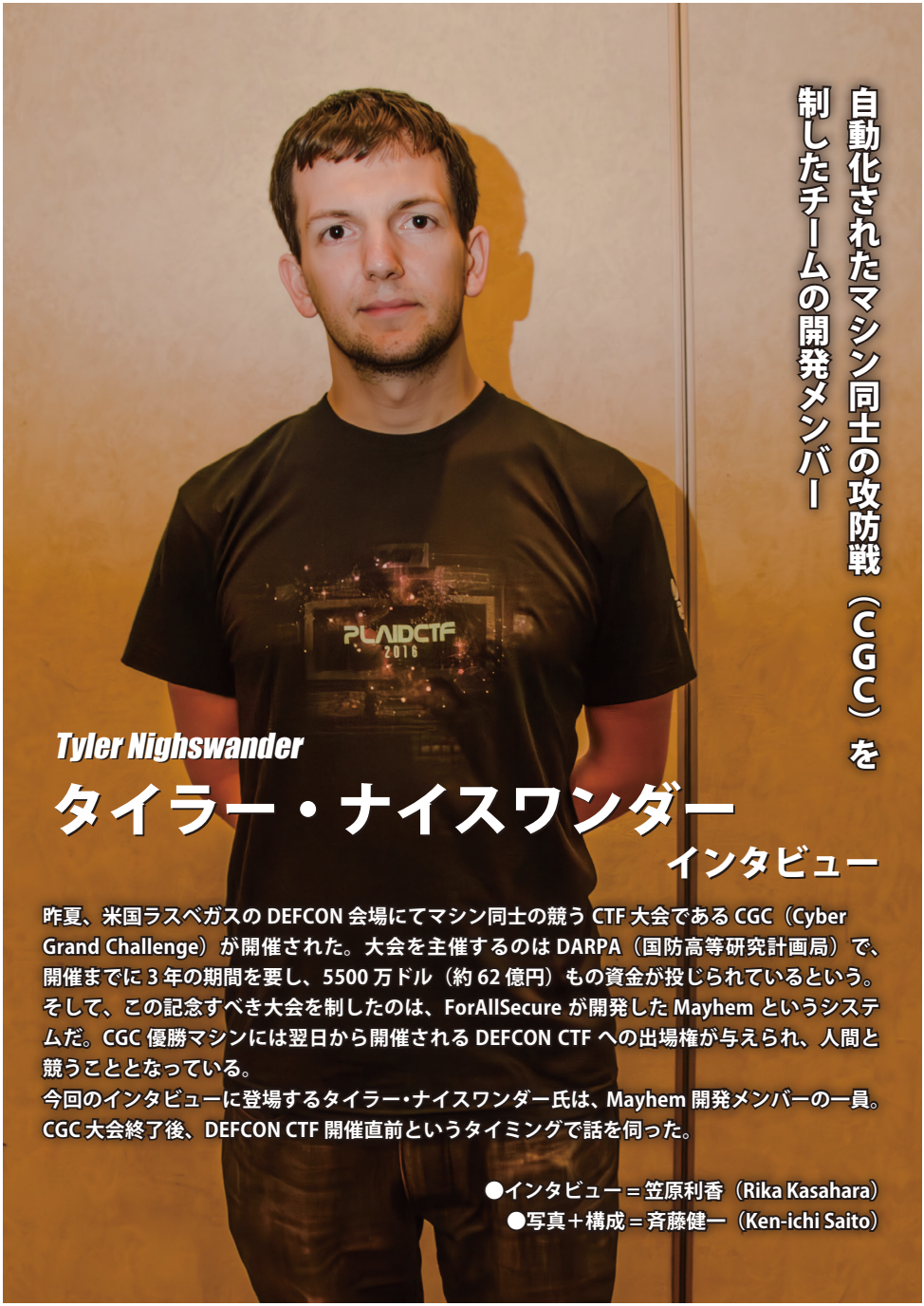
自動化されたマシン同士の攻防戦（CGC）を制したチームの開発メンバー
タイラー・ナイスワンダー インタビュー …… 3

