LAC

サイバーセキュリティ仕事ファイル②

～みんなが知らない仕事のいろいろ～

株式会社ラック

もくじ

はじめに

こんにちは！株式会社ラック サイバー・グリッド・ジャパンの高橋です。

ようこそ、サイバーセキュリティの世界へ！

早速ですが、『サイバーセキュリティ仕事ファイル 1』を読んでくれましたか？読んだ人から「こんなにサイバーセキュリティの仕事があるなんて知らなかったよ」という声をたくさんもらいました。また、「他にどんなサイバーセキュリティの仕事があるのかな？」という声もたくさんもらいました。

そこで、この『サイバーセキュリティ仕事ファイル 2』を作りました。たくさんあるサイバーセキュリティの仕事の中から、サイバーセキュリティを語る上で外せない仕事、前から紹介したいと考えていた仕事、近い将来皆さんが関わるかもしれない学校の仕事などをピックアップしました。

今回もサイバーセキュリティの仕事をしている人にインタビューをしたのですが、私も名前しか聞いたことがなかったけれど、インタビューをすることで知ることができた仕事もありました。仕事で起きた大変な出来事や面白い体験など、いろいろなお話を聞くことができました。

協力してくれた人のお話を思い出しながら、これを読む皆さんがサイバーセキュリティの仕事を想像できるような文章を目指しました。また、文章だけだと分かりにくいので、少しでも仕事をイメージできるようにイラストも載せました。

このページを開くと、いよいよ仕事の紹介が始まります。ページを開くと左側には仕事の説明が載っています。右側にはその仕事についてインタビューを受けてくださった方の仕事についての考え方やエピソードなどが載っています。読んでいくと、サイバーセキュリティの仕事の裏側をのぞくことができますよ。

サイバーセキュリティを知る第一歩として、『サイバーセキュリティ仕事ファイル 1』と併せて読んでみてください。そして、「サイバーセキュリティについてもっと知りたい」と思ってもらえたら、とてもうれしいです。

さあ、世の中を守るサイバーセキュリティの仕事を一緒に見ていきましょう！

将来の予測が難しい社会を生き抜く力を伸ばします

高校情報科の先生

情報を正しく使う人を育てる案内人

皆さんの周りには、どんな先生がいますか？小学校の先生、中学校の先生、部活の先生、塾の先生などがいますよね。高校にも先生がいます。そして、高校にはサイバーセキュリティに関する授業を行う先生がいます。そこで、今回はサイバーセキュリティに関する授業と、担当する先生の仕事について紹介します。

サイバーセキュリティに関する授業は「情報科」という授業で行われます。情報科は「情報Ⅰ」と「情報Ⅱ」の二つがあります。この中からサイバーセキュリティに関する授業を取り出すと、次のようになります。情報社会の問題解決（情報セキュリティの重要性を理解する）の授業。情報通信ネットワークとデータの活用（情報セキュリティを確保する方法について考える）の授業。情報とデータサイエンス（たくさんのデータを集めて分析することが情報社会に役立つことを理解する）の授業。高校の内容なので小中学校の皆さんには少し難しいですが、「情報社会」「情報セキュリティ」「データの活用」「データの分析が情報社会に役立つ」という言葉から、サイバーセキュリティに関係していることが分かると思います。

情報科の授業を担当する先生は、学校の中にあるコンピュータ、インターネットを使うためのネットワーク、さまざまな情報システム（情報を保存・取り扱い・伝えるための仕組み）を管理することを任せられることもあります。そして、他の科目を担当する先生が授業でコンピュータやプロジェクタ、電子黒板などを使うときに相談を受けることもあります。

01

情報科の先生は学校の先生ですからクラス担任をしたり、文化祭や修学旅行などの学校行事を担当したりします。また、高校を卒業したら大学か短大、高等専門学校に進学するのか、会社に就職するのかなどの進路について相談に乗ったりアドバイスしたりします。他には、部活動の顧問を担当することもあります。

実際の高校情報科の先生のお話

この仕事のやりがい

情報科の先生をしていると、生徒がコンピュータや情報通信ネットワーク、情報セキュリティなどについてどんどん力を付けていく姿を間近で見ることができます。そして、そのサポートに関われるのは、とてもやりがいのある仕事だと思います。

この仕事の難しいところ

難しいところは、情報の授業でやるべきことがとても多いことです。学校にいる先生の中で、情報の先生は１人だけということがあります。そのため、１人で１年生から３年生まで教えなければなりません。とても大変ですが、先生としてたくさんのスキルを身に付ける努力をしたり、よりよい授業になるように工夫をしたりしています。

最後に一言

「人と人とのつながりを大切にする学校の先生の仕事って、いいかも！」と思ってくれる人が一人でも増えるとうれしいです。

この仕事でうれしかったこと

生徒にSNSや地図などのアプリ、コンピュータやスマートフォンなどの便利な使い方を教えていると、「そんな便利な機能があるの？　先生すごい！」と言われることがあります。「いやいや、すごいのはコンピュータだから」と答えるのですが、生徒が驚いたり、何か発見したりする姿を見るとこちらもうれしくて、ワクワクしますね。

必要な資格や能力

必要な資格は、情報科の教員免許状（情報科の先生教員になるための資格）です。教育系の大学や工学系の大学などで取ることができます。この資格を取って、採用試験（学校で働くための試験）に受かる必要があります。

生徒に勉強を教えることや、生徒のために行動するのが先生の役割ですので、必要な能力は責任感、物事をやり遂げようとする気持ちです。もちろん、生徒を想う気持ちも大切です。

お話を聞いた人

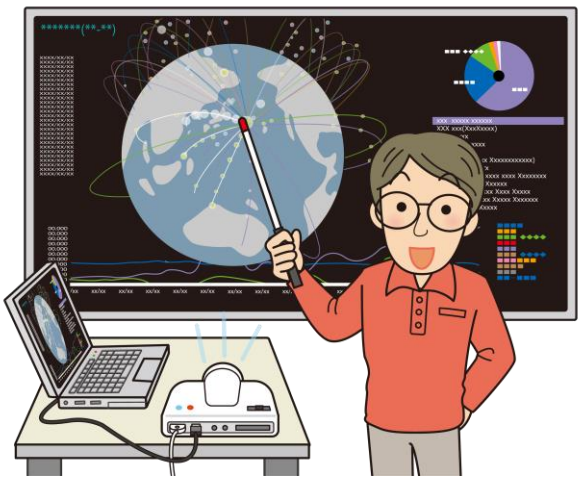
阿南 統久さん

（茨城県立ＩＴ未来高等学校　令和５年４月開校）

サイバーセキュリティの種をまいて
成長を見守ります

大学教授

サイバーセキュリティで大学を支える先生



大学の先生の仕事というと、「教えることかな？」と思うかもしれませんが、大学の先生の仕事はそれだけではありません。今回はサイバーセキュリティに関わる大学教授の大切な役割である、「サイバーセキュリティで大学を守る」仕事を紹介します。

サイバーセキュリティで大学を守るため、サイバーセキュリティに関わる大学教授は、大きく分けると四つの任務に取り組む必要があります。

一つ目は、大学の学長や教職員にサイバーセキュリティの重要さを知ってもらい、サイバーセキュリティについて学んでもらうことです。何かセキュリティの問題が起きてしまった後で、大学で働いている人たちがその重大さを知っても遅いのです。ですから、その前に事の重大さを理解してもらう必要があります。そうしないと、問題を直ぐに解決することが難しくなってしまいます。

