HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.42

株式会社 日立システムズ

Human * IT

Hitachi Systems security Jounral VOL.42

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

現実のサイバー脅威を教材に!?
台湾企業が実施したセキュリティの実践教育とは？

TeamT5 オンライン・インタビュー

取材・文＝斉藤健一／日英通訳＝エル・ケンタロウ／中英通訳 =Cheryl@TeamT5

サイバーセキュリティの強化は世界各国が直面する喫緊の課題だ。日本においても産官学それぞれが連携してセキュリティ人材の育成に取り組んでいる。しかしながら、教育課程で学んだこととサイバーセキュリティの最前線との間には大きなギャップがある。

台湾のサイバー脅威分析のスペシャリスト集団、TeamT5 はこのギャップを埋めるため、独自の人材育成キャンプを実施したという。その取り組みについてインタビューするとともに、台湾の情勢についても素朴な疑問を投げかけてみた。地政学的な脅威や市民の意識、さらに女性の社会進出など、他国の状況を知ることは日本のことを考えるきっかけにもなるだろう。

インタビューには、TeamT5 の CEO である TT（Sung-ting Tsai）さんをはじめ、キャンプ開催の中心となった Turkey さん、キャンプ講義を技術面から支えた DuckLL さんが参加した。

企業ネットワークに近い環境で行なわれる実践的な教育プログラム

斉藤（以下 S）：本日は TeamT5 キャンプ（以下 T5 キャンプ）について伺います。早速ですが、T5 キャンプが行なわれた日程と参加人数を教えてください。

Turkey（以下 Tu）：開催期間は 2021 年 1 月 19 日～2 月 3 日。この間に、週 2 回のペースで講義が行なわれました。受講者は 15 名ほどです。協力関係にある大学の関係者に声を掛けたり、SNS で募集したりして、集まった 100 名の中から選ばれた学生たちです。キャンプという名称ですが、宿泊が伴っていたわけではありません。台北にある TeamT5 のオフィスが会場として使われました。

S キャンプは無償で行なわれたのでしょうか。また、講義の内容はどのようなものでしたか。

DuckLL（以下 D）：無償です。講義はインシデントレスポンス、リバースエンジニアリング、ぜい弱性調査、脅威インテリジェンスなどが行なわれました。

S 脅威インテリジェンスとは興味深いテーマですね。具体的にどのような講義だったのでしょうか。

D マルウェアを解析して得られた情報を元に、攻撃者を特定していくというものです。

S 攻撃者を特定するということは、実際のマルウェアが教材として使われたのですか。だとすると危険なのではありませんか。

D 推察のとおり、教材は実際のマルウェアです。ただし、C2（コマンド・アンド・コントロール）サーバーの情報は書き換えていますので、生徒に危害が及ぶことはありません。

S 生徒の反応はいかがでしたか。

D マルウェアの解析にはアセンブリの知識が要求されますが、中には苦手の生徒もいて、非常に難しい作業だったという声も聞かれました。講義では、得られた結果を基に OSINT（open source intelligence：公然情報を利用した情報収集・分析）も行ないます。Google の検索結果やパッシブ DNS のログなどを精査することで攻撃者を特定していくのです。多くの学生にとって、このプロセスは興味深いものだったようで、好評を得ました。

S キャンプ全体を通じた生徒の感想はいかがでしたか。

Tu 教科書に載っていることではなく、実例に基づいた教材に興味を持った学生が多かったように思います。このキャンプは CTF とも違います。CTF は主催者によってコントロールされた環境下で行ない、競技のレギュレーションも決まっています。

● Turkey

TeamT5 D39 Vulnerability Research Lab. のプロジェクトマネージャー。台湾初の女性サイバーセキュリティ・コミュニティとなる HITCON Girls の共同設立者であり、台湾ハッカー協会（HITCON）ディレクターも務めている。HITCON、360 conference、iThome CYBERSEC などで講演経験を持つ。