国内初の試み セキュリティ向上と人財育成をめざす
千葉大学　セキュリティバグハンティングコンテスト レポート …… 6

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 …… 10

●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



自動化されたマシン同士の攻防戦（CGC）を制したチームの開発メンバー

Tyler Nighswander
タイラー・ナイスワンダー
インタビュー

昨夏、米国ラスベガスの DEFCON 会場にてマシン同士の競う CTF 大会である CGC（Cyber Grand Challenge）が開催された。大会を主催するのは DARPA（国防高等研究計画局）で、開催までに 3 年の期間を要し、5500 万ドル（約 62 億円）もの資金が投じられているという。そして、この記念すべき大会を制したのは、ForAllSecure が開発した Mayhem というシステムだ。CGC 優勝マシンには翌日から開催される DEFCON CTF への出場権が与えられ、人間と競うこととなっている。
今回のインタビューに登場するタイラー・ナイスワンダー氏は、Mayhem 開発メンバーの一員。CGC 大会終了後、DEFCON CTF 開催直前というタイミングで話を伺った。

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

CGC の優勝マシン Mayhem の実力

笠原利香（ 以下 R ）：CGC（Cyber Grand Challenge）での優勝、おめでとうございます。歴史的な大会を制した見事な勝利でした。今回のインタビューでは、CGC のために開発されたシステムである Mayhem（メイヘム）の実力や、自動化によってもたらされるセキュリティ業界の変化などについて伺いたいと思います。よろしくお願いします。

タイラー・ナイスワンダー（以下 T ）：こちらこそ、よろしくお願いします。

R 早速ですが、ForAllSecure というチームについて教えていただけますか。

T 私が所属している ForAllSecure は 2012 年に創立された企業のチームです。ソフトウェアをよりセキュアにするという理念のもと、カーネギーメロン大学の教授らが中心となり創立されました。従業員もすべて同大学の卒業生で、私自身はリサーチャー兼 Mayhem 開発チームの一員として従事しています。

R どのような経緯で CGC に参加されたのでしょうか。

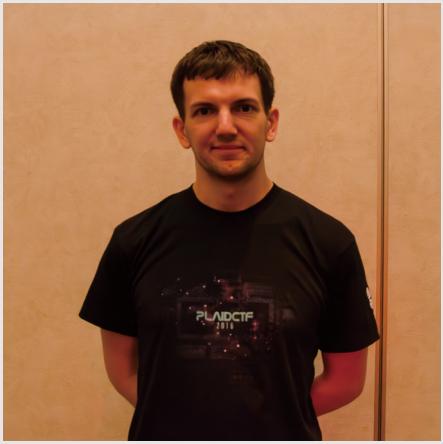
T 私自身は Exploit（エクスプロイト）の自動生成を研究テーマとしており、その成果をどこかで発表したいと考えていました。そこにちょうどよいタイミングで CGC が開催されることとなったのです。

R 単刀直入にお聞きしますが、CGC で優勝できた要因は何だと思われますか。

T 基本的にはハードワークにあると思います。競技に参加した他チームの人たちは、CGC の他にもプロジェクトを抱えていたと思いますが、私個人は、これまでの 2 年間を CGC のためだけに費やしてきました。時期によってばらつきはあるものの、週に 40 時間〜 100 時間ほど働いてきました。

R 次に Mayhem の性能についてお聞きします。例えば、Mayhem では一定時間にどのくらいのぜい弱性を見つけることができるのでしょうか。

T CGC の競技データはまだ検証できていませんが、通常であれば、10 分間に 12（1 ダース）ほどのぜい弱性を見つけ出し、その Exploit を生成することができます。



●タイラー・ナイスワンダー
（Tyler Nighswander）
カーネギーメロン大学学生の CTF チームである PPP（Plaid Parliament of Pwning）の初期メンバー。PPP は DEFCON CTF をはじめ世界各国の CTF 大会で優勝を飾っている。その後、ForAllSecure 社に在籍。2016 年、開発に携わった全自動ハッキングシステム、Mayhem が DARPA 主催の CGC で優勝を果たす。

R 開発ではどのような点で苦労されましたか。

T 先ほども言いましたが、私とチームメンバーのアレックス・ロバート（Alex Robert）は Exploit の自動生成を研究テーマとしていましたから、ぜい弱性を見つけることはそれほど難しくありませんでした。むしろ、ぜい弱性を修正するパッチ生成の部分で苦労しました。