二つ目は、大学生にもサイバーセキュリティについて学んでもらうことです。大学生は勉強や就職活動にインターネットを使うことが多いのですが、前もってサイバー攻撃などについて学んでいれば、もし被害を受けても直ぐに教職員に助けを求めることができます。

三つ目は、大学で起こるさまざまなセキュリティの事件に中心となって対応することです。例えば、サイバー攻撃に対応するチームを大学内に作ったり、大学がサイバー攻撃を受けてしまったときにそのチームと一緒に何が起こっているかを確認して原因を見つけて、解決したりします。

四つ目は、大学全体のセキュリティに関することを決めることです。大学で起きそうなセキュリティの事件をいくつか想定して、事前にそれらを「とっても危険！」や「それほど危険ではない」などに分けたり、実際にセキュリティの事件が起きたときの解決方法や誰に連絡するかを決めたりします。

また、最高情報セキュリティ責任者（CISO）と呼ばれる仕事をしていることもあります。CISOについては、後の仕事ファイルで紹介しますね。

実際の大学教授のお話

この仕事のやりがい

私は大学で特任教授として、大学が初めて取り組むサイバーセキュリティに関わる事を全て担当しています。初めての取り組みなのでとても難しいですが、協力してくれる人たちのおかげで全てがやりがいになっています！

この仕事の難しいところ

私が所属する大学には、教職員と大学生合わせて約1万3,000人います。そして、毎年約3,000人が大学に入学しているのですが、サイバー攻撃などから全員を守らなければならないことがとても難しいです。

大学に入学してくる学生にサイバーセキュリティについて学んでもらう方法をずっと考えていたのですが、2022年度に新入生向けのサイバーセキュリティのビデオを作ることができました。このビデオを見て被害に会わないように気を付けることや、もし被害にあってしまったときにどうすればよいかを学んでほしいです。

最後に一言

楽しく・正しく、そして、賢くインターネットを使いましょう！

この仕事で面白いと思うところ

この仕事の全てが面白いです。大学でサイバーセキュリティが当たり前になるように、最初はさまざまな新しいことに挑戦してきました。その結果、ここ数年で多くの人たちにサイバーセキュリティの大切さを知ってもらうことができたと思います。また、サイバー攻撃などのセキュリティの事件に対応できる人が何人もいるため、もし何か起きてもその人たちとチームを組んで対応できるようになりました。

必要な資格や能力

教授になる場合は、博士号と呼ばれる最高レベルの学位（大学や大学院を卒業するときに与えられる）が必要なことが多いです。私の仕事は特任教授という名前ですが、博士号は必要ありませんでした。

必要な能力は、リーダーシップ、コミュニケーション能力、物事がうまくいくように調整する力です。そして、私のように今までの仕事の経験全てがサイバーセキュリティの仕事に生きていますので、さまざまな仕事の経験があればきっと役に立つと思います。

お話を聞いた人

佐藤 豊彦さん

（国立大学法人鹿児島大学 兼 株式会社ラック）

新しい世界を創造します

サイバーセキュリティ研究者（技術）

インターネットの未来を守る職人

「研究」という言葉で想像するのは、夏休みの宿題として出される自由研究ではないでしょうか。自由研究のテーマを何にすればよいか悩んだことがある人はきっといると思います。自由研究ですから、自分の興味のあることや好きなことについて調べたり、作ったり、実験したりするなど、さまざまでしょう。

では、仕事としての「研究」は、どのようなことをすると思いますか？

研究を仕事としている研究者も興味のあることや好きなことを研究しています。研究のテーマはさまざまですが、サイバーセキュリティの研究者は皆さん以上に想像力を発揮して、未来のために役立つようなことをいつも考えています。

そんな研究の中でも、インターネット上で皆さんを守る技術を研究する仕事、サイバーセキュリティの技術研究者の仕事を紹介します。インターネット上のトラブルに巻き込まれないように危険なWebサイトをブロックするフィルタリングの他に、皆さんの身の回りにはサイバーセキュリティの技術がたくさんあります。例えば、攻撃する者に気づかれない方法でサイバー攻撃を見つける方法を試したり、パソコンやスマートフォンの中にあるコンピュータの心臓と呼ばれるCPU（Central Processing Unit）でマルウェア（悪さをするプログラム、ウイルスとも言います）を見つけるものを作ったりするなど、未来のために役立つような技術の研究をしています。

「新しい方法を思いついた！」「この問題を解決する研究をしたい！」となったときに、サイバーセキュリティの技術研究者はどうすればうまくできるかを考えます。そして、その研究に関係がありそうな日本や海外の論文（研究の結果が書かれた文章）を読んで、他の人が同じ研究をしていないかを確認したり、ヒントをもらったりします。

次に、研究に必要な情報や資料を集めて十分な知識がたまったら、実験をしたり試しに作ったりします。うまくいかない場合は原因を探して、結果が出るまで何度も何度もやり直します。最後に、結果を論文にまとめて発表します。

このように、サイバーセキュリティの技術研究者によって、今よりも安全で早く、便利にインターネットを使うことができるようになります。

実際のサイバーセキュリティ研究者（技術）のお話

この仕事のやりがい

簡単にできないからこそ、研究することがやりがいであると考えています。サイバー攻撃の方法は常に変化していくため、あれこれ工夫することが必要です。試したことがうまくいくか、良い結果が出るかは分からないため、とても手ごわいですが、そのために飽きることがありません。

この仕事でうれしかったこと

成果が見えたときです。例えば、動かないものが動いたときや今までできなかったことができたときは、とてもうれしいです。

私はハードウェア（コンピュータなどの機械）を使ったセキュリティの技術について研究をしていますが、もともとは「こんなことができたら世の中の役に立つだろうな」という思いつきから始めました。最初のうちは、思いついた方法が実際にできることなのかどうかも分からずに進めていました。少しずつできることが増えていき、ついに動くハードウェアが完成したときはとてもうれしかったです。

必要な資格や能力

サイバーセキュリティの国家試験である情報処理技術者試験など、情報関係の資格を持っているとよいと思いますが、必ず必要であるということではありません。

それよりも、研究者はコツコツ続ける力や、「何でだろう？」と一生懸命に考えて原因を見極めようとする力が必要です。また、研究の結果を論文にまとめなければなりませんので、さまざまな情報を整理してみんなが理解できるように説明することができる力も大切です。

最後に一言

キャラクターやロボットを動かすプログラムを作ってみましょう！ 技術はやればやるほど手も頭も覚えてくるため、学校の授業でも興味を持って一生懸命にプログラムを作ってほしいです。それが将来の研究者への道につながります。

お話を聞いた人
加藤 雅彦さん（長崎県立大学）

まだ誰も知らない守り方を見つけます

サイバーセキュリティ研究者（社会心理学）

安心・安全な未来をつくる研究者

サイバーセキュリティの研究者をこの一つ前のページで紹介していますが、他にも紹介したい研究者の仕事があります。それは、サイバーセキュリティについて社会心理学の分野から研究する仕事です。社会心理学とは、人のさまざまな行動を理解することや、人がこれからどのような行動をとるのかを研究することです。

でも、人の行動についての研究は、一体何をするのでしょうか？人をよく観察すればよいのでしょうか？

サイバーセキュリティについて社会心理学から考える研究者は、サイバーセキュリティのルールや技術が人にとって守りやすいものかどうか、たくさんの人が交流するSNSなどによるインターネット上のトラブルにはどんな問題があって、どのような対策ができるかなどを見つけます。