● DuckLL（Liao Zih-Cing）

TeamT5 のシニア脅威インテリジェンス・リサーチャー。CTF プレイヤーであり、リバースエンジニアリング・Exploit・Web セキュリティに強い関心を寄せている。TeamT5 では、自動化された脅威ハンティングの改善を担当し、研究を推し進めるためのツールを開発している。セキュリティコミュニティにも積極的に関与し、カンファレンスで研究発表を行なっている。

● TT（Sung-ting Tsai）

TeamT5 の創立者であり CEO。セキュリティ業界で 16 年以上にわたる経験を持つ。確かな技術バックグラウンドとサイバー脅威の知識でチームを率い、数多くのユニークな脅威探索技術と解決策を考案・開発してきた。また、TT は HITCON（Hacks In Taiwan Conference）の創設メンバーの 1 人であると同時に初代議長でもある。

一方、われわれのキャンプが生徒に提供したものは、実際の企業ネットワークに近い環境です。実践に近いノウハウが得られると思います。

S 興味深い取り組みです。キャンプの運営に携わった TeamT5 のスタッフは何名くらいですか。

Tu 10 名ほどです。

S 開催にあたり最も苦労されたのはどのような点でしたか。

Tu 生徒たちのスキルのレベルが違うことがいちばんの問題でした。教材を作る際、ある生徒には難しくても、別の生徒にとっては簡単なものになってしまうというのは避けたかったのです。共通の教材のレベルをどのあたりに設定するか、調整するのに苦労しました。また、学生の中には高校生もいました。彼らが参加するには保護者の承諾書が必要です。こういった運営面での仕事にも苦労しました。

S 見えないところの苦労がうかがえますね。開催してみて楽しめましたか。

Tu はい。楽しめました。

TT（以下 TT）：私の方から、T5 キャンプについていくつか補足したいと思います。キャンプには 2 つの目的がありました。1 つは教育現場のカリキュラムとエンタープライズ・セキュリティの最前線との間にあるギャップを埋めることです。学生たちは現実に起きている問題やその対策について理解していません。一方、企業側は即戦力として活躍できる人材を求めています。そういった理由から、われわれが自ら学生たちにセキュリティのセオリーを講義しようと考えたのです。もう 1 つの目的はシンプルで、優秀な人材を獲得するためでした。

S 人材は見つかりましたか。

TT もちろんです。優秀な学生にはこちらからインターンの提案を行ないました。今後もキャンプを続けていくつもりです。

台湾の地域性と市民の意識

S 台湾のセキュリティ人材育成について、もう少し視点を拡げてみたいと思います。政府が主催する人材育成の取り組みにはどのようなものがありますか。

TT 個別の取り組みを具体的に挙げることはできませんが、台湾では各省庁が主導して人材育成の施策を講じています。例えば、経済部（Ministry of Economic Affairs）は産業に直結するセキュリティに関して主導していますし、教育部（Ministry of


T5 キャンプの様子（TeamT5 の公式 Twitter より）https://twitter.com/TeamT5_Official/status/1357171879375609860

Education）であれば、セキュリティプロフェッショナルを育てています。

S その背景にはやはり中国との緊張関係があるのだと思いますが、いかがでしょうか。

TT この問題は複雑です。確かにここ数年、中国からの攻撃は増えています。これは事実です。ただ、台湾政府がサイバーセキュリティを重要視するようになったのは十年ほど前にまで遡ります。政府としてサイバー脅威から台湾を守るために、さまざまな形で投資を増やすなどの施策を行なってきました。そうした取り組みが現在につながっているのだと思います。

S 台湾市民はサイバー脅威についてどのように感じているのでしょうか。

Tu サイバー攻撃に関するニュースは多数報道されています。ですが、多くの台湾市民が生活の中でサイバー脅威を意識しているかといえば、そうではないと思います。

TT 一般市民のセキュリティ意識の向上は今後の課題の１つです。

S 市民の意識に関してお尋ねします。台湾は新型コロナウイルスを早期に封じ込めることに成功しました。その取り組みの一環として話題になったのが、マスク在庫の管理アプリです。台湾のデジタル担当大臣のオードリー・タン氏が主導してシステムが構築されたと、日本でも紹介されています。タン氏によれば、システムの構築にはシビック・ハッカー（市民によるボランティア）の貢献が大きかったとのことです。台湾ではこういったプログラミングスキルによる社会貢献といった意識がコミュニティ内に根付いているのでしょうか。

