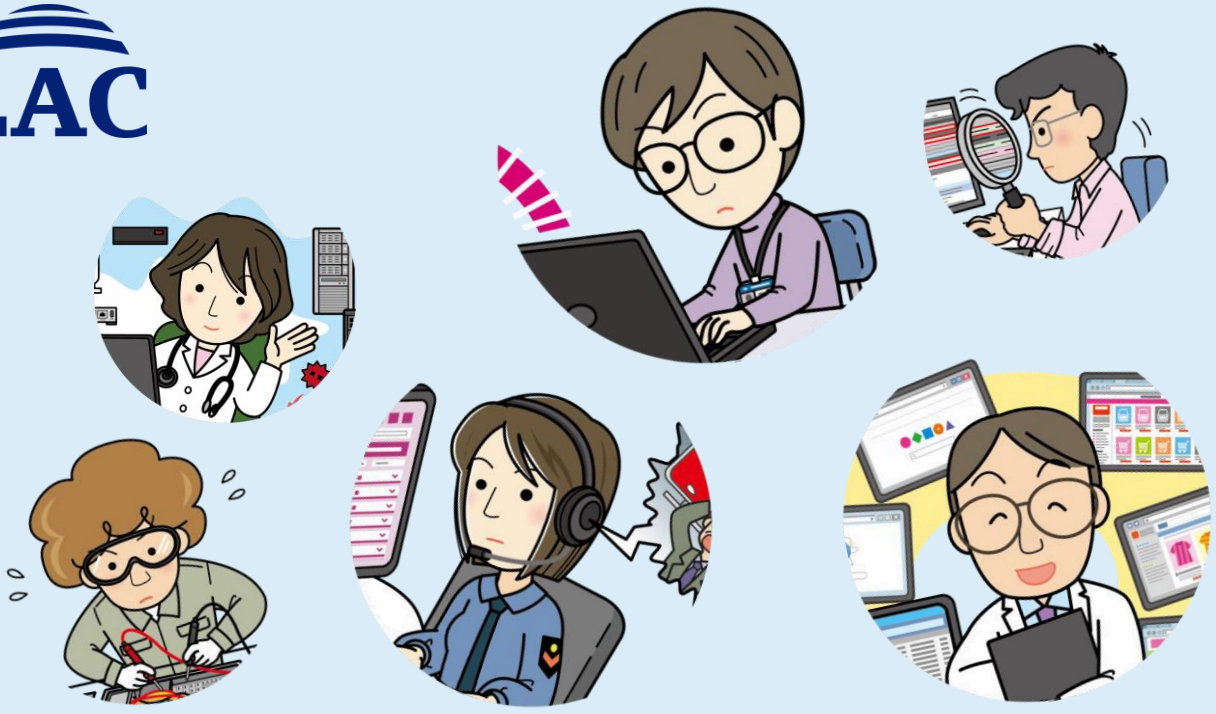
LAC



サイバーセキュリティ仕事ファイル①

～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。

この『サイバーセキュリティ仕事ファイル』では、サイバーセキュリティに関わる仕事を紹介しています。いきなりサイバーセキュリティの仕事と言われても、“サイバーセキュリティ”が何であるか分かりませんよね？　知り合いの小学生に聞いてみたところ、「セキュリティはゲームで出てきたので知っているよ。サイバーは、日本語じゃないよね？」と返ってきました。その通りです。サイバーは、英語をそのままカタカナにしています。この本のどこかに“サイバーセキュリティ”について説明していますので、見つけてみてください。

『サイバーセキュリティ仕事ファイル』を作成したのは、大人でも知っている人が少ないサイバーセキュリティの仕事を、「将来を担う子供たちをメインに大人にも知ってもらいたい！」と考えたからです。

『サイバーセキュリティ仕事ファイル』では、「王道」（正当な道、定番）と呼ばれるサイバーセキュリティの仕事を中心に、バラエティーに富んだ種類の仕事を入れました。加えて新型コロナウイルスの感染が心配される中、サイバーセキュリティの仕事をしている人にオンラインでインタビューをして、仕事を紹介する文章を作りました。

仕事についての紹介では、仕事の内容や魅力を簡単に説明しています。そして、もっと仕事のイメージを持ってもらえるように、実際に仕事をしている人のお話も載せました。もし、興味が持てるような職業があれば、ぜひ、詳しく調べてみてください。

『サイバーセキュリティ仕事ファイル』における私（高橋）の役割は、専門的なことを皆さんに分かりやすく紹介する「通訳」です。サイバーセキュリティで使う言葉を分かりやすく説明したり、印象的なエピソードを入れたりと、楽しく読んでもらえるような文章を目指しました。また、漢字にはふりがなを付けましたが、分からない言葉や表現があれば、辞書で調べたり、周りの人に聞いてみたりしてください。『サイバーセキュリティ仕事ファイル』はこれからも続きますので、楽しみにしていてくださいね。