人がルール違反したりトラブルを起こしたりするきっかけが分かれば、それを事前に防ぐことができるかもしれません。そのために、たくさんの人にアンケート調査や実験に参加してもらうことで、サイバーセキュリティに関する人の行動を明らかにします。

このような研究によって見つけた新しいことや考え方をサイバーセキュリティに生かすためには、ある問題がすでに他の研究者によって解決されていないか、日本や海外の論文（研究の結果が書かれた文章）を読んで確かめた上で研究することを決める必要があります。

研究することが決まったら、まず、論文やレポート（調査した結果が書かれた文章）をくわしく読み、まだ解決されていないことを見つけます。次に、実験や調査を通して「今あるものを、もっと便利にすること」「今ある問題を新しい仕組みで解決すること」などについて研究していきます。最後に、研究の結果を正確で分かりやすい文章にして論文にまとめ、世界中の研究者と共有します。

このように、サイバーセキュリティの社会心理学研究者によって、人が守りやすく使いやすいサイバーセキュリティを広めたり、インターネット上での人同士のトラブルを防ぐ対策をしたりして、今よりも安全にインターネットを使うことができるようになります。

実際のサイバーセキュリティ研究者（社会心理学）のお話

この仕事のやりがい

私はディスインフォメーション（インターネットにばらまかれる本当かうそか分からない情報）の研究をしています。残念なことに、世の中には本当かうそか分からない情報や正しくない情報があふれていますが、そのような情報に振り回されたり、惑わされたりしないような社会にすることが目標であり、やりがいです。皆さんがインターネットを通じて誰かにあやつられない、誘導されない、惑わされない社会にしたいです。

この仕事の難しいところ

絶え間なく研究を積み重ねていくことです。そして、見つけたことを論文として書いたり発表したりすることも難しいです。自分が何の研究をしている研究者なのか、サイバーセキュリティの専門家に認めてもらうことがとても難しいです。

論文はどんなものでもよいというわけではなく、質の高さ（信頼できるものであること）が求められます。そのため、「これまで世の中になかった新しい研究であること（新規性）」「使いやすく役に立つこと（汎用性）」「正確であること（信頼性）」の三つが求められるのですが、これらがきちんと示されている論文を書くことがとても難しいです。

この仕事でうれしかったこと

私の研究が「将来的に必要なものである」と言ってもらえたことがありました。そのときはとてもうれしかったです。

必要な資格や能力

必要な資格はありません。その代わりに、大学や大学院などで研究のやり方をしっかり学ぶことが大切です。どんな研究でもよいです。研究の結果を分かりやすく書くための知識や経験は、研究者となって論文を書くときに100%生かすことができます。

必要な能力は、何事に対しても問題意識を持つことと、当たり前のものをなぜ当たり前なのか疑うことです。興味あることについて疑ってみるようにすると、「どうしてこうなっているの？」「違うやり方があるのではないかな？」と考える習慣がつき、研究につながっていくと思います。

最後に一言

日本の未来の安心・安全なインターネット空間を一緒につくっていきましょう

お話を聞いた人

鈴木 悠さん（株式会社ラック 兼 情報通信研究機構）

インターネット時代の転ばぬ先の杖

弁護士

困っている人に寄り添う法律の専門家

この『サイバーセキュリティ仕事ファイル2』のもくじ（2ページ目にあります）を見て、サイバーセキュリティの仕事の中に「弁護士もあるの？」と思った人がいることでしょう。

弁護士はどんな仕事をしていると思いますか？と聞かれると、「困っている人を助ける」「弱い人を守る」といったことを想像するのではないでしょうか。実は、弁護士はインターネットやサイバーセキュリティに関わる仕事もたくさんしています。今回はその中の二つを紹介します。

一つ目は、インターネットやコンピュータをめぐって問題に巻き込まれていたり、困っていたりする人から相談を受けることです。インターネットやコンピュータに関わる相談は、オリジナルのもの（自分で作ったもので他にないもの）やアイディア（考えや発想）で価値があるもの（「知的財産」と言います）やインターネットやコンピュータを使う技術に関するものなどがあります。例えば、「自分が作ったオリジナルのものを他の人が勝手に使っていることをインターネットで発見したので、使わないようにしてもらいたい」や「ある会社にソフトウェア（コンピュータを動かすプログラム）を作ってもらう約束をしたけれども、決められた日を過ぎても終わらないため困っている」などの相談を受けます。

相談を受けたら、まず相談者から詳しく話を聞いて、SNSの書き込みやWebサイトなどで本当に相談内容のことが起こっているかを確認します。そして、相談内容が本当に問題といえるのか、困ったことをしている人に「やめてほしい！」と言えるのかを判断します。判断できたら、困ったことをした人の情報をSNSやWebサイトの運営会社から出してもらい、困ったことをした人に連絡して解決に向けて動きます。でも、どうしても話がまとまらないときは、裁判（裁判官がお互いの言い分を聞いて法律により結論を出すこと）になります。

二つ目は、NGO活動（お金を儲けることを目的にせず、一般の人々が活動を行うこと）です。NGO活動では、皆さんがインターネットを安心して楽しく使うことができるように弁護士としてどんなことができるのかを考えたり、インターネットを安全に使うためのアドバイスをしたりします。

また、「それをするとなぜいけないのか？」を説明することもあります。説明するときは、法律の知識が必要になります。弁護士の仕事をしていると、実際にどんな問題があるかを知ることができるため、皆さんがトラブルに巻き込まれた場合に知っておくべきことやどうすればよいかをたくさんの人に話すことができます。

実際の弁護士のお話

この仕事のやりがい

弁護士としてさまざまな安全対策に関われることは、とてもやりがいがあります。私は小さい頃からけんかが嫌いで、前もってけんかやトラブルを防ぐ方法をいろいろ考えたいと思っていたため、弁護士になりました。毎日の生活の中で「これって変じゃない？」という感覚を大事にしているためか、よく「弁護士らしくない」と言われます。私はそれを褒め言葉だと受け止めています。

この仕事の難しいところ

正解がないということが、とても難しいです。弁護士は人を相手にする仕事ですので、これが正解！ということがありません。法律は、相手に対する『説得の技術』と言われますが、法律をもとにどのように相手を説得しようかといつも考えています。

最後に一言

興味のあるマンガを読んだり好きなゲームで遊んだりしても勉強になります。勉強には限界がありませんので、興味のあることは全てやってみてください。

この仕事でうれしかったこと

子どもたちが楽しみながら活発にインターネットを使うということに関われることが、うれしいです。私は、第二東京弁護士会の『子ども SNS 相談』で子どもたちの悩みを聞いています。また、違法・有害情報相談センターで法律の専門家として、インターネットの利用者からの相談に関する回答について、その内容を確認し、助言を行っています。

そのため、もし皆さんがトラブルに巻き込まれたり、困ったことになったりしたら、ぜひ安心できる先生や家族などに相談してほしいです。安心できるところに相談することも、セキュリティですから。

必要な資格や能力

弁護士になるには、弁護士資格が必ず必要です。

必要な能力は、国語の力とコミュニケーション能力です。法律を読み解き、人を説得させるために国語の力が必要です。そして、人の話を聞くことが重要な仕事ですので、コミュニケーション能力も大切です。

