



INTERNET YOU



SecureWorks Japan株式会社 Counter Threat Unit 中津留勇

セキュリティインシデント対応支援業務、マルウェア分析・対策研究業務を経て、2016年3月から現職。現在はSecureWorksのリサーチチーム、Counter Threat Unitの一員として、最新のサイバー攻撃の調査研究を行うとともに、インシデント対応および関連するマルウェア等の解析業務に従事している。セキュリティ啓蒙活動にも力を入れており、WASForum Hardening Project実行委員、Internet Weekプログラム委員、セキュリティ・キャンプ全国大会講師などを務める。



▲セキュリティ専門家としてコメントする中津留さん



▲中津留さんが低温調理で作った牛カツ



▲SECURITY CONTEST (secccon) 2017国内決勝大会



セキュリティ分野におけるコミュニティでも大活躍されているSecureWorks Japan株式会社の中津留勇さんにお話を伺いました。プライベートでは、スマートスピーカーやIoTデバイスのカスタマイズに凝っているそうで、ご自身を「テクノロジーやインターネットが好きすぎる人間」と評する中津留さんに、現在の仕事に進まれた経緯や、社内外の活動を通してめざしているものについて、語っていただきました。

中津留さんがインターネットに興味を持ったきっかけ

小学生の頃は家にPCはありましたが、インターネットというものにきちんと意識をもったのは中学生の頃です。当時は、Yahoo!のディレクトリ検索で、モーニング娘。の最新情報をいち早く入手する、ライトユーザーでした。そうしているうちにPCに興味が出てきて、やりたいことだけをやりたい子だった自分は、母親の勧めで福岡の高専に進みました。そこでインターネットそのものに興味を持ちました。

高専で学んだことや、これまでのキャリアについて

高専は、そもそも“物事がどう動くか”を勉強するところです。プログラムやコンピュータの基礎も高専で学びました。通っていた高専には授業のためPCを1人1台購入する決まりがあり、インターネット接続し放題だったので、暇さえあればネットを徘徊し、遊ぶことで知識を深めていきました。ある日、PCが変な動きをするなどと思い再起動したら、システムファイルが全部消去されるという経験をしました。世の中にはコンピュータウイルスというヤバイものがあることを知り、「セキュリティ」を意識するきっかけになりました。ファイルが消されPCが起動しなくなったとき、まず動作として面白いという驚きと、自分が詳しくならないと引がかかってしまうという気づきを得ました。そこからは、IPAの資格試験を受けたり、Security Akademeiaなどの有名サイトを読みだりして、インターネットを支える技術について勉強するようになりました。

高専を卒業する頃には、東京で自分のITスキルを生かして就職することを考えました。推薦企業の中に株式会社ラックが載っていて、「インターネットのセキュリティ事業を営んでいる」とありました。セキュリティと聞くと警備のような物理的なものしか思い浮かばなかったのが、攻撃を防ぐという考え方が目から鱗でした。ラックに入社してから半年間は、さまざまな業務に触れながら、ひたすらインターネットセキュリティについて勉強していました。そこからJPCERTコーディネーションセンター(JPCERT/CC)に出向になりました。JPCERT/CCでは、インシデント対応支援を1年ほど担当し、その後分析センターという部署で今の専門であるマルウェア解析を担当しました。インシデント対応では日本に関係したさまざまなサイバー攻撃について学ぶことができ、また分析センターでは踏み込んだ複雑な技術に触れることができ、面白かったです。

出向を終えてラックに戻り、マルウェア対策の研究に1年半ほど携わった後、今度は正職員としてJPCERT/CCに約3年勤めました。JPCERT/CCで海外との繋がりを持つ中で、将来海外に住みたいという気持ちや、高度な技術者が多数いる海外の環境に行ってみたいという気持ちが強くなりました。そんな中、Secureworksがサイバー攻撃の面白い解析結果を出しているのを

見て興味を持ったところに、たまたまお誘いをいただき転職を決意しました。私生活では、結婚して子どもができたこともあり、リモートワークできることも魅力の一つでした。まさにご縁があった訳です。

Secureworksでは、世界中のサイバー攻撃をリサーチする専門部隊であるCounter Threat Unitに所属しています。その中で、特に日本のサイバー攻撃に注目してリサーチを行い、その結果を自社サービスへ還元したり、インシデント対応やSOCのサポートもしたりします。また、対外的な活動を通してプレゼンスを上げるとともに、日本全体を良くしていく活動も重要な役割です。自分が担う日本のサイバー攻撃のリサーチ結果が、世界的に使われていると思うと感慨深いし責任もあります。

インターネットセキュリティ、そしてコミュニティへの思い

セキュリティの考え方について、時代が変わってきたなと感じています。サイバー攻撃、特に標的型攻撃においては、マルウェアは一つの要素でしかありません。インシデントを把握するためには、エンドポイントの監視や、正規の手段でのアクセスにおける悪意の有無を判定することも重要です。例えばマルウェア解析の話をするときに「マルウェア解析そのものの面白さ」に興味を持つ方が多いのですが、解析作業は対策の中の一つの要素に過ぎないと理解しておかないといけません。セキュリティにおいては「多様な目線」が一番大切です。

コミュニティ活動には、マルウェア解析技術を高めていったことでお誘いいただくことが増えていきました。Internet WeekではJPCERT/CCにいた2014年からプログラム委員を務めています。コミュニティ活動で多様な背景を持つ人と関わることは勉強になり、人脈も広がりました。社外でしか経験できないことも多く、会社のビジネスにも還元できています。コミュニティ活動を頑張る人は、日本全体を良くしたい思いを持つ人が多く感じているのですが、私自身も、「世界平和」をまじめに考える性質であるため、時間の捻出は大変ですが、続けていきたいと思っています。

最後にインターネットに対する愛情のこもったメッセージをお願いします!

地球は広いですが、インターネットは距離を感じさせなくする技術です。2歳になる自分の娘も含め、これからもみんなが使っていく、大好きなものです。自分は、いわゆるネットワークを作るエンジニアではありませんが、大好きなインターネットを維持するために、セキュリティの分野であれば活躍できると自負しています。日本ひいては世界中の人が、安心してインターネットを使うように取り組んでいきたいです。