インターネット被害者の味方

インシデントハンドラー

インターネット世界の正義のヒーロー

インシデントハンドラーとは、皆さんが持っているコンピュータなどにさまざまな方法でインターネットを使って攻撃（サイバー攻撃）された被害者（攻撃を受けた人）の救急救命士と言える職業です。インシデントは「事件」、ハンドラーは「扱う人」という意味です。

サイバー攻撃を受けた場合、大切な情報を取られたり、お金を要求されたりと、とても困ったことになります。また、何もせずそのままにしてしまうと、他のコンピュータもサイバー攻撃を受けてしまうことがあります。

サイバー攻撃は、お休みの日であろうと夜中であろうと、いつでも攻撃することができます。そのため、インシデントハンドラーには、サイバー攻撃を受けた被害者からいつでも電話やメールで連絡が来ます。

連絡を受けてから、まずは何が起こっているかを聞き取り、状況を把握してダメージを広げない方法をアドバイスします。被害者がサイバー攻撃の原因や影響について知りたい場合、コンピュータの科学捜査担当者（コンピュータフォレンジッカー）に調査を依頼します。

実際のインシデントハンドラーのお話

この仕事のやりがい

困っている人のお話を聞き、できる限り助けになりたいと思えるところです。また、日々進化する攻撃を最前線で経験することができるため、インシデントハンドリングの技術を学べるところも魅力です。

連絡を受ける＝被害者にとっての「緊急事態」であるため、被害者を守るためにも、これからも成長していきたいです。守る側である私たちと同じように、攻撃する側も人間であるため、負けたくない気持ちがあります。

この仕事の難しいところ

攻撃する側はどこからでも弱いところを狙って攻撃することができ、いつも攻撃する方が有利なため、被害者を守る必要があるところです。また、サイバー攻撃やコンピュータについての知識も人によって違うため、被害者の立場に立つことが必要です。専門的な言葉をなるべく使わないよう説明や質問方法を工夫し、積極的にコミュニケーションを取るように心がけています。

この仕事でうれしかったこと

被害者から、「助かりました」や「ありがとう」という言葉をいただけた時がとてもうれしいです。

必要な資格や能力

経験が一番大切です。持っていると良い資格は、情報セキュリティの資格（例：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）、GIAC（フォレンジックなど）、情報処理安全確保支援士（サイバーセキュリティの国家資格）、ＥｎＣＥ（EnCase Certified Examiner（デジタルフォレンジックの資格））です。その他には、英語の文章を読む能力（インターネットの最新情報は海外の記事などから知ることが多いため）です。

最後に一言

一緒にサイバー空間を守ってくれる将来の「正義のヒーロー」を募集しています。

お話を聞いた人

郷 晴奈さん（株式会社ラック）

インターネット空間の名探偵

コンピュータフォレンジッカー

悪事を明らかにする捜査専門班

パズルや推理ゲーム、宝探しは好きですか？推理したり謎を解いたりすることが好きな人にピッタリの仕事が、コンピュータフォレンジッカーです。フォレンジッカーは、「証拠を見つけるための鑑識調査や科学捜査をする人」という意味です。この仕事はテレビで見るような鑑識や科学捜査のように、パソコンの中で何が起こっているかを調べます。

では、どのような場合にパソコンの中を調べるのでしょうか？それは、パソコンがマルウェア（悪さをするプログラム、ウイルスとも言います）に感染した場合や、パソコンを使って怪しい動きをしている人が会社の中にいる（他の会社に自分の会社の大切な情報を渡しているなどの）場合に、会社から依頼を受けてパソコンの中に残されている痕跡（足跡）を調べます。また、会社で使っているパソコンに何も問題がないかを確認してほしいと依頼を受けることもあります。

コンピュータフォレンジックは、インシデントハンドラー（インターネットを使ったコンピュータへの攻撃に対応する専門家）から依頼を受けて調査を開始します。パソコンに残された大量のデータから、なぜその攻撃が起こったのか、どのようなことが行われたのかを突き止めていきます。限られた情報から攻撃者の考えを推理し、証拠を見つけていくことから、探偵の仕事にとても似ています。

実際のコンピュータフォレンジッカーのお話

この仕事のやりがい

調べる方法がいつも同じとは限らないため、どのように調べるかを考えることが面白いです。

また、新しい攻撃方法や調べることが難しい攻撃方法、攻撃者の狙いを解き明かしたときにやりがいを感じます。

この仕事の難しいところ

最近の攻撃は、痕跡（足跡）が残らない高度な攻撃が増えているので、攻撃者の痕跡を見つけ出すことが難しくなっています。そのため、いつも最新の情報セキュリティの技術や、攻撃者の間でこれから流行するもしれない攻撃方法を、頭に入れておかなくてはいけないのが大変です。