TT あくまで個人的な意見ですが、そもそも台湾は、過去数十年にわたり大学でコンピューター科学や電子工学といった分野のエンジニア育成に取り組んできました。その意味から、コンピューターやネットワークの専門的な知識を持っている人は多いと思います。一方、台湾市民それぞれの社会への帰属感は薄いかもしれません。別の言い方をすれば独立心が強いとも言えます。

S 興味深いですね。

TT 台湾の人は自分のことを独立した存在だと考えているので、政府から強制されることを嫌います。政府はそういう人たちに対して、社会に参加することのメリットを明確に示す必要があります。マスク管理アプリについていえば、そういったメリットがうまくコミュニティに示せたのではないでしょうか。

S なるほど。政府が市民の力を取り入れることに関して、日本よりも台湾の方がうまいのだと、話を伺って思いました。

サイバーセキュリティを女性にとって魅力ある仕事に

S Turkey さんはサイバーセキュリティの女性コミュニティ、HITCON Girls の中心メンバーでもあると聞いています。HITCON Girls 誕生の経緯を教えていただけますか。

Tu もともとサイバーセキュリティに興味のある女性を集めて、勉強会を開いていました。しばらくすると、参加者から定期的な開催を望む声が上がりました。わたしたちも同じ想いを持っていましたから、HITCON Girls として活動をはじめたのです。

S 始めたのはいつごろですか。

Tu 2014 年のことです。

S 勉強会はどのようなテーマで行なわれているのですか。

Tu 参加者の興味にあわせて毎回異なるテーマで開催しています。例えば、Web 診断、マルウェア解析、デジタルフォレンジックなどで、各会ごとに講師も異なります。

S 勉強会にはどれくらいの人が集まりますか。

Tu 50 名ほどです。

S 集まる人の学生・社会人の割合はどれくらいですか。

Tu ほぼ同じか学生の方がわずかに多いくらいです。

S 日本でも CTF for Girls という女性だけのグループがあります。彼女らに話を聞くと、サイバーセキュリティについて学びたいけれど、セミナーや勉強会で男性ばかりの中に混じっていると居心地が悪かったといい、それがコミュニティを始めるきっかけの 1 つとなっていると語ってくれました。この点、台湾ではどうでしょう。

Tu そうした雰囲気は台湾にもあります。

TT 私は女性ではありませんが、同じような状況だったと思います。私は HITCON の主催者として、Turkey たちから HITCON Girls の企画書を受け取りました。セキュリティ業界において、女性はまだまだ少数派です。だからこそ、女性だけが集まるイベントを開催したいというのが発足の趣旨でした。発足当初は、業界で活躍する人たちに講師を依頼していましたが、その後は、自分たちでさまざまなイベントを企画するようになりました。これらのイベントは女性にセキュリティ業界を知ってもらい、興味を持ってもらうことを目的としています。

S 日本では女性がエンジニアをめざすことは、どちらかというと珍しいことになるのですが、台湾ではどうでしょう。

TT 日本と比較すると、台湾の方が女性エンジニアは少し多いように思います。もちろん、私自身、業界全体のことを把握しているわけではありません。TeamT5 に限っていえば、五十数名いるリサーチャーやインテリジェンスアナリストのうち 10 名ほどが女性です。

S 台湾はアジアの中で最もジェンダー・ギャップ（男女の格差）が少ないといわれています。日本ももっと台湾を見習う必要がありますね。話題を戻します。HITCON Girls で他国の女性グループと交流する機会はありますか。