お話を聞いた人

上沼 紫野さん（虎ノ門南法律事務所）

日本のためにサイバー空間を守ります

サイバー防衛隊（自衛隊）

大胆さと繊細さを併せ持つサイバー空間の防人

「自衛隊」というと、どのような仕事をしている人たちだと思いますか？日本の上空や海上、陸上を守っている人たちのことを思い浮かべるのではないでしょうか。また、地震や豪雨などで災害が起きたときに行方不明の人を探したり、けがをした人を治療したり、車が通れるように道路に散乱した土砂などを運び出したりする自衛隊の人たちをニュースや新聞などで見たことがあると思います。このように自衛隊の任務は日本の安全と平和を守ることです。そして、自衛隊にもサイバーセキュリティの仕事があるのです。

皆さんも知っているように自衛隊には、日本の国土を守っている陸上自衛隊、日本の海を守っている海上自衛隊、日本の空を守っている航空自衛隊があります。陸上や海上、上空を守るためには情報を収集して分析し、自衛隊全体で共有することがとても重要です。そこで、自衛隊の情報システム（情報を保存・取り扱い・伝えるための仕組み）を守る必要があります。世界のどこからかサイバー攻撃を受けるかもしれないからです。この任務を果たしているのが、「サイバー防衛隊」です。

サイバー防衛隊の仕事は大きく分けて二つあります。

一つ目は、自衛隊の情報システムを 24 時間いつでも見張っていることです。昼夜問わず見張ることで、サイバー攻撃を受けたときに直ぐに対応することができます。それだけでなく、システムの守りをより強くするために必要な対策をしたり、サイバー攻撃についての最新の情報を集めたりしています。また、日本のサイバー空間を守るために、内閣サイバーセキュリティセンター（NISC）と共に、国の情報システムを守る活動も行っています。

二つ目は、自衛隊員のサイバー攻撃に対する訓練をサポートすることです。陸上自衛隊、海上自衛隊、航空自衛隊ではそれぞれで訓練していますが、より高度な訓練を行って世界レベルの能力に高めるため、サイバー攻撃を想定した訓練の支援を行っています。

サイバーセキュリティの技術を鍛えるために、アメリカ、イギリス、オーストラリアなどと一緒にサイバー対戦を行ったり、新しい情報や攻撃方法などの情報を教え合ったり、意見を交換したりして、安全・安心な世界を目指して日々訓練を行っています。

実際のサイバー防衛隊（自衛隊）のお話

この仕事のやりがい

2014年にサイバー防衛隊ができたのですが、私はその時の隊長でした。「初代サイバー防衛隊長」なんていうカッコいい呼び方を今も使っています。

サイバー防衛隊でのやりがいは、自衛隊でしかできないたくさんの経験ができることです。大きなサイバー攻撃から日本の情報システムを守ったり、サイバー空間で活動をしたりと、一般の会社ではできないさまざまなことを世界的な規模で経験することができます。

この仕事で面白いと思うところ

世界各国の仲間たちと仕事ができることが面白いです。また、サイバーセキュリティの技術で腕を競い合う大会で最高の結果を出すことができた時は、とてもうれしかったです。

この仕事の難しいところ

いつ世界のどこからサイバー攻撃を仕掛けてくるかが分からないため、どんな時でも情報システムをしっかり守らなければならないことが難しいです。サイバー攻撃を受けていることに気が付き、サイバー攻撃の状況やダメージを受けていないかを確認しないといけません。そのために、昼夜問わずにさまざまな活動をしています。

必要な資格や能力

自衛隊は入った後の教育訓練がしっかりしているため、自衛隊に入る前に必要な資格はありません。国際的に認められた情報セキュリティのプロの認定資格（CISSP）や国際的に認められた情報システムを調査するプロの認定資格（CISA）などは、自衛隊に入ってから取得することができます。

能力で必要なのは、負けず嫌いであることや、探究心（興味を持って原因を見極めようという気持ち）があることです。何よりも「サイバー防衛隊に入りたい！」という夢を持ち続けることが一番大切だと思います。

最後に一言

日本のサイバー空間の安全を守るのは皆さんです。

お話を聞いた人

佐藤 雅俊さん（株式会社ラック）

コラム１　未経験でサイバーセキュリティの仕事をすることについて

こんにちは。株式会社ラックのサイバー・グリッド・ジャパンで仕事をしている手嶋といいます。私がサイバーセキュリティの会社で働くことの楽しさや大変だと思ったことについて紹介したいと思います。

私は２年前からサイバーセキュリティの仕事をしています。その前は別の会社で「事務職」といわれる仕事をしていました。具体的にはお客様に送る文書を作成したり、社員の給料や労働時間を計算したりするといったことをしていました。ところが今は危険なサイバー攻撃を事前に防ぐために使うデータを集めたり分析したりする専門的な仕事をしています。

皆さんの中で、サイバーセキュリティに限らず専門的な仕事をしている人について「学校に通っているときから専門的な知識を勉強している」「ずっと同じ業界で働いている」というイメージを持っている人もいるかもしれません。もちろんこれに当てはまる人もたくさんいますが、私のように未経験の状態から仕事を始める人もいます。

私は事務職とはまったく違うサイバーセキュリティの会社で働くことになったため、大変だったこともたくさんありました。サイバーセキュリティの仕事で当然のように使われる言葉や、仕事で必要なツール（道具）の使い方が分からず、毎日が苦労の連続でした。また、サイバーセキュリティの情報を載せているサイトの多くが英語で書かれていることも難しく感じられる原因でした。翻訳サイトを使うことでどうにか読めるようになったものの、何か一つ調べるのにも多くの時間がかかってしまいました。

それでも働き続けたいと思ったのは、『自分なりに工夫する楽しさ』を感じるようになったからです。どうすれば手間をかけずに多くの情報を集められるかを考えたり、仕事を自動でできるようにしたり、「どうすればもっと良くなるか」を考えることがとても楽しくなりました。さらに、私自身が身の回りのセキュリティについて気を付けるようになりました。パソコンやスマートフォンに心当たりのないメールやメッセージが届いたとき「これは怪しいメールではないか」と思ったり、自宅のパソコンにもしっかりとウイルス対策のソフトを入れたりするようになりました。家族や友達にも「最近はこういう詐欺があるよ」と紹介するようにしています。サイバーセキュリティの知識を身に付けることは、身近な人を危険から守ることにもつながります。他にもサイバーセキュリティの仕事を続けたい理由があります。

一つ目は、自分に合った働き方ができることです。サイバーセキュリティを含めたIT企業（インターネットやコンピュータなどに関する技術やサービスを提供している会社）では、在宅ワーク（自宅で仕事をすること）を取り入れているところが多くあります。会社に行くことが少ないため、時間や場所にとらわれない働き方ができます。人生は長いので、生活スタイルもさまざまに変化します。引っ越し、結婚、出産、子育て、介護など。在宅ワークであれば、そのような変化にも柔軟に対応することができます。私自身も在宅ワークで働くようになり、余裕をもって家事をしたり、自分の時間を過ごすことができたりするようになりました。もちろん在宅ワークだからと言って楽な仕事というわけではありません。仕事のレベルアップのために資格を取ることや、普段からサイバーセキュリティの情報にアンテナを張っておくなど、やるべきことはたくさんあります。大変だと思うことも多いですが、とてもやりがいを感じています。