また、最新の攻撃方法やその攻撃の痕跡がパソコンの中のどこに残っているかなどを知らないと、どのような攻撃をしたかを明らかにすることがとても難しいです。そのため、海外の記事で情報を集めたり、自分で攻撃を再現することでどのような痕跡がどこに残るのかを確認したりして、情報のアップデート（更新）を行っています。

必要な資格や能力

一番大切なのは、根気です。二番目は、さまざまな情報から必要な情報を選び、その情報を整理して痕跡（足跡）の順番に説明することができることです。三番目は、英語や中国語など外国語の記事を探す能力です。情報セキュリティの最新情報は海外の記事から集めることが多いからですね。

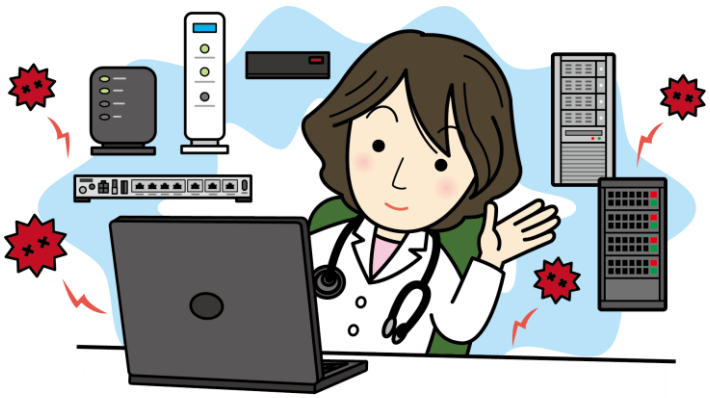
資格は特に必要ありませんが、情報セキュリティの資格、例えば、ＣＩＳＳＰ（国際的に認められた情報セキュリティのプロの認定資格）、GIAC（フォレンジックなど）、情報処理安全確保支援士（サイバーセキュリティの国家資格）、ＥｎＣＥ（EnCase Certified Examiner（デジタルフォレンジックの資格））は、コンピュータフォレンジックや情報セキュリティ全体の勉強になります。

お話を聞いた人

髙橋 勇介さん（株式会社ラック）

システムの健康診断

プラットフォーム診断士



攻撃を事前に防ぐ陰の立役者

皆さんがインターネットで動画を見たり音楽を聞いたり、メールを使って友だちにメッセージを送ったりするときには、パソコンやスマホを使いますよね。でも、そのためには文字や画像、音楽などのデータ（情報）をやり取りするシステムが必要です。このシステムの中心部分をプラットフォームと言います。このプラットフォームは、人間の体で言えば心臓です。そんなプラットフォームを守る仕事の一つに、プラットフォーム診断があります。

プラットフォーム診断は、攻撃者からの攻撃に対してプラットフォームの守りの強さを調べることが重要な役目です。例えば、オンラインゲームが止まらないようにしたり、プラットフォームへの侵入をたくらむ攻撃者から大切な情報を盗まれたりしないように、守りの弱いところがないかを確認します。確認するものは、サーバ（システムが入っているコンピュータ）やネットワーク機器（コンピュータやサーバをつなぐ機器）です。

プラットフォームの弱点を調べるため、本物の攻撃に見せかけた偽の攻撃をして、反応（リアクション）を見ます。専用のツールを使って確認が必要な反応をすべてチェックし、いろいろな弱点を洗い出します。

そして、プラットフォーム診断で見つけた弱点や、システムの守りを強くするためのアドバイス、他のお客様のシステムと比べたときの強さや弱さなどを書いた報告書をまとめ、プラットフォーム診断の依頼をしたお客様に報告します。このときには報告会を行ってお客様の前で説明することもあります。

実際のプラットフォーム診断士のお話

この仕事の難しいところ

攻撃されやすいサーバやネットワーク機器の弱点の情報が世の中に公開されると、攻撃者による悪用（悪い目的のために使うこと）が突然増えます。

攻撃されやすい弱点が公開された場合、私たち診断員は直ぐにその弱点が「どう悪用されるか？」などを調べるために、サーバやネットワーク機器について詳しく知っている必要があります。だから、いつも勉強しています。

また、ニュースサイトやＳＮＳを使って、さまざまな情報をいつでも集めておく必要があります。攻撃されやすい弱点の情報は土日に発表されたり、海外のサイトは（日本時間の）夜中に公開されたりすることがあるので、情報を集めるのも大変です。