Tu 韓国と日本のグループとは交流があります。

S 交流や意見交換などをしたときに、他国の状況に興味を持ったことはありますか。例えば、国ごとの差違や、反対に国を超えた共通点などです。

Tu 韓国と日本では女性グループが主催した CTF 大会があります。HITCON Girls でも CTF 大会も主催したいと思っています。

S HITCON Girls の今後の目標などあれば教えてください。

Tu より多くの女性にサイバーセキュリティに興味を持ってもらい、コミュニティに参加してほしいと思っています。そして、このキャリアの魅力を広めていきたいとも思っています。

S 本日はありがとうございました。

SECCON 2020 電脳会議 レポート

DEFCON CTF 主催者が開発したハッカー教育のプラットフォームとは

文 = 斉藤健一

2020 年 12 月 19 日、SECCON 2020 電脳会議（以下、電脳会議）がオンラインで開催された。テレビ会議システムを使った講演を中心に、ワークショップやコンテストの結果発表・表彰式などの企画により構成される。元々は SECCON CTF 決勝戦で併催されるカンファレンスだが、新型コロナウイルス感染症（COVID-19）の拡大によって CTF 大会がオンライン開催に移行、それに伴いカンファレンスもオンラインへと移行することとなった。

CTF 決勝戦の模様は前号で紹介済みだ※ 1。今号では電脳会議の中で筆者が注目したセッションを紹介しよう。

セッションはアーカイブ視聴が可能

電脳会議は 2 トラック制となっており、Web サイトにはタイムテーブルの他、各セッションの概要が記載されている※ 2。また、SECCON の YouTube チャンネルでは多くのセッションの動画がアーカイブされている※ 3。

SECCON CTF は世界各地から参加者が集う国際的な大会だ。同様に電脳会議でも海外から数名のスピーカーを招いており、YouTube チャンネルでは英語版に加えて同時通訳の音声による日本語版の動画も公開されている。

ハッキングの基礎を実践的に学ぶサイバーセキュリティ道場

電脳会議で筆者が注目したのは、ヤン・ショシテイシヴィリ（Yan Shoshitaishvili a.k.a. Zardus）氏、コナー・ネルソン（Connor Nelson a.k.a. kanak）氏らが登壇した「情報セキュリティの教育機会・教材としての CTF の可能性 ~ pwn.college の試み ~」のセッションだ。後述するが誰もが利用できるという点に興味を持ち取り上げることとした。

両氏ともに米国ネバダ州立大学（ASU）に所属。ショシテイシヴィリ氏は准教授であり、2018 年から DEFCON CTF を主催する “Order of the Overflow” の創設者。ネルソン氏は博士課程の学生で、世界トップクラスの CTF チームの 1 つ “Shellphish” のメンバーとしても活躍している。

大学でサイバーセキュリティを研究する彼らが開発したのが “pwn.college（ポウン・カレッジ）” だ※ 4。ハッキングの基礎を実践的に学ぶためのプラットフォームで、講義の教材として作られたものだが、ネットでも公開され誰でも無料で利用することができる。

余談になるが、pwn とは own のタイプミスがそのまま定着したもので、「所有する」という本来の意味から、ハッカーの間では対象システムの掌握や権限奪取を表す言葉として使われている。

※ 1 **Hitachi Systems Security Journal**
https://www.hitachi-systems.com/report/specialist/hj/
※ 2 **SECCON 2020 電脳会議** https://www.seccon.jp/2020/ep201219.html
※ 3 **SECCON YouTube チャンネル「SECCON 2020 電脳会議」**
https://www.youtube.com/playlist?list=PL8EZB49XjAP5vk8b9WqpnHaWl_vo8FTuF
※ 4 **pwn.college** https://pwn.college/

また、CTF 競技においては、ぜい弱性を突きバッファオーバーフローなどを引き起こす exploit（攻撃コード）問題の呼称として pwnable といった表記が使われている。