二つ目は、チームで一緒に働くことができることです。皆さんの学校でもたくさんの先生が一緒に働いていますよね。それと同じです。ただし、学校と違うのは、サイバーセキュリティの仕事はサイバー犯罪を行おうとする相手と戦うために、チームメンバーが一緒になってプログラムを書いたり、データを分析したりします。つまり、相手の考えを読み解き、その上をいく考えを導き出すことが仕事の中心になります。私は考えることが大好きです。チームで新しい考えを導き出すことにとても魅力を感じています。

サイバーセキュリティの仕事をする人が不足しているといわれますが、その中でも女性は少ないです。その理由の一つに「イメージのしにくさ」があるのではないかと思っています。それは、セキュリティの仕事を身近に感じられないからです。サイバーセキュリティの仕事をしている知り合いがおらず、具体的な話を聞く機会が少ないため、仕事の内容がイメージできないことが多いようです。

好奇心や挑戦したいと思う気持ちは、誰にでもあると思います。知らないことは難しいと感じてしまうのも、レベルアップのために勉強が必要なのも同じです。世界を見るとサイバーセキュリティの仕事をして活躍している女性がたくさんいます。

サイバーセキュリティの仕事は、誰もが知っているメジャーな仕事ではないかもしれません。しかし、会社や政府、そしてインターネットを正しく利用しようとしている全ての人をサイバー攻撃から守る大切な仕事です。このコラムを通して、皆さんの将来の選択肢の中に”サイバーセキュリティ”の仕事を加えていただけるととてもうれしいです。

（株式会社ラック　手嶋 千春さん）

悪い人から会社を知恵で守ります

サイバーセキュリティ会社の経営者

情報を守るプロ集団を束ねる指揮官

偉い人と聞いて、どのような仕事を思い浮かべますか？学校では校長先生、会社では社長、スポーツをしている人ならチームの監督、歴史が好きな人なら武将や大名を思い浮かべた人もいると思います。今回は会社で偉い人、社長について紹介します。

社長には、「経営者」というカッコいい名前もあります。経営とは、「会社を続けていくこと」という意味です。将来社長になりたい！と思っている人や実際に経営者を目指している人は、ぜひ参考にしてください。

サイバーセキュリティ会社の経営者だけでなく、経営者の仕事は会社を取り仕切ることです。やらなければいけない仕事が経営者にはたくさんあるのですが、まずは会社を続けるためにお金をしっかりと稼がなければなりません。お金を稼ぐことができなければ、働いている人に給料を払うことができず、会社を続けていくことができません。そうならないように、安定してお金を稼ぐことができる仕組みが会社にあることがとても重要です。例えば、サイバーセキュリティでお客様の情報を守る代わりに、お客様からお金をもらう約束（契約と言います）を結ぶことで、1年間分のお金を稼ぐことができます。このような仕事をどれだけ増やすことができるかがポイントです。

しかし、新しいサイバー攻撃が出てきたり、サイバー攻撃をされやすい弱いところが見つかったりと、サイバーセキュリティの世界はとても変化が激しいです。そのため、その変化にサイバーセキュリティの会社が対応できるように、知恵をしぼって新しい取り組みや仕事を始めていくことも経営者の大切な仕事の一つです。

また、人や物、情報など、会社を続けていくために必要なものがいくつかありますが、その中で経営者にとって最も重要なものは会社で働いている社員、つまり、「人」です。

07

サイバーセキュリティの会社ではサイバーセキュリティの専門家が数多く働いていますが、他にも商品やサービスを売る人や会社のお金を管理する人、会社をアピールする人など、さまざまな人が知恵を出し合って活躍しています。このようにたくさんの人に各自の能力を発揮してもらうことが会社にとってとても大切です。その人たちが成長や経験ができる場を作るため、多くの社員とたくさん話して良い関係を作ることが経営者の腕の見せ所です。もちろん、仕事のプロである社員から新しいアイディアについて話を聞いたり、仕事の相談に乗ったりすることができるように、経営者は知らないことや新しいことを勉強する努力をしています。

このように経営者は、会社に関係するさまざまな人のため、そして会社のために会社を導く指揮官なのです。

実際のサイバーセキュリティ会社の経営者のお話

この仕事のやりがい

会社には若い社員が多いため、社員の成長を見守ることがやりがいです。若い社員が活躍したり新しいことを始めたりして、より活気のある会社にしてくれることを楽しみにしています。

この仕事の難しいところ

「いかに今の仕事を壊すことができるか」が大切なのですが、逆に難しいところでもあります。このことは、サイバーセキュリティ以外の仕事にも言えるのですが、昔からある仕事が今も残っている場合、うっかりすると「このままでいいや」とずっとそれを守ってしまいます。皆さんの場合、例えば、ゲームで古くぼろぼろになった剣ではなく、新しくカッコいい剣を使いたいですよね？　私たちの会社も同じで、新しいことを始めて攻め続けられるように頑張っています。

必要な資格や能力

必要な資格はたくさんあります。例えば、日本では情報処理安全確保支援士などがあります。海外では、多くの人が憧れるアメリカのOffensive Security社の資格もありますので、興味のある方はぜひ挑戦してみてください。

必要な能力は、元気なこと、勇気があること、我慢強いことなどたくさんありますが、一番必要なのは「人の力を借りられること」だと思います。人の力を借りられる能力が大切であるということを、前の社長から学びました。自分でできることは限られているため、積極的に動いてたくさんの人を巻き込んで、それぞれが力を出せるように背中を押すことで、社員が成長すると共に、会社も成長すると思います。

最後に一言

セキュリティ・キャンプって知っていますか？もし気になったら、調べてみてください。知ると、やがて皆さんも参加したくなるかもしれません。

お話を聞いた人

西本 逸郎さん（株式会社ラック）

情報セキュリティで信頼を勝ち取ります

最高情報セキュリティ責任者（CISO）

社内のセキュリティの司令塔

皆さんは学校でタブレット端末を使って学習することが多いと思います。そのタブレット端末の中にはたくさんの情報が入っているでしょう。もし、その情報を誰かに盗まれてしまったとしたら、どうしますか？きっと、先生やお家の人に相談すると思います。

会社で働いている人も同じです。会社の大切な情報を盗まれてしまった場合、会社の情報を守っている人たちに相談します。けれど、情報を守っている人たちでも手に負えないことや、直ぐに判断できないことがあります。そんなときは、情報を守っている人たちの頼りになるサイバーセキュリティのリーダーに相談します。

そのリーダーは、最高情報セキュリティ責任者と言います。名前がちょっと長いので、CISO（Chief Information Security Officerの略）と呼ぶことが多いです。CISO がいるのはサイバーセキュリティの会社だけではありません。例えば、化粧品会社にもいます。

商品を販売している会社では、商品の値段や発売日、会社のホームページに載せている情報など、さまざまな情報がたくさんあります。もし、その情報をサイバー攻撃によって盗まれてしまったり、誰かに売られてしまったりしたら大変です。もしかしたら、そんな会社は信用できないとお客様に思われてしまうかもしれません。このようなことから、サイバー攻撃が起きたときに対応するための専門のチームを前もって作ったり、会社にあるさまざまな情報がどのくらい危険であるかを前もって調べたりして、情報の保管方法を考えるのが、CISO の仕事です。

また、CISO は情報の扱い方を決めるチームリーダーでもあるので、会社で扱う全ての情報について責任を持っています。チームメンバーと一緒に情報を守るためにさまざまなことを決めています。例えば、情報の守り方を社員に学んでもらう方法を考えたり、情報に関わる法律が変わった場合に今あるルールを見直したりしています。