必要な資格や能力

情報処理安全確保支援士（サイバーセキュリティの国家資格）と同じくらいの知識が必要です。

能力としては、分析力（複雑なものをバラバラに分けて、その一つ一つを理解すること）が必要です。プラットフォームに本物の攻撃に見せかけた偽の攻撃をして、返ってきた通信（信号）を分析しながら、攻撃されやすい弱点があるかどうかを判断する必要があります。

また、サーバを構築する（自分のコンピュータ内にサーバ環境を作る）ことで、プラットフォーム診断をする知識が得られると思います。

この仕事でうれしかったこと

プラットフォーム診断は、皆さんが学校で毎年受ける健康診断と同じように、毎年同じお客様から依頼を受けて行うことが多いです。繰り返し行うたびに、お客様の弱点が改善され、診断結果が良くなっていくときは、お客様の役に立てていると実感します。

最後に一言

プラットフォーム診断員は、持っている高いレベルの知識を生かして、プラットフォームの安全を支えます。

お話を聞いた人

佐宗 方祐子さん（株式会社ラック）

Webサイトの防御力アップ

Webアプリケーション診断士

Webサイトを強化して守るサポーター

皆さんも学校でインターネットを使って勉強をしたり、家でゲームをしたりすることがあると思います。いつも皆さんが使っているインターネットのWebサイトには、専門的な別の呼び方があります。それは、「Webアプリ（Webアプリケーション）」です。

では、Webアプリとは何でしょうか？Webアプリとは、インターネットで使えるソフトウェア（コンピュータを動かすプログラム）です。このWebアプリを使うためには、必ずブラウザと呼ばれる「インターネットでWebサイトを見るためのソフトウェア」を使用します。そのため、Webアプリは、インターネットなしでは使うことができません。

スマホやパソコンで使っているアプリと似ているので、混乱してしまうかもしれません。スマホやパソコンに入れる（ダウンロード＆インストールして使う）アプリは、インターネットなしでも動くものがあります。分かりやすく言うと、アプリをスマホやパソコンに入れなくても、ブラウザを使って利用できるアプリが、Webアプリです。

このWebアプリの攻撃されやすい弱点を見つけることを任務とする仕事が、Webアプリケーション診断です。お客様から自分の会社のWebアプリを診断してほしいと依頼されたら、コンピュータで自動的に調査ができるツールを使用しながら、スペシャリストと呼ばれる専門家が一つ一つ手を使って診断します。

診断が終わったら、その結果をまとめた報告書を作成して、お客様に報告します。このときには報告会を行う場合もあります。報告会では、攻撃されやすい弱点の内容や、弱点を利用して攻撃された場合のダメージ（損害）とそれを解決する対策（方法）を説明します。

実際のWebアプリケーション診断士のお話

この仕事のやりがい

多くの人が普段使っているWebサイトを診断することがあるため、身近なWebサイトのセキュリティ対策や社会に貢献しているという実感があります。攻撃に使われたら大変なことになる危険度の高い弱点を見つけたときは、安全を保つことができたと感じますね。

この仕事の難しいところ

とにかく、あらゆる攻撃されやすい弱点を覚えることです。Webアプリの数が多いため、Webアプリケーション診断の仕事を始めた頃は大変でした。

一つ一つのWebアプリに個性があるので、その性格に合わせた診断をすることが難しいと感じます。

この仕事でうれしかったこと

深刻なダメージを受ける前に攻撃されやすい弱点を見つけ出すことで、先回りしてダメージを防ぐことができたときはとてもうれしかったです。

ちょっと工夫しないと見つけられないような、レベルの高い弱点を見つけたこともありました。皆さんが難しいゲームを攻略したり、裏技を見つけたりする達成感に似ていると思います。

必要な資格や能力

必要な資格はありません。実際に経験して覚えていくことの方が大切です。情報処理安全確保支援士（サイバーセキュリティの国家資格）と同じくらいの基本的な知識があったり、情報処理（コンピュータとかネットワーク）の言葉を知っていたりすれば、仕事の速さが違うと思います。皆さんが学校で勉強しているようなプログラミングの知識もあればいいですね。

必要な能力は、コミュニケーション能力と想像力です。お客様と話をする機会があるので、相手の話をよく聞いて、お客様の立場に立って考えることができることが必要です。

最後に一言

Webアプリはインターネットでいろいろなところで使われているため、とても身近なものです。陰ながら、皆さんを守っています。

お話を聞いた人

江泉 翔汰さん（株式会社ラック）

多和田 鶴稀さん（株式会社ラック）

インターネット空間の捜査官

サイバー犯罪捜査官

インターネットの世界でも現実でも正義の味方

警察の仕事にはどんなものがあると思いますか？お巡りさんや刑事、白バイなどの仕事がありますが、インターネット犯罪捜査の仕事もあります。この仕事は、インターネット空間で起こる犯罪（サイバー犯罪）を捜査します。