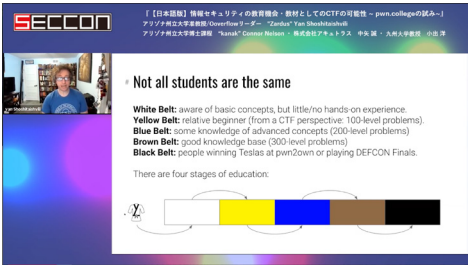
ハッキングスキルの習得を武道の修行に見立てる

セッションの冒頭、ショシテイシヴィリ氏はハッキングスキルを教えることの難しさを語った。例えば、講義でバッファオーバーフローを解説した上で生徒にデモを体験してもらったとしても、彼らが次に体験する機会はおそらくない。一方、いきなり CTF に参加したとしたら、何も達成できずにフラストレーションが溜まるだけだ。かといって、演習の場合でも、ガイダンスが不十分であれば、生徒のモチベーションはなかなか上がらない。

ハッキングスキルの習得には継続したトレーニングが必要となるが、生徒のスキルは個人ごとに異なっている。この課題を解決するためにショシテイシヴィリ氏らが考えたのは、ハッキングスキルの習得を武道の修行に見立てることだった。

まずは、ハッキングスキルのレベルを 5 段階に区切り、それぞれを武道の段位を表す帯の色に例えた。白帯から始まり、黄・青・茶・黒へと進む。白帯はコンピューターの基礎的な知識はあるが実践経験はほとんどないというレベル。黄帯は CTF 初心者、青帯が CTF 初・中級のプレイヤー。茶帯は中・上級のレベルで、最高段位の黒帯は世界的な CTF 大会で活躍したり、ぜい弱性発見コンテストで入賞したりできるレベルだ。

青帯までたどり着ければ、その後は CTF 大会に参加するなどして自ら研さんを深めることができる。しかし、そこにたどり着くまでの体系的なカリキュラムがこれまでは存在していなかった。こうした溝を埋めるために作られたのが、pwn.college であり、白帯から黄帯・青帯へとステップアップするためのサイバーセキュリティ道場だとショシテイシヴィリ氏は語る。



ヤン・ショシテイシヴィリ（Yan Shoshitaishvili a.k.a. Zardus）氏。ハッキングスキルを武道の帯の色に例えて説明

スキルの習熟は緩やか繰り返しの鍛錬が重要

セッション中、1980 年代半ばに制作された映画「ベスト・キッド」のエピソードが紹介された。日系人の空手の師匠が主人公の少年に自動車のワックスがけを命じるシーンだ。「ワックス・オン、ワックス・オフ」これは劇中の名セリフ。命じられたときには知るよしもなかったが、手にしたスポンジで円を描くワックスがけの動作が、相手の攻撃をかわす空手の動きと同じであり、日々ワックスがけを続けていた主人公がこの動きを自然に体得していたというものだ。

ショシテイシヴィリ氏によれば、ハッキングスキルの習得もこれと同じだという。学習の効果を示す曲線は緩やかであり、繰り返し鍛錬することが重要なのだと説く。同様に、成長を促すための適切なガイダンスや、モチベーションを維持するための仕掛けも必要だという。

Pwn.college はさまざまなインターネットサービスを使って構成されている。あらかじめ収録された講義の動画が YouTube で公開されており、学期の期間中（8 月～ 12 月）にはリアルタイムの講義が Twitch で配信される。また、生徒のサポートには Discord やメーリングリストが使われている。

1 学期でシェルコードが書けるようになる !?

講義はコンピューター科学の基礎を履修した生

コナー・ネルソン（Connor Nelson a.k.a. kanak）氏による pwn.college の解説。図は上位ユーザーを表示するスコアボード

セッション終盤では中矢誠氏（画面左上）と小出洋氏（画面右上）が加わり質疑応答や日米の教育の違いなどが議論された

徒が対象だ。1 学期間をかけてシェルコードが書けるようになることをめざすという。授業は週に 3 時間。当然、これだけの時間では足りず、生徒は自らチャレンジ（課題）に取り組む。大学が提供する仮想マシンにインターネットを通じてアクセスし、Web ブラウザー上に表示されたコンソール画面からコマンド操作を行なう（SSH で直接仮想マシンに接続することも可能）。