ルールを変えたり、新しく作ったりしたことを、社内外にお知らせすることもしています。

もちろん、CISOやチームメンバーだけでは会社の情報を守ることができません。会社の経営者である社長やたくさんの社員の協力が欠かせません。みんなで力を合わせるために、全員をつなぐ役割も、CISOの仕事です。そのために、経営方法や法律、技術、トレンド（世の中の流れ）など、さまざまなことを知る努力がCISOには必要です。このように、CISOは会社にいるたくさんの人と一緒に、会社に関係する情報を守っています。

実際の最高情報セキュリティ責任者（CISO）のお話

この仕事のやりがい

会社にとって重要な情報を守っていることが、一番のやりがいです。情報そのものが会社の売上に影響を与えることがあり、私たちが正しく情報を扱っているかどうかをお客様はしっかりと見ていらっしゃいます。そのため、責任感を持って、CISOの仕事に取り組んでいます。

この仕事で面白いと思うところ

とても面白いのは、情報を守るには、いつも新しい情報や技術、これからのトレンド（世の中の流れ）などを理解する必要があるところです。サイバーセキュリティの世界はとても変化が速いため、最新の情報をいち早くゲットするたびにワクワクしています。

最後に一言

物事に対する使命感や正義感が強い人はぜひ、最高情報セキュリティ責任者（CISO）を目指してください。

この仕事の難しいところ

会社の情報を守ることです。コンピュータやインターネットがなかった昔とは違って、今は紙の情報ではなくデジタルで情報を扱うようになってきているため、情報がどこにあるかが分かりにくくなっています。情報をコピーされて盗まれてしまった場合、元の情報はそのままあるので、盗まれてしまったことさえ分かりません。そんなことにならないように、会社全体の情報を把握して、しっかりと守ることができるよう努めています。

必要な資格や能力

必要な資格はありません。資格よりも、何かの資格を取るために得た知識をどのように使うかを考える方が大切です。

必要な能力は、強い使命感とさまざまなことに関心を持つことです。自分が守っているものをきちんと理解して、それに対する使命感を持たなければなりません。そして、サイバーセキュリティの技術だけでなく、SNSなども含めたさまざまな情報に関心を持ち、これから起こることを予想して、情報の守り方を考えていくことができればいいですね。

お話を聞いた人
斉藤 宗一郎さん（株式会社資生堂）

セキュリティの最前線で見張ります

セキュリティアナリスト

ネットワークの門番

皆さんが学校で勉強をしたり遊んだり、家で寝ていたりしている間も、世界中のどこかでサイバー攻撃が行われています。いつどこでサイバー攻撃を受けるか分からないため、守る側は 24 時間いつでも守れるようにしなくてはなりません。24 時間対応しているサイバーセキュリティの仕事はいくつかありますが、今回はその中の一つであるセキュリティアナリストを紹介します。

「セキュリティ」は「守る」という意味ですが、コンピュータの世界では「情報を守る」という意味になります。また、「アナリスト」は「分析する人」という意味です。ですから、セキュリティアナリストは「情報を守ったり分析したりする人」を指します。

セキュリティアナリストは、ネットワーク（コンピュータやサーバをつなぐ技術）に流れているコンピュータ同士のやりとり（通信）を見張り、普段とは違う通信を瞬時に見つけて、サイバー攻撃かどうかをチェックする仕事です。通信をいつでも確認できるようにしなければならいため、数人で交代しながら 24 時間 365 日ずっと見張っています。

「会社のネットワークに流れる通信を見張ってほしい」とお客様から依頼を受けたら、お客様の会社のネットワークに通信の異常を検知するセンサーを置きます。

センサーはサイバー攻撃を検知すると「アラート」（警報）を出してサイバー攻撃を受けたことを知らせます。セキュリティアナリストは、そのアラートを確認して、サイバー攻撃が実際に効いているかをさらに細かく分析します。もし、攻撃が効いていれば、お客様にサイバー攻撃について連絡します。その後にサイバー攻撃を止めるなどの対応は、インシデントハンドラーが行います。※インシデントハンドラーについては『サイバーセキュリティ仕事ファイル 1』の 4〜5 ページで紹介しています。

セキュリティアナリストは、センサーで通信を検知するためのルールを作ることもします。攻撃されやすい新しい弱点や、サイバー攻撃の方法などが見つかったときにルールを作ります。新しい弱点が見つかったときは、実際にその弱点を攻撃して確かめて、それをもとにルールを考えることもします。

実際のセキュリティアナリストのお話

この仕事のやりがい

サイバーセキュリティの最前線で戦っていて、私たちがお客様を守っていると感じられることが、やりがいです。

この仕事の難しいところ

難しいところは、間違った対応をしないようにしなければならないことです。セキュリティアナリストは今流れている通信をリアルタイム（同時）に分析しているので、一つのミスや対応の遅れがお客様の損害につながってしまいます。

そのため、通信を見ている間は、いつも集中していなければいけません。

最後に一言

サイバー攻撃は、大きな会社や組織に対してだけ行われるものではありません。皆さん自身が被害者となってしまうことがあります。スマートフォンやインターネットを利用するときには、まずは自分を守るためにセキュリティに興味を持ってほしいと思います。

そして、自分を守るだけではなく他の人を守りたいと思ってくれる人がいれば、とてもうれしいです。

この仕事でうれしかったこと

最近の出来事なのですが、発見することがとても難しいサイバー攻撃を見つけることができました。お客様にそのサイバー攻撃について連絡し、お客様の会社のネットワークを守ることができたときはとてもうれしかったです。

必要な資格や能力

セキュリティアナリストの仕事をするために必要な資格はありません。しかし、セキュリティの資格を取得するために勉強したことは、仕事をするときに役に立つと思います。

能力としては、自分から進んで勉強することが必要です。サイバー攻撃や攻撃されやすい弱点などはすぐに新しいものが発見されるので、セキュリティアナリストは自分から情報を集めて勉強しないといけないからです。他にもいろいろな能力が必要ですが、自分から進んで勉強することができる人は、仕事をしているうちに他の能力も身についていきます。

お話を聞いた人

齊藤 大将さん（株式会社ラック）※インタビュー当時

偽サイトのない世の中を目指します

フィッシングハンター

インターネットの詐欺から守る正義の味方

皆さんは、フィッシング（Phishing）って聞いたことありますか？　「魚を釣ることかなあ」と思った人もいるでしょう。魚を釣ることを英語でFishing（フィッシング）と書きます。言い方は同じでも英語のスペル（つづり）がちょっと違いますよね。Phishing（フィッシング）は、インターネット上で行われる詐欺（人をだまして損をさせること）の一つです。サイバーセキュリティの世界ではこのフィッシングをなくすことも大事な仕事です。

フィッシングを行う悪い人はまず、本物そっくりの画面の偽サイトをつくります。そして、本物のメールにとても似ている偽メールをたくさんの人に送ります。そのメールは「急いでサイトを確認しなくちゃ！」と思わせるような内容なので、受け取った人はだまされてしまい、偽サイトのリンクをクリックしてしまいます。そうすると、偽サイトが出てきて、いろいろな情報の入力を求めてきます。その画面でユーザIDやパスワード、クレジットカードの番号などを入力させて、個人情報を盗むのです。