サイバー犯罪の捜査が始まるきっかけは、大きく分けて二つあります。

一つは、インターネットなどで被害を受けた人や、被害を受けた可能性がある人から被害の届出を受けた場合です。被害を受けた人のパソコンや悪用されてしまったサービスを確認して、違法なことをした人（犯人）を見つけ出します。その後、その人を取り調べたり、サイバー犯罪と関わりがあると思われる物（証拠）を集めて調べたりして、本当に犯人であるかを見極めます。

もう一つは、サイバーパトロールと呼ばれる捜査です。インターネット上を見て回り、違法なWebサイトや偽物を売っているWebサイトがないか調べます。例えば、偽物を売ったり、他人のものを勝手に使ったり（著作権侵害）しているWebサイトを見つけ出します。そして、そのWebサイトを管理している人を調べたり、違法なことをしている人を特定したりします。

実際のサイバー犯罪捜査官のお話

この仕事のやりがい

ニュースに取り上げられる事件も多く、これまで警察が苦手としていたインターネットを使った事件を今、自分が担当していることです。担当した事件では、「にせ自炊代行」という事件があります。これは自炊代行（本を買った人から依頼を受けてスキャンしてデータにすることでお金をもらう）のサービスを提供しているように見せかけて、実際は既に保存していた本のデータを販売していた犯人を逮捕しました。著作権法違反（譲渡権侵害）の容疑です。新聞にも載りました。

犯人はスキャンしたデータを購入者に渡して代金を受け取るだけでなく、そのデータ自体をインターネットで売っていました。この事件では、購入者が受け取ったデータを私たちサイバー犯罪捜査官が解析し、データの作成日時などから法律違反であることを明らかにしました。

また、サイバー犯罪では今までの捜査とは違う捜査方法を考えることがとても面白いです。今はインターネットが身近なものであることから、被害にあう人が増えているため、被害を防いでいくことがやりがいですね。

最後に一言

ぜひ警察官になってください。そのときは、長崎県警へ。

この仕事の難しいところ

キャッシュレス決済（現金を使わずにクレジットカードや電子マネーでお金を払う方法）などを使った新しいサービスは、犯罪者が被害者をだますために使うことが多いです。そのため、新しいサービスに関する犯罪が起きたときは、そのサービスを勉強することから捜査を始めます。また、今までの捜査方法がそのまま使えないこともあるので、いろいろな捜査方法を試していくことが難しいです。

この仕事でうれしかったこと

サイバー犯罪の捜査に限らず警察の仕事では、犯人の逮捕、犯人がなぜ犯罪を起こしたのかが分かったとき、被害を受けた人やその家族が安心してくれて被害回復（被害を受けたショックから立ち直り、元通りの状態に回復）していくときです。感謝の言葉をかけていただけるのもうれしいです。

必要な資格や能力

必要な資格はありませんが、持っているとよいのは、情報処理技術関係の資格です。

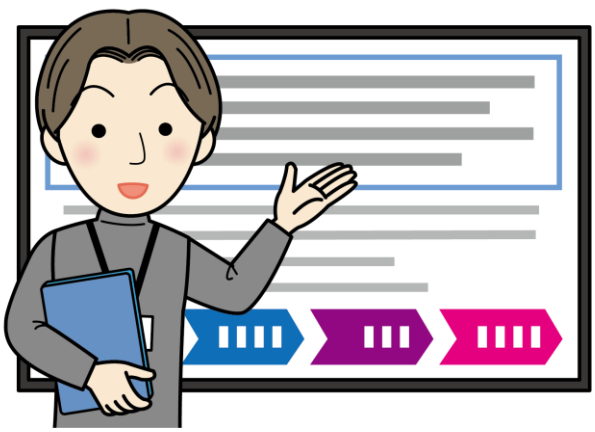
能力で一番必要なことは、「絶対に犯人を捕まえる」という強い意志と、粘り強さです。

お話を聞いた人

秋月 竜太さん（長崎県警察本部）

サイバーセキュリティの勉強ならお任せあれ

セキュリティインストラクター



セキュリティの先生

学校では勉強中に分からないことがあると先生が教えてくれますが、大人になると分からないことは本やインターネットを使って勉強することが多いです。また、専門の学校に通って勉強することもあります。サイバーセキュリティの仕事をしていると、分からないことがたくさん出てきます。そんなとき、サイバー攻撃を受けてからセキュリティについて勉強することや、セキュリティに詳しい人に聞くこともできますが、それではサイバー攻撃の対策に時間がかかってしまいます。