チャレンジは CTF のバイナリ解析の問題そのものと言ってよい。学習のテーマは、バッファオーバーフロー、リバースエンジニアリング、ROP（リターン・オリエンテッド・プログラミング）、カーネル・エクスプロイテーション、ぜい弱性探索の自動化など全部で 12 あり、それぞれがモジュールとして分類されている。また、モジュール内には難易度が異なるチャレンジが多数用意され、すべてを合計すると 360 問を超えるという。バイナリ解析に特化しているのは、ショシテイシヴィリ氏の専門分野だからだ。

生徒は自分のスキルレベルにあわせて学習を進める。エクスプロイテーションに関するチャレンジがクリアできれば黄帯、すべてのチャレンジを終えることができれば青帯を獲得できる。

ゲーム感覚が学習意欲を促進
対象分野の拡大が今後の課題

セッションの中盤では、ネルソン氏がデモを交えながら pwn.college の使い方を具体的に紹介した。Web ページのスコアボードには、多くのチャレンジを解いた上位ユーザーの名前が掲示され、さらに黄帯・青帯ユーザーを賞賛するページもある。ネルソン氏によれば、こうした仕掛けが生徒のモチベーションを高めることに繋がっているという。実際、多くの学生が熱心に取り組み、週に 10 ～ 40 時間を費やしたそうだ。これは 1 つの講義にかける時間としては異例の長さだという。

セッション終盤では、九州大学教授の小出洋氏と株式会社アキュトラストの中矢誠氏が加わり、質疑応答や日米の教育の違いなどについて議論が交わされた。まず、日本側から pwn.college の難易度の高さを懸念する声が上がった。米国側もこのことは承知しているようだった。pwn.college に登録した ASU の学生は 150 名ほどで、その中から黄帯に昇級した学生が 14 名、青帯は 6 名とのこと。来期は、黄帯と青帯をベーシックとアドバンスのような形で 2 つの講義に分けたり、カリキュラムの内容を見直すなどして改善を図りたいと述べた。一方、米国側からは、ローカルな CTF 大会が多い日本の状況をうらやむ声も聞かれた。

pwn.college の講義スタイルが米国でも特殊だということはショシテイシヴィリ氏も自認している。しかしながら、コロナ禍で対面授業ができないことから、講義を動画に収録したり、生徒とのコミュニケーションに Discord を使ったりするなど、フルオンライン化を進めた結果、世界中に開かれた教育システムというイノベーションを実現することができたと力説する。今後は、Web・暗号・デジタルフォレンジックといった対象分野の拡大を検討しており、協力可能な組織を広く募っているとも語った。

おわりに

筆者も実際に pwn.college にアクセスしてみた。何よりも膨大なチャレンジの数に圧倒されるのだが、一方でチャレンジを起動してみると、丁寧なコメントがあり、生徒に対する細かな配慮も感じられた。もちろん、筆者にバイナリ解析の知識はなく、接したチャレンジも初歩の 1 ～ 2 問ほどだった。しかし、コンテンツが作り込まれていることは十分に感じられ、講義の動画を見ているとチャレンジしてみようという気持ちも強くなった。

バイナリ解析は CTF の中で最も専門性が高い分野だ。問題を解くには CPU・アセンブリ・プログラミングなど幅広い知識が要求される。大学・大学院などでコンピューター科学を勉強をしてきた人や、趣味や仕事でプログラミングをしてきた人ならば、この世界にも抵抗なく入ることができるかもしれない。だが、そうでない人にとって、このハードルは極めて高い。これまでなら、プレイヤーが書いた WriteUp（解答例）を読むなどして勉強してきたと思うが、問題の難易度にばらつきがあったりドキュメントが点在したりして、まとまったものは存在していなかった。その意味から考えると体系的な教材はありがたい、しかも無償だ。開発に携わったショシテイシヴィリ氏とネルソン氏に感謝して使わせてもらうことにしよう。