R 先ほどのお話では 10 分間で 1 ダースのぜい弱性発見と Exploit 生成が可能とのことでしたが、パッチの方はどの程度の速度なのでしょうか。

T パッチの生成だけを見れば、ぜい弱性の発見に比べて 3 倍ほどの速度で処理できます。ただし、パッチには検証が必要です。具体的には、パッチ適用前のオリジナルとパッチ適用後のプログラムを付き合わせなくてはならず、結果としてより多くの時間が掛かってしまうのです。

R CGC の競技では、対象となるプログラムは DARPA が意図的にぜい弱性を含めて作成された

ものだと聞いています。ここで疑問なのですが、オープンソースなどで公開されている一般的なソフトウェアに対して Mayhem を使用したことはあるのでしょうか。

T 使用したことはありません。対象となるプログラムの容量に制限はありませんが、ソフトウェアが大きくなると、それに応じて処理時間が大幅に伸びてしまうからです。

R Mayhem には他に特徴的な実装などはありますか。

T CGC の競技では、DARPA が作成したチャレンジ（ぜい弱性を含むプログラム）を解析し、生成した Exploit を使って他のチームに攻撃を仕掛けられるという側面があります。Mayhem では自身が発見できなかったぜい弱性が使われた攻撃を受けた場合、その Exploit を解析するような機能も実装しています。

コンピューターによる自動化によってセキュリティは今後どのように変化するのか？

R DARPA では各チームのプログラムソースや競技中のネットワークトラフィックのログといった CGC の成果を公開する予定です。これによって現実の世界に何か影響を与えられると考えていますか。

T 影響は 2 つあります。1 つはこういった攻防戦が全自動で実現できたと世界に示せた点だと思います。もう 1 つは、全自動システムを構築したいと考える人たちの参考になるという点です。DARPA が作成したチャレンジと各チームのシステムを比較しながら読むことで、より理解が深まると思います。

R 一般的な質問ですが、このような全自動システムを攻撃者が悪用する可能性はあると思いますか。

T もちろん、その可能性は大いにあると思っています。ただし、このようなテクノロジーを誰もが使えるということは、簡単に悪用できるぜい弱性が減ることにもつながるはずですから、長い目で見れば攻撃者に不利な状況になると思います。

R CGC での優勝により Mayhem は DEFCON 24 の CTF 本戦に出場することとなりましたが、勝算はありますか。

T 全くありません（笑）。

R では、将来的にはどうでしょう。

T 皆目見当もつきません。というのも、マシンと人間では特性が異なるのです。例えば小さなプログラムが 100 個あり、それらのぜい弱性を次々と解析していくのであれば、マシンの方が圧倒的に有利です。しかし、大きなプログラムのぜい弱性を解析する場合は人間の方が得意だと思います。人間が解析をする場合には、コードの重要な部分とそうでない部分を判断することができますが、マシンにはこれができません。ただし、これは現時点での話であって、5 年後くらいには状況が変わる可能性もあります。

R とても興味深いお話です。人とマシンの関係性を踏まえて、今後 10 年でセキュリティの仕事はどのように変化すると思いますか。

T 現在、私は 1 日あたり 10 時間ほど、プログラムのバグを見つける作業をしています。今後は、マシンがバックグラウンドで常に動いていて、何かしらの判断が必要な場合に限り、人が介在するような状況になっていくと思います。

R 今後、プログラムが実用的なプログラムを書くような時代は来ると思いますか。

T マシンがそこまでできるようになるにはより多くの時間が必要です。ただし、人が書いたプログラムを解析したりパッチを当てたりすることは、近いうちに実現できると思います。

R 未知の攻撃（ゼロデイ）に対してマシンで防御することは可能だと思いますか。

T OS やブラウザーといった巨大なプログラムでは無理ですが、IoT 関連などで使われる小さなプログラムであれば対応できると思います。

R これまでの話を伺い、現在のマシンでできること、まだ実現できていないことなどが明確になりました。今後しばらくは人とマシンが協調する時代なのですね。

T そのとおりです。マシンが得意なことはマシンに任せて、人はより創造的な活動に取り組んでいくのがよいと思います。

R 本日はありがとうございました。

国内初の試み セキュリティ向上と人財育成をめざす

千葉大学 セキュリティバグハンティングコンテスト レポート

取材・文＝斉藤健一

さまざまな組織に広がる「バグ報奨金制度」

新聞をはじめとする各種メディアで報じられているとおり、サイバー攻撃による被害は増加の一途を辿っている。その要因の 1 つがダーク Web などと呼ばれるブラック・マーケットの存在だ。通信経路を秘匿する特殊なブラウザーを用いるために、一般ユーザーが目にすることはない。ここでは麻薬・銃器・児童ポルノなどあらゆるものが売買の対象となっているが、他にもボットネットのレンタル・マルウェア作成キット・ソフトウェアのゼロデイぜい弱性なども売買されている。