ですから、事前にセキュリティの教育や訓練を受けておくのがよいです。短い時間で集中的にセキュリティの知識や技術を手に入れることができ、本物のサイバー攻撃に似せたゲームを体験して実際の攻撃のために準備することもできます。

このようにセキュリティについて学びたい人のためにセキュリティの教育や訓練を行うのが、セキュリティインストラクターです。つまり、セキュリティの先生です。セキュリティインストラクターは、セキュリティの授業を行います。授業内容を考えたり、授業で使う資料を作成したりします。

授業によって内容のレベルは違いますが教えることは幅広く、初心者向けからセキュリティについて詳しい上級者向けまであります。授業の方法は、受けたい人が多い内容を何回も定期的に行う授業、個別に要望を受けた内容で行う授業、そしてオンライン授業などがあります。学校と同じように教室で授業を行うことが多いのですが、オンライン授業では録画しておいた授業をオンラインで見て学んでもらいます。「聞きのがしちゃったな」「分からなかったな」というところは、何度でも繰り返して見ることができます。

実際のセキュリティインストラクターのお話

この仕事のやりがい

学校のように1年間を通して授業を行うのではなく、数時間しか行わない授業が多いです。そのため、1回1回の出会いを大切にし、失敗したことや苦労したことなど思わず笑ってしまうような自分の経験を混ぜながら、印象的な授業になるように努力しています。授業を受けた人（受講者）から授業後に、「明日からセキュリティを変えていきたい」という言葉をもらえることがやりがいです。

この仕事で うれしかったこと

受講者が熱心に質問してくれたり、話したことに関して何か反応をしてもらえたりすると、話を真剣に聞いてくれていることが分かるため、とてもうれしいです。

受講者と会話する中で、セキュリティインストラクターの私たちが常識だと思っていることが、実は常識ではないということを気づかされることも、うれしいことの一つです。

この仕事の難しいところ

受講者がセキュリティの知識や技術を身につけることが授業のゴールです。そのゴールに達したかどうかが授業の満足度につながると思っていますが、全員に満足してもらえることはなかなか難しいです。

必要な資格や能力

セキュリティインストラクターとして活躍するための「ものさし」として、取ることが難しい資格を持っていた方がよいです。例えば、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）、CompTIA Security+（セキュリティエンジニアの資格）、情報処理安全確保支援士（サイバーセキュリティの国家資格）です。

能力としては、受講者を喜ばせたり楽しませたり、面白い授業にするための、サービス精神です。

最後に一言

大人になったら勉強しなくていいと思っているかもしれませんが、大人になると自分の興味があることを自分で学ぶことができます。ぜひ、知識や経験が豊かな格好いい大人になってください。

お話を聞いた人

大竹 章裕さん（株式会社ラック）

大塚 英恵さん（株式会社ラック）

ゲーム裏の最後の砦

ゲームセキュリティ診断士

ゲームセキュリティの立役者

皆さんはインターネットのゲームをしたことがありますか？ゲームで優位に立とうとして相手をだましたり、不正行為をしたりすることをチートといいます。そして、だましたり不正行為をしたりする人のことをチーターといいます。皆さんが安心して楽しくゲームができるように、ゲームのことを仕事にしている人たちがいます。今回はこの人たちのことを紹介します。

ゲームの仕事にはどのようなものがあると思いますか？ゲームクリエイターやゲームプログラマーは聞いたことがあるかもしれません。他にも、キャラクターを作り出すキャラクターデザイナー、ゲームで流れる音楽を作るサウンドクリエイター、キャラクターのセリフやサブストーリーを考えるシナリオライターなど、さまざまな仕事があります。その仕事の中にサイバーセキュリティに関する仕事があります。それは、チートの撲滅を目指すゲームセキュリティ診断です。

ゲームセキュリティ診断士は、ゲームの中で攻撃されやすい（チートされやすい）ところを見つけ出すことが仕事です。仕事の始まりは、ゲームを作っている会社から「このゲームを調査してほしい」という依頼が来ます。そして、そのゲームでチートできそうなところを全体的に調べて、その結果を依頼されたゲーム会社に報告します。

実は、チーターはゲームをプレイしながら、自分のスタミナ（ゲームを続けるために必要なゲーム内の体力）や攻撃力を上げることができるところを探して、チートするのです。そのため、ゲームセキュリティ診断士もチーターと同じようにゲームをプレイして、チートできるところを見つけ出します。その結果をゲーム会社に報告するのです。

実際のゲームセキュリティ診断士のお話

この仕事のやりがい

私たちの仕事はゲームの発売前や発売後にアップデートされたゲームをプレイして、攻撃されやすいところやセキュリティの問題を見つけ出すことです。チートできてしまうところを見過ごしてしまうと、その後にプレイする人たちの「ゲームの楽しさ」を奪ってしまうため、責任感を持って仕事をしなければならないことにやりがいを感じます。