2020 年度を振り返る

ニューノーマル時代で顕在化したサイバー空間における問題

文＝佐久間一輝、江頭誠

はじめに

2020 年度は、新型コロナウイルス感染症(COVID-19、以下コロナと表記)の感染拡大に伴い、リモート勤務の推奨など働き方も大きく変化し、ニューノーマル（新しい生活様式）への移行が急速に進んだ 1 年だった。そして、攻撃者は、このような状況に乗じてさらなる攻撃を仕掛けてきている。例えば、保健所や厚生労働省などの実在する公共機関を装い、コロナに関した内容を騙るフィッシングメールなどの被害が発生している。

本稿では 2020 年度におけるサイバー空間の問題（以下、サイバー問題と表記）を紹介する。前半では、コロナ感染拡大に伴い、ニューノーマル時代で顕在化したサイバー問題に焦点を当て、後半では、ニューノーマル時代が顕在化の理由ではないものの、今後も継続して注意が必要だと考えるサイバー問題について、その概要を紹介する。

ニューノーマル時代で顕在化したサイバー問題

2020 年度は、コロナの感染拡大に伴いニューノーマル時代の生活様式が取り入れられ、この社会動向に便乗したサイバー攻撃が数多く発生した。また、リモート勤務での業務が多くなったことで、従来のセキュリティモデルでは攻撃を防ぐことができない問題も見られ、「すべての通信アクセスを信頼しない」という考えに基づいた新たなセキュリティモデルが注目を集めた年でもあった。

ここでは、ニューノーマル時代で顕在化したサイバー問題を取り上げる。

新型コロナウイルス感染症に便乗した感染症対応機関を騙るサイバー攻撃

コロナの感染拡大に便乗したサイバー攻撃が多数観測された。国内では、保健所、厚生労働省、国立感染症研究所などの感染症対応機関を装ったフィッシングメールや Emotet(マルウェア) が添付されたメールが確認された。また、海外では、ワクチンを開発している製薬会社が保有する機密情報の窃取を目的としたサイバー攻撃も確認されている。

攻撃者は、社会的な関心に便乗しサイバー攻撃を仕掛けてくる。コロナは未だ収束していないため、2021 年度も引き続き感染症対応機関を騙ったサイバー攻撃の発生が予想される。例えば、日本国内においてもコロナのワクチン接種を謳ったサイバー攻撃の発生などが懸念されるため、注意が必要と考える。

リモート勤務増を狙ったオンライン会議ツールへのサイバー攻撃

コロナの感染防止の観点から、出勤率を下げるためにリモート勤務が推奨された。その結果、オンラインでの会議形態が必要となったため、オンライン会議ツールが多く使用されるようになった。しかし、一部のオンライン会議ツールには、会議室の URL を知っていると誰もが参加可能 (URL の推測が可能) な問題が存在した。攻撃者はこの問題を悪用し、勝手に会議に参加し、悪意のある画像や動画を共有するといった攻撃を行なった。

この問題は、利用者の利便性とセキュリティ対策のトレードオフに起因すると考える。サービス提供者側は、問題の発生を予測するなど、サービ

ス設計時点で注意を払うことが重要と考える。一方、新たなツールの利用が普及してきた際には、攻撃者もその状況を察知し、攻撃対象として狙う可能性があるため、利用者も、ツールが提供するセキュリティ設定を確実に行なうなど注意を払いたい。

リモート勤務下での従来セキュリティモデルの不備を狙ったサイバー攻撃

リモート勤務推進に向けた政府の取組みもあり、リモート勤務の利用率が増加したが、そこを狙った攻撃が見られた。国内企業において、従業員がリモート勤務で利用している業務用端末を社内の管理されたネットワークを経由せず、直接社外ネットワークへ接続することもある。この時、SNS の利用などを通じてマルウェアに感染してしまい、その後、当該従業員が出社した際に感染した PC を社内ネットワークに接続することで、社内へマルウェアの感染が広まる問題が発生した。

企業のセキュリティ対策における従来の考え方は、ネットワークの内側は信頼でき、外側は信頼できないというモデルに基づくものだった。しかし、このモデルでは前述のような事案を防ぐことが難しい。こうした状況を鑑みて、新たなセキュリティモデルである「ゼロトラストセキュリティ」というキーワードが大きな話題となる年でもあった。