こうした状況に対抗するため、自社のソフトウェアや Web サービスなどのぜい弱性を発見した社外の技術者に対して報奨金を支払う「バグバウンティ・プログラム」を設ける企業も出てきている。米国では Google やマイクロソフトなどの IT 大手企業はもちろんのこと、ユナイテッド航空などの企業や陸軍といった組織にまで広がりを見せており、日本国内でもサイボウズ社や LINE 社といった企業がこの制度を設けて外部の力を活用している。

大学の Web サービスを学生自身が調査するコンテスト

このような中、千葉大学が「セキュリティバグハンティングコンテスト」を実施した。在学生を対象としたバグ報告奨励制度で、学内ネットワークのセキュリティ強化と人財育成を目的としている。日本の大学としては初の試みとなる。主催は同大学の CSIRT、技術協力を行なったのはセキュアスカイテクノロジー社だ。

コンテストの開催期間は 2016 年 12 月 15 日から 2017 年 1 月 15 日までの 1 ヵ月間。参加には事前に行われる講習を受講し、ハンターライセンスを取得する必要がある。ハンターは大学から指定されたサイトへ、学内ネットワーク・インターネットを問わず接続可能で、コンテスト期間中にぜい弱性を調査し、そのレポートを提出する。

コンテストが開始される 12 月 15 日には講習会が開かれた。参加者は学内に貼り出されたポスターなどを見て興味を持った学生たちで、理系に限らず文系学部の学生も含め 47 名の参加があった（後日行われた補講には 16 名が参加）。これは大学側が予想していた数字を大幅に上回るものだったという。

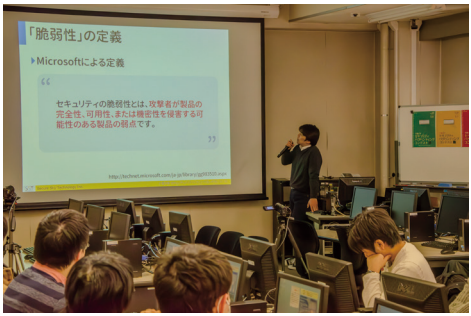
法律と技術、2 本立ての講義

講習会では石井徹哉副学長による法律・倫理面の講義と、セキュアスカイテクノロジー社の長谷川陽介氏による Web セキュリティの基礎に関する講義が行われた。

石井副学長の講義では、バグという言葉の説明から、ぜい弱性診断などの行為に関連する不正アクセス禁止法の解説が行われた。さらに終盤では、発見したぜい弱性の取り扱いについても言及し、IPA（独立行政法人 情報処理推進機構）が窓口となっている「ソフトウェア等のぜい弱性届出受付」などが紹介された。

一方、Web セキュリティの基礎講義はぜい弱性の定義を考えるところから始まった。ぜい弱性はバグの一種で「本来できてはいけないことができてしまう」というのが一般論だが、講師の長谷川氏は経済産業省や IPA、マイクロソフトなどの定義を紹介し、ソフトウェアの開発者・運用者・利用者・業務としてソフトウェアの診断を行なう人

講習会開会の挨拶に立った千葉大学石井徹哉副学長は法律・倫理の講義も担当



セキュアスカイテクノロジー社の長谷川陽介氏による Web セキュリティの基礎講義

など、立場や状況により解釈が異なることを示した。また、セキュリティ強化のためにはプログラムの品質向上が重要であるとも強調した。

また、ぜい弱性の種類も万別で、一意に識別するための CVE（Common Vulnerabilities and Exposures：共通ぜい弱性識別子）や、ぜい弱性の深刻度を測る CVSS（Common Vulnerability ScoringSystem：共通ぜい弱性評価システム）などの意義についても語った。