この仕事の難しいところ

ゲームで新しい機能を作れば「よいところ（プラス面）」を生み出していることになりますが、残念ながら私たちはチートという「よくないところ（マイナス面）」を減らすことしかできません。でもマイナス面を減らすことがゲーム全体のプラス面になります。

初めてのお客様（ゲームを作っている会社）にゲームセキュリティ診断のプラス面を直ぐに知ってもらうことが難しいです。そのため、日ごろからお客様と信頼関係を築くことが大切です。

この仕事でうれしかったこと

私たちだからこそ見つけられるチートがあると、自信を持って仕事ができます。そのようなチートを見つけたときにとても達成感を感じます。

また、お客様から「こんなところ見つかったの？」や「あなたたちだから見つかったのだね」と褒めてもらうことがうれしいです。

必要な資格や能力

資格は必要ありません。とはいえ、他の診断士やお客様との会話の中で技術的な言葉を使うため、情報処理安全確保支援士（サイバーセキュリティの国家資格）があれば、コミュニケーションしやすいと思います。

能力で一番必要なことは、ゲームをより良くしたい、正しいことをするという正義感です。他にも、ネットワーク（コンピュータやサーバをつなぐ技術）などの技術的なことや、ゲームを真剣にプレイしていたり、ゲームを開発した経験があったりと、ゲームに詳しいことも必要です。

最後に一言

私は、大学在学中に会社を作りました。そのためにはさまざまな知識が必要でしたが、その知識は自分で勉強して得ました。そこで分かったことは、勉強する場所や環境は関係ないということです。

私の今の夢は、多くの人にゲームの楽しさをもっと提供する（ゲーム関連の）オーナーになることです。小さい頃からずっと夢を抱いてきましたので、若い人たちにも夢や憧れを持ってほしいです。

お話を聞いた人

森島 健斗さん（株式会社Ninjastars）

コラム１　サイバーセキュリティや サイバー攻撃って、何だろう？

「これってどういう意味だろう？」と思ったことはありませんか？分からないことってたくさんありますよね。私の知り合いに「なんで？」が口癖だった人がいます。その人は分からないことがあると、いつも誰かに聞いていました。大人になった今でも、分からないことは人に聞いたり、自分で調べるようにしたりしているようです。

コンピュータの仕事をしている私たちも、分からないことはいっぱいあります。そのため、インターネットや本で調べたり、他の人に聞いたりと、いつでも勉強するように努力しています。

このサイバーセキュリティ仕事ファイルを読んでいて、「IT」と呼ばれるもの（例えばコンピュータやインターネット）は、カタカナやアルファベットが多く使われていることに気づきましたか？そもそも、これらは外国から来たものであるため、言葉をそのままカタカナやアルファベットにしています。もちろん、日本語にしているもの（例えば証拠や診断など）もあります。

ここでは、新聞やニュースで取り上げられることが多くなってきた「サイバーセキュリティ」と「サイバー攻撃」について、明らかにしていきましょう。

「サイバー」は、「インターネットの」をカッコいい言葉にしたものです。サイバースペース（空間）やサイバー戦争など、多くの言葉で使われていますね。

「セキュリティ」は、「守ること」という意味です。セキュリティというと、家や学校・会社など、形があるものを守ることを想像すると思います。コンピュータの世界でもセキュリティという言葉を使いますが、この場合は形がない「情報」のことです。サイバーセキュリティとは、この「情報を守ること」です。

では、情報を守ることの反対は何でしょうか？例えば、情報を盗むことや、コンピュータへの侵入、コンピュータウイルス感染などがあります。つまり・・・「サイバー攻撃」です。

「サイバー攻撃について説明してください」と言われると、難しいですよね。サイバー攻撃は、コンピュータやスマホなどの機械を使った攻撃です。しかも、コンピュータなどの機械を使っていれば、インターネットを使わない攻撃もサイバー攻撃と呼ばれます。こう言うとややこしいですね。

例えば、レストランなどでお茶を飲みながらパソコンを使ってパスワードを入力しているときに、後ろにいる人がそのパスワードをのぞき見して、パスワードを盗まれてしまったと想定してみましょう。この場合、犯人はインターネットやパソコンを使っていませんが、サイバー攻撃を受けたことになります。これは、人間のちょっとした油断を狙った攻撃の一つです。

そんなサイバー攻撃から、皆さんを守っているのがサイバーセキュリティです。目に見えないので「守られているなあ」と感じることはほとんどないと思います。皆さんが動画を見ている時でも、オンラインゲームで遊んでいる時でも、友達にメッセージを送っている時でも、24時間いつでも皆さんの大切な情報や通信を守っています。