この偽サイトを止めるサイバーセキュリティの仕事を、フィッシングハンターと呼びます。フィッシングハンターは、本物の会社のサービスに似せた偽サイトを見つけて、お客様が偽サイトにアクセスしてしまわないようにしています。

フィッシングサイトと呼ばれる偽サイトをどうやって見つけるのかというと、新しく作られたサイトの中から本物と似ているサイトを見つけるシステムを使ったり、SNSなどで情報を集めて、その中から本物と似ている偽サイトを見つけたりします。ただ、このシステムは完ぺきではないので、見つけたサイトが本当にフィッシングサイトかどうかをフィッシングハンターが調べて判断していきます。

見つけたサイトがフィッシングサイトである事を確認したら、次は、お客様がこのフィッシングサイトを本物のサイトだと思いこんでユーザ ID やパスワードなどを入力してしまわないようにするために、フィッシングサイトにアクセスできないようにします。

例えば、インターネットにかかわるさまざまな企業や団体に「フィッシングサイトを見つけました！」と報告すると、そのフィッシングサイトにアクセスできなくしたり、フィッシングサイトにアクセスしようとすると「フィッシングサイトの疑いがありますよ！」といった赤い警告画面（アラート）を出して、アクセスしたサイトがフィッシングサイトであることを知らせたりします。また、盗んだユーザ ID やパスワードなどを不正に使おうとする悪い人たちの行動を分析して、お客様のユーザ ID が悪い人に使われないよう利用者を守るようにしています。

さらに、次のようなこともしています。フィッシングについてのお客様向けの説明サイトを作ることやフィッシングの注意を呼びかけること、他の会社と協力してお客様に注意を促すイベントを開催することなどです。こうしたいろいろな方法でお客様が悪い人にだまされないようにしています。

実際のフィッシングハンターのお話

この仕事のやりがい

フィッシングハンター同士で協力してフィッシングサイトを止めてお客様を守ることができたときに、やりがいを感じます。

必要な資格や能力

特に必要な資格はありませんが、IT やサイバーセキュリティの技術について幅広い知識を身に付けるとよいと思います。
能力としては、私たちが気付かなかったことや新しいことをライバルの会社の人たちに教えてもらえますので、コミュニケーション能力が必要です。また、ほぼ間違いなくフィッシングサイトは海外で作られるため、何が書いてあるか分かる程度の英語力があるといいですね。

この仕事で面白いと思うところ

ライバルと呼ばれる会社の人たちと助け合うことが、この仕事の面白いところです。フィッシングで困っているのは私たちの会社だけではないため、フィッシングに対抗するための情報を教え合ったり、「皆さんがフィッシングメールなどにだまされないために何ができるかな？」と一緒に考えたりしています。

最後に一言

私たちの仕事は、人をだまそうとする悪い人たちからお客様を守ることです。皆さんが安心してさまざまなサービスを利用することができるように、こういう仕事をしている人たちがいるということを覚えておいていただけたら、とてもうれしいです。

お話を聞いた人
新井 契さん（KDDI 株式会社）
平子 雅敏さん（KDDI 株式会社）

保険を通じて安心をお届けします

アンダーライター

世の中を支えるサイバー保険のコーディネーター

皆さんは自転車を持っていますか？「持っています！」という人は自転車保険に入っている人が多いと思います。自転車を運転中に万が一、転んでケガをしたときに、保険に入っていると治療費が出ます。また、車にぶつかってしまったときに、保険に入っていると修理代が出ます。今回紹介する仕事は、この保険についてです。

保険とは、たくさんの人が毎月または１年単位でお金を出し合って、病気、ケガ、火事、地震などの困ったことに備える仕組みです。大けがをしてしまってその治療にとてもお金がかかる場合、直ぐに用意できるとは限りません。そんなことになる前に、けがをしたときに必要な助けを得るための保険に入ってお金を払っていると、治療にかかるお金などを受け取ることができるのです。

保険にはさまざまな種類があるのですが、その中に「サイバー保険」というものがあります。この保険は、サイバー攻撃によって起こる困ったことに備えます。サイバー攻撃によって会社の業務ができなくなったときや、サイバー攻撃を受けた原因を調べるときに、必要な助けやお金などを受けることができます。

サイバーセキュリティの中には、サイバー保険に関する「アンダーライター」という仕事があります。実は、アンダーライターという仕事は保険以外でもありますが、今回はサイバー保険に関するアンダーライターついて紹介しますね。

サイバー保険は保険会社で扱っています。そして、サイバー保険に入るのは会社です。会社はサイバー攻撃を受けたら困るからです。会社がサイバー保険に入るとき、サイバー攻撃を受けた場合にもらえるお金や受けられるサポートの内容について決めます。このときの手助けをするのがアンダーライターです。また、サイバー保険に入りたいと考えている会社の相談に乗り、保険の内容をかためていくのもアンダーライターの仕事です。

アンダーライターは、相談を受けた会社がサイバー攻撃を受けた場合のさまざまなダメージを想像して、実際にサイバー攻撃を受けた後の調査にかかる金額やサイバー攻撃によるダメージの金額などを計算します。そして、会社はサイバー攻撃を受けた際にサイバー保険による助けやお金を受ける代わりに、その会社から毎月いくら出してもらう必要があるかを決めるのです。

サイバー保険について説明する場合、言葉だけでは分かりにくいことがあります。そのため、サイバー保険を紹介するパンフレットを作ったり、さまざまな会社で実際に起こったサイバー攻撃を集めてサイバー保険が必要であることを知ってもらう資料を作ったりします。

サイバー保険をよりよくするためのアイディアを出して、それが実際できるようにしていくのもアンダーライターの仕事です。初めてサイバー攻撃を受けてしまった会社は、何から手を付ければよいか分からず困ってしまいます。そんなときにいつでも連絡できる相談センターを作ったり、サイバーセキュリティの事件や事故が起きたときに何が起こっているかを調べてくれる会社を紹介したりして、サイバー攻撃で困っている会社のために日々、何ができるかを考えています。

実際のアンダーライターのお話

この仕事のやりがい

「アンダーライターのサポートがあってよかった」「サイバー保険に入っていて助かった」など、お客様の声をいただくことがやりがいです。

この仕事の難しいところ

サイバーセキュリティについて理解し、それから新しいサイバー保険を考えることが難しいです。これからもサイバーセキュリティについて情報を集めたり、たくさん経験を積んだりしながら、サイバーセキュリティの専門家として「お客様のために何ができるのか？」を考えていきます。

最後に一言

あらゆる人が豊かに、そして、安心して生活できる手助けができる仕事だと思います。

必要な資格や能力

特に必要な資格はありません。

必要な能力は、世の中に興味を持つ好奇心です。ニュースや新聞、インターネットなどを使って、サイバーセキュリティや世の中のことを進んで探し、知ることができるとよいと思います。そして、想像力も必要です。サイバー攻撃やサイバーセキュリティの事故によってどのような影響があるのかを想像できれば、保険で世の中のために何ができるのかを考えることができます。