講義中盤では実際のぜい弱性が紹介され、SQL インジェクション、クロスサイトスクリプティング（XSS）、クロスサイト・リクエスト・フォージェリ（CSRF）といった代表的なものの仕組みが解説された。

優れた診断者になるためのポイントとは？

Web セキュリティの講義はさらに続き、内容はぜい弱性の見つけ方といった核心部へと移る。もちろん、実際に試すのは許可を得たサイトに限られると長谷川氏は学生に対して釘を刺す。講義では時間の都合から診断ツールの使い方などについては参考資料（記事末のリストを参照）の提示にとどめ、主にぜい弱性を見つけるための考え方や診断レポートの書き方に関して、ポイントを絞って解説を行なった。

長谷川氏によれば、ぜい弱性を見つけるには技術的な知見も必要だが、それ以上に診断者の意識が重要だという。例えば、Web アプリにさまざまなパラメーターを入力したときに現れる挙動のちょっとした違いに気づく感性や、開発者の思考を探りその裏を突こうとするチャレンジ精神などが挙げられる。

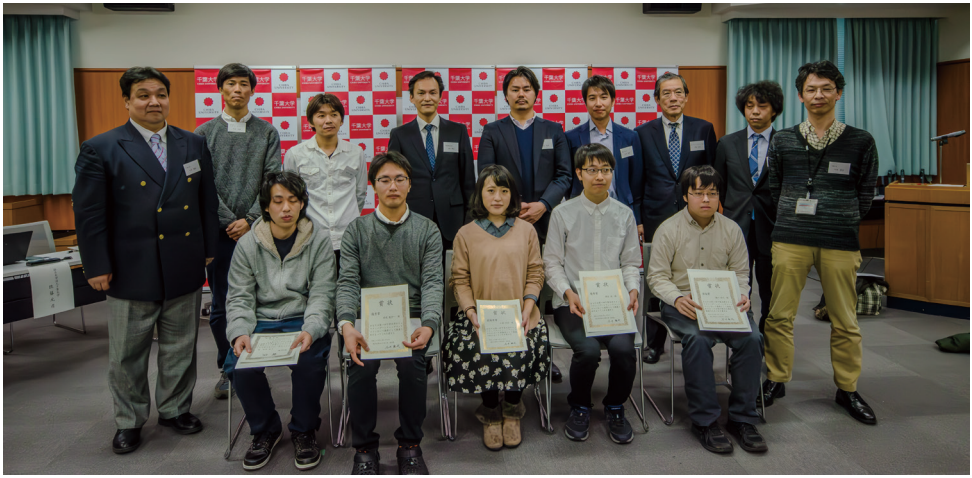
一方、診断レポートに関しても読む側への配慮が大切だとし、診断の結果発見されたぜい弱性や問題点は現実にどのような脅威や被害をもたらす可能性があるかを想定したり、ぜい弱性が発見されなかった場合にはその根拠を示したりすることなども重要だと力説した。また、診断作業の記録を残しておけば、仮に不測の事態が起こったとしても診断者の責任の範囲を明確にすることができ、ひいては診断者自身を守ることにもつながる、と長谷川氏はアドバイスした。

コンテストを想定した演習も実施

講義終了後にはコンテストを想定した演習が行われた。用意されたのは図書館のサービスを模したサイトで、貸し出し履歴の閲覧などを行なうことができる。講習の会場となった教室にはデスクトップ PC が設置されており、学生たちはこのマシンを使ってサイトに接続して隠されたぜい弱性を探っていく。

30 分間ほどの短時間であり、ソフトウェアのインストールも制限された PC ということもあって、多くの学生が苦労していたようだが、それでも SQL インジェクションなどのぜい弱性を発見できた参加者もいた。

また、演習の最後には長谷川氏が想定していたいくつかのぜい弱性が紹介された。



表彰式で記念撮影。前列が各賞を受賞した学生で後列が審査員

コンテストの対象は学生ポータルと学習管理システム

講習の最後にはコンテストの対象となるサイトの発表やルール説明の他、ハンターライセンスの交付が行われた。

コンテストの対象となるサイトは 3 つ。1 つは前述の演習でも使われたようなコンテストのために制作された環境だが、残りの 2 つは学生ポータルと Moodle（ムードル）という学習管理システムで実際に運用されているものと同等のものとなる。そして、これこそが「セキュリティバグハンティングコンテスト」と冠し、他の CTF 大会などとは一線を画す理由でもある。