でも、残念ながら、皆さん自身が注意しないと、コンピュータやスマホのデータを消されてしまったり、情報を盗まれてしまったりと、大切な情報を守れないこともあります。

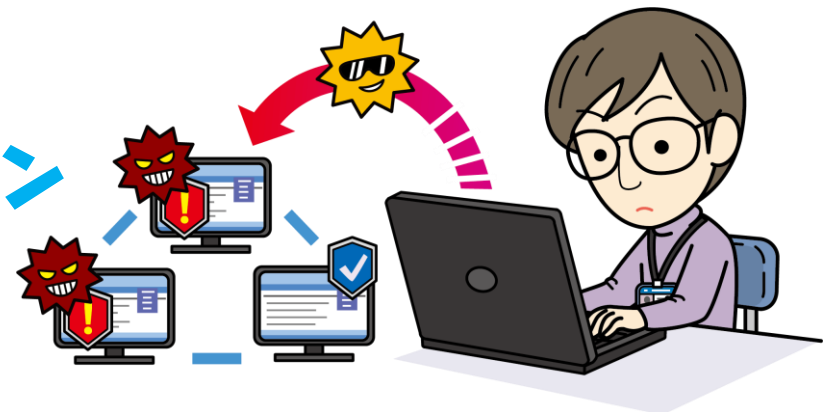
だから、怪しいメールは開かない、自分のＩＤやパスワードを他の人に教えない、分からないときや困った時は身近にいる人（家族や先生）に聞くなど、皆さんも気を付けるようにしてくださいね。

この『サイバーセキュリティ仕事ファイル』でお話を聞いた人の多くは、常に最新の情報を集めていると答えていますね。皆さんもニュースや新聞でサイバーセキュリティに関する情報や興味のある情報を集めてみてください。

（サイバーセキュリティ仕事ファイル担当　高橋 怜子）

限られた時間でミッションを達成します

情報システムペネトレーションテスター



インターネット界のすご腕調査官

ペネトレーションテストという言葉を聞いたことはありますか？きっと、ほとんどの人が知らないと思います。ペネトレーションテストとは、「侵入テスト」という意味があります。会社から依頼を受けて、その会社のネットワーク（コンピュータやサーバをつなぐ技術）に偽のサイバー攻撃を行うために侵入します。そして、守りの効果や、どのくらいサイバー攻撃に耐えられるかを確認します。この方法を「情報システムペネトレーションテスト」と言います。ちなみに、テスターとは、「テストをする人」という意味です。

まず、依頼を受けた会社のネットワークの状況を確認し、テストの準備を行います。次にその会社へ偽のサイバー攻撃を行い、サイバー攻撃の結果や会社のネットワーク上の守りで問題があるところを報告し、守りを強化する方法を提案します。

偽の攻撃では、限られた時間に社員が使っているパソコンに侵入して「最高権限」（会社で何でもできる力）を探し、最も重要な情報（実はテスト用ファイル）を会社の外に持ち出すことができるかを試します。また、実際に悪さをするプログラム（マルウェア）にパソコンが感染した時に、どのようなダメージを受ける可能性があるかを調べることもします。

実際の情報システムペネトレーションテスターのお話

この仕事のやりがい

依頼を受けた会社との取り決めで「偽の攻撃をする許可」をもらっているため、その会社へ偽の攻撃を行うことができます。サイバーセキュリティの仕事はたくさんありますが、実際にサイバー攻撃を行う者と同じようなことができることを許可されているのはペネトレーションテストだけだと思うので、とてもやりがいを感じています。

この仕事の難しいところ

偽の攻撃をする際に、依頼を受けた会社のネットワークに絶対に問題を起こさないように緊張感をもって仕事をすることです。また、お客様（依頼を受けた会社）に攻撃の結果を報告するときに、お客様に「もっと守りを強化しよう！」と考えてもらえるような説明をしなければならないことも難しいです。

この仕事でうれしかったこと

お客様から感謝されたときは、とてもうれしいです。ペネトレーションテストによって、お客様のネットワークに障害を起こしては絶対にいけないので、実際に障害が起きずに調査が終わったときもうれしいですね（正直、ホッとします）。

必要な資格や能力

必要な資格はありません。

能力としては、知りたいと思う気持ち（知的好奇心）が必要です。この仕事は日々勉強する必要があるため、知りたいことを率先して勉強できる人が向いています。

また、ルールを守ることと判断力も必要です。偽物ではありますが攻撃ができてしまうため、やっていいことと悪いことを判断できるかどうかが大切です。

最後に一言

ペネトレーションテストでは「守りが固いところから、欲しいものを時間内に持ち出せるか」が求められているため、針に糸を通すような仕事ですが、とても楽しいです。