能力ではないのですが、アンダーライターは計算することが多いので、算数や数学をしっかりと勉強しておくとよいと思います。

お話を聞いた人

出雲 真平さん（損害保険ジャパン株式会社）

大岡 朋代さん（損害保険ジャパン株式会社）

サイバー攻撃から会社を守る最終ディフェンスライン

インシデントマネージャー

サイバー事故対応の指示役

マネージャーという役割や仕事は、世の中にたくさんあります。部活のマネージャーや芸能人のマネージャーなどを思い浮かべるかもしれませんね。

マネージャーは「管理する人、サポートする人」という意味がありますので、ピッタリな言葉ですね。

今回紹介するマネージャーは、インシデントマネージャーという仕事です。インシデントは「事件」という意味です。このことから「事件を管理する人なのかな？」と思うかもしれませんが、実際の役割としては「事件を管理して、事件に立ち向かう他のメンバーに指示したり、サポートをしたりする人」という説明がピッタリです。

CSIRTと呼ばれる「サイバーセキュリティの事故が起きたときに立ち向かう専門チーム」の一員であるインシデントマネージャーの役割は、サイバーセキュリティの事故が起きたときに状況を確認し、CSIRT メンバーに指示を出すことです。

CSIRT メンバーが怪しい通信を見つけたら、最初にインシデントマネージャーに連絡が来ます。そして、その通信が会社のどこで起こっているか、実際にサイバー攻撃を受けているかを確認して、大変なことが起こっている可能性がある場合には、怪しい通信が起きている場所の担当者に連絡します。同時に、上司に状況を説明して、対策を考えます。そして CSIRT メンバーの役割を決めて、みんなで力を合わせて事件を解決していきます。

そして、会社内に「どんなことが起こっていて、どのような対応をしているか」を連絡し、事件を解決したら、最後にどんなサイバー攻撃が来ていて、それに対して何をしたかをまとめて、上司に報告します。

他にも、サイバーセキュリティやサイバー攻撃についての情報を集めたり、集めた情報もとに「実際にコンピュータがサイバー攻撃を受けたら、どのくらいのダメージになるか」を確認したりすることもしています。

情報によっては、会社内に「こんな情報が出ているから、サイバー攻撃を受けないように守りを固めてね」という連絡をすることもあります。

実際のインシデントマネージャーのお話

この仕事のやりがい

私はお客様を守ることが一番大切であり、お客様を守っていると実感できることが、やりがいです。私が働いている銀行は、世界にオフィスがあります。そのため、私たち CSIRT の仕事は、世界中のお客様のお金を守ることです。

この仕事の難しいところ

大きい会社ですので、みんながサイバーセキュリティの仕事をしているわけではありません。ですから、私たちが仕事でいつも使っている言葉（専門用語）を使うことができません。そのため、集めた情報をみんなが分かるようにして伝えないといけないところが難しいです。

もっと難しいのが、サイバー攻撃を受けてしまってこれ以上ダメージを広げないために、銀行の仕事を「止めるのか」「止めないのか」という判断する状況になったときです。判断は上司がするのですが、私たちは今の状況とこれから起こる可能性があるダメージを整理して、上司に報告します。このようなことはプレッシャーですが、面白いと感じる仕事でもあります。

この仕事でうれしかったこと

海外の情報を集めるために、会社の多くの海外オフィスと毎日英語で連絡を取っていました。メールには必ず「Thank You」（ありがとう）と入れていたところ、南アフリカのスタッフから「You are trying hard」（頑張っているね）という返信をもらいました。顔が見えない人とのコミュニケーションは、ちゃんと言いたいことが伝わっているか心配になることがありますが、コミュニケーションを取れたことが分かりうれしかったです。

必要な資格や能力

資格は必要ありません。でも、自分の知識や技術、行動レベルなどを確認するために取っていればよいと思う資格があります。例えば、情報セキュリティマネジメント試験（情報セキュリティを管理するための国家資格のための試験）や CISSP（国際的に認められた情報セキュリティのプロの認定資格）などです。

コンピュータの基本的な仕組みやアプリ、認証（利用者本人であることを確かめること）などの知識があると、インシデントマネージャーの仕事をするときに役に立ちます。また、私たちが日々集めている情報はほとんど英語で書かれているため、英語の読み書きは必要です。

お話を聞いた人

中村 健太さん（株式会社みずほフィナンシャルグループ）

※インタビュー当時

コラム２　CSIRT（シーサート）って何のこと？

皆さんの周りで、「スマホに変な画面が出た！」ということを聞いたことがありますか？あるとしたらサイバーセキュリティの事故か事件かもしれません。こうしたサイバーセキュリティの事故や事件、サイバー攻撃は、今この瞬間にも世界中のどこかで起きています。もし、皆さんがそのようなことになったら、どうしますか？きっと誰かに相談しますよね。大人も同じです。

では、もし会社や役所などがサイバー攻撃を受けてしまったら、どうすると思いますか？答えは、「CSIRT」が対応します。この仕事ファイルの 28～29 ページで CSIRT は「サイバーセキュリティの事故が起きたときに立ち向かう専門チーム」と説明しました。CSIRT はComputer Security Incident Response Teamの頭文字を取っています。

国や地域、会社、大学などに CSIRT が作られているのですが、人の数はさまざまです。大きな CSIRT ではたくさんの人が事件や事故に対応する準備を常にしていますが、小さな CSIRT ではなかなか専門チームに人を置くことができないため、いつもは他の仕事をしています。そして、事件や事故が起きたときに集まって CSIRT を結成します。

CSIRT では、サイバーセキュリティのオールスター（選りすぐり）と呼ばれる人たちが活躍しています。『サイバーセキュリティ仕事ファイル I』で紹介したインシデントハンドラー、コンピュータフォレンジッカー、リスクマネジメント（リスクマネージャー）なども、この CSIRT の一員になることがあります。他にも、事件が起きたときに何をすべきかの優先順位を決める人、世界中のサイバーセキュリティの情報を集める人、他の CSIRT や警察などに情報を伝える人、CSIRT で使う機械のメンテナンス（整備）をする人もいます。

また、この仕事ファイルの 22～23 ページで紹介したセキュリティアナリストから、「サイバー攻撃を受けた！」と連絡が来ることもあるので、そのときも CSIRT が力を合わせて解決していきます。

このように、サイバーセキュリティの専門家が集まって CSIRT というチームを結成して、サイバーセキュリティの事故、事件、サイバー攻撃に対応しているのです。

（サイバーセキュリティ仕事ファイル担当　高橋 怜子）

サイバーセキュリティ仕事ファイル２（PDF 版）は、以下からダウンロードすることができます。

https://www.lac.co.jp/corporate/pdf/shigotofile2.pdf

サイバー・グリッド・ジャパンは株式会社ラックの研究開発部門です。
サイバー攻撃や各国のセキュリティ事情、セキュリティ防御技術などに関する最先端の研究のほか、
複数のセキュリティ企業との連携や新たな製品・サービスの開発、各種啓発活動などにより
日本のセキュリティレベルと情報モラルの向上に貢献しています。

サイバーセキュリティ仕事ファイル２　～みんなが知らない仕事のいろいろ～

2023 年 3 月　発行

株式会社ラック
サイバー・グリッド・ジャパン　ICT 利用環境啓発支援室　製作

監修
村井 万寿夫　北陸学院大学 教授
佐藤 豊彦　　国立大学法人鹿児島大学 特任教授 兼 株式会社ラック

協力（掲載順）
茨城県立 IT 未来高等学校、情報通信研究機構、長崎県立大学、
虎ノ門南法律事務所、株式会社資生堂、KDDI 株式会社、
損害保険ジャパン株式会社、株式会社みずほフィナンシャルグループ

株式会社ラック
サイバー・グリッド・ジャパン