コンテストの結果は？

コンテストの表彰式が行われたのは 2017 年 2 月 27 日。千葉大学の発表によると、コンテスト終了後にレポートを提出したハンターは 15 名（レポートは 26 本）だったという。審査委員長である千葉大学 CSIRT チームリーダーの今泉貴史氏は総評で、提出されたレポートについて、限られた時間で行われた講習の内容を越えるものであり高く評価していると述べ、コンテストについても成功だったと語った。

その後、成績優秀者 5 名が表彰されたが、特筆すべきは発見されたぜい弱性の中にはコンテスト対象の実運用サイトに修正が反映されるものもあったという点であろう。

表彰式の終了後、この学生たちに話を聞いてみた。筆者は当初、熱心に CTF 大会などに参加し、将来はセキュリティ業界へ進むことをめざすような学生を想像していた。しかし、実際はそのような人物は少なく、多くは情報セキュリティに興味を持っているレベルで進路も未定という学生が多かった。

また、レポートの内容が講義内容を越えられた点について質問してみると、多くの学生がインターネットで検索したり、情報セキュリティに詳しい友人に助言を求めたりしたとの答えが返ってきた。

実運用環境のぜい弱性を発見・修正できたという大きな成果とともに、多くの学生が興味を持って参加したという点も成果だといえる。このような革新的な取り組みを行なった千葉大学の実行力は大いに評価されるべきだろう。

また、石井副学長によれば、来年度以降は他の大学を交えた展開も検討しているとのことなので、このような取り組みが広がるよう期待したい。

講義で紹介された診断ツール・参考資料

●代表的な診断ツール

- **Fiddler**
  http://www.telerik.com/fiddler
- **Burp Suite**
  https://portswigger.net/burp/
- **OWASP ZAP**
  https://www.zaproxy.org/

●その他のツール

- **sqlmap（SQL インジェクションの診断ツール）**
  http://sqlmap.org/
- **ratproxy（Web アプリの診断ツール）**
  https://code.google.com/archive/p/ratproxy/
- **skipfish（Web アプリの診断ツール）**
  https://code.google.com/archive/p/skipfish/

●参考書籍など

- **安全なウェブサイトの作り方（IPA）**
  https://www.ipa.go.jp/security/vuln/websecurity.html
- **体系的に学ぶ 安全な Web アプリケーションの作り方（徳丸浩著・ソフトバンククリエイティブ刊）**
  http://www.sbcr.jp/products/4797361193.html
- **HTTP の教科書（上野宣著・翔泳社刊）**
  http://www.shoeisha.co.jp/book/detail/9784798126258
- **Web セキュリティ担当者のための脆弱性診断スタートガイド（上野宣著・翔泳社刊）**
  http://www.shoeisha.co.jp/book/detail/9784798145624

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

24 AI 時代におけるサイバーセキュリティの攻防

文＝エル・ケンタロウ

人工知能を搭載したマルウェアの脅威

日々変わり続けるサイバー脅威に対抗すべく、さまざまなセキュリティベンダーが人工知能（AI）を利用したソリューションを開発している。本誌 Vol.20 においても、生物界の免疫システムにヒントを得た防衛ソリューションを開発した Darktrace 社の取り組みを紹介した。一方、攻撃者もこの技術を応用したマルウェアの開発を急いでおり、AI 技術はいわば諸刃の剣であるとも言える。

経済誌フィナンシャルタイムズ誌がロンドンで開催したサイバーセキュリティサミットに参加した Darktrace 社テクノロジーデレクターのデイヴ・パルマー（Dave Palmer）氏によれば、マルウェアは日進月歩で進化を続けており、AI を搭載する日も近いだろうと警鐘を鳴らしている。AI マルウェアでは、標的の行動の監視・分析、有効な感染経路の特定、感染のトリガーとなるメール文書の作成までを自動化できる可能性があるという。

文書の自動生成についていえば、ニューラルネット（脳の神経組織の仕組みを模したコンピューターの学習機能モデル）を使った記事の作成や、クリックベイトと呼ばれるユーザーの誘導を目的とした Web ページやヘッドラインの作成などが挙げられる。そして、このような技術を使えば、標的型攻撃とはほぼ特定できないメール文章が作成できるようになるというのだ。