リモート勤務増に伴う VPN 製品を狙った不正アクセス

先述のとおり、2020 年度のリモート勤務利用率は増加した。それに伴い、リモート勤務を行なうために欠かせない VPN 製品のぜい弱性を悪用する攻撃が多くみられた。攻撃が成功した場合、VPN の認証情報が不正アクセスにより窃取されるだけでなく、インターネット上に公開されることもあった。

これらの攻撃に悪用されたぜい弱性の修正パッチは、2019 年に公開済であり、最新パッチを適用していれば、攻撃者からの攻撃を防ぐことができた問題である。パソコンのみならず、IoT 製品などの周辺機器に関するセキュリティ情報を日々収集し、常に最新の状態に保つことを心掛けるべきである。

ニューノーマル時代との関連はないが今後も注意が必要だと考えるサイバー問題

例年発生しているランサムウェア攻撃や不正アクセス、IT 基盤停止による業務停止などのサイバー問題は、ニューノーマル時代でも変わることなく発生していた。

ここでは、ニューノーマル時代への移行に関係なく 2020 年度に発生したサイバー問題の内、被害が大きく今後も注意が必要だと判断したものを取り上げ、概要を説明する。

セキュリティの不備を狙ったキャッシュレスサービスの不正利用

経済産業省が 2020 年 12 月に報告した調査結果によると、約 4 割の消費者がキャッシュレス決済サービスを利用しており、その数は増加傾向にあるという。その変化に伴い、多くのキャッシュレスサービスが提供されている。その中で、2020 年に新設されたキャッシュレスサービスのセキュリティ不備が悪用され、キャッシュレスサービスに紐づけられた銀行口座から不正に預金が引き出されるなどの被害が相次ぎ発生した。

海外拠点を起点とする国内大手企業への不正アクセス

国内の企業において、海外拠点を起点とした不正アクセス事例が散見された。不正アクセスの被害に遭った企業の中には、社内の機微な情報が流出した恐れのある企業もあった。また、サービスの提供を終了している顧客の情報が含まれているサーバーを攻撃され、サーバーに保管されていた情報が漏えいするといった問題も発生した。

クラウドサービス障害に伴う大規模システム停止被害

国内の組織は業務システムを自社内ではなく外部のクラウドに設置するケースが増えている。しかし、利用しているネットワークやクラウドに障害が発生すると、従業員や一般の利用者はそのサービス、業務システムを利用することができなくなるケースが存在する。2020 年度は前年度か

ら引き続き、多くの利用者をかかえる大手クラウドサービスに障害が発生したことで、メールサービスや電子マネーサービスなど、クラウドを用いて提供されていたサービスが停止するなど、深刻な被害をもたらした。

おわりに

2020 年度は、コロナの感染拡大に伴うニューノーマル時代への変化の年であった。サイバー空間においては、ランサムウェア攻撃や標的型攻撃のような従来のサイバー攻撃に加え、ニューノーマル時代に必要なリモート勤務環境を狙った攻撃の発生も見られた。また、ニューノーマル時代における、従来のセキュリティモデルでは対策できないリスクへの対処を行なうため、「ゼロトラストセキュリティ」が話題になった年でもある。

2021 年度もニューノーマル時代での生活様式が続くため、2020 年度に増加したオンライン会議や VPN へのサイバー攻撃などは引き続き注意が必要である。加えて、コロナ終息後に生活スタイルの変化が再び起こった場合、その変化を狙った攻撃や、東京オリンピック・パラリンピックの開催といった社会的なイベントに便乗したサイバー攻撃の発生も予想される。攻撃者はその時々の世界情勢を利用してサイバー攻撃を仕掛けてくるため、注意が必要である。

今後も最新のサイバーセキュリティに関する情報を日々収集し、迫りくるサイバー攻撃の変化を迅速に察知し、配信していきたい。

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.42

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