また、AI マルウェアでは、標的の行動を監視・分析した後に攻撃を展開するようになるとパルマー氏は指摘する。例えば、取引先とのミーティング直後に「次回のミーティングはこちら」といった内容で地図が添付されたメールを送るなど、業務での連絡をマルウェアが偽装するようになるという。

さらに、このマルウェアは直接的な破壊活動のみならず、データ改ざんなどを行なうことで、感染に気づかれることなく業務を妨害する可能性もあるという。例を挙げれば、石油プラントを破壊するようなマルウェアは即座に発見され駆除されるだろう。しかし、プラントのネットワーク内にあるデータ収集センサーにマルウェアを感染させ、長期間にわたりデータを改ざんし続ければ、いずれ事業運営を困難にする状況を作り出すことも可能だという。

パルマー氏は AI を搭載したランサムウェアの登場も予想している。ネットワークの状況を監視しながら、最大限の被害を生み出すタイミングを見計らって一気に攻撃を開始するというものだ。

マルウェアに対抗して構成や設定を変化させるネットワークの研究も

ICT 情報ニュースサイト、Information Age の記者であるニック・イスマエル（Nick Ismail）氏によれば、すでに一部のマルウェアでまだ稚拙なレベルであるとしながらも AI 的な機能を持つものが現れてきていると指摘する。

マルウェアを開発する者たちはマルウェアの検知や解析を回避するための技術に注力している。例えば、マルウェアがどのような環境に置かれているかをマルウェア自身が判断し、サンドボックスや解析用の仮想環境では悪意ある挙動を見せないといった機能が挙げられる。さらに、こうした技術は洗練された一部のマルウェアから一般的なマルウェアと広がっていくだろうとも示唆している。

しかし、守る側も手をこまぬいているわけではない。米国政府はこのような新たな脅威に対してもさまざまな対策を検討している。米国陸軍は軍

事企業の Raytheon 社と共同で、ネットワークの構成を変化させる（シェイプシフト）防衛アルゴリズム、Morphinator（Morphing Network Assets to Restrict Adversarial Reconnaissance）を開発している。Morphinator の特長は、ネットワーク運用における管理性を損なうことなく、ネットワークの設定状況やホスト・アプリケーションの設定をダイナミックに変化させることで、マルウェアによるネットワーク調査・推測を困難にさせるという点にある。

現在開発が進められているプロトタイプでは、無線通信などで使われる周波数ポッピングのように、アプリケーションが使用する IP アドレスやポートをダイナミックに変更する機能を実装している。

また、この Raytheon 社の技術以外にも Azos AI 社では CogDat という技術を開発している。これはコグニティブ（認識）データをファイルに埋め込み、ファイルがどこに保存されているのか、ファイル自身が判断するというものだ。仮にファイルが盗まれ攻撃者の元にあると判断すれば、CogDat は攻撃者のマシン環境に関する情報を収集、正規の管理者へ送信後に自己破壊を行なうという。

AI のアルゴリズムも窃取の対象に

このように、AI は次世代防衛策の要と期待されているが、スイス連邦工科大学ローザンヌ校と米国ノースキャロライナ大学の共同研究チームは、今では AI のアルゴリズムそのものが窃取の対象になっているとの論文を発表した。研究チームでは AI のアルゴリズムに対してさまざまなやりとりを行ない返答を分析することで基礎となっているアルゴリズムのリバースエンジニアリングに成功したと発表している。

AI の開発は日進月歩で進化しており、2016 年ラスベガスで開催された DEFCON 24 で話題になった DARPA の Cyber Grand Challenge と同様にアルゴリズム対アルゴリズムのサイバー覇権争いが勃発する日もそう遠くないかもしれない。

●参考 URL

“Artificial intelligence-powered malware is coming, and it’s going to be terrifying”
https://www.businessinsider.com/darktrace-dave-palmer-artificial-intelligence-powered-malware-hacks-interview-2016-10

“How to Steal an AI”
https://www.wired.com/2016/09/how-to-steal-an-ai/

How does advanced malware act like AI?
https://www.information-age.com/advanced-malware-act-like-ai-2545/

The Next Big Threat: AI Malware
http://semiengineering.com/the-next-big-threat-ai-malware/

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.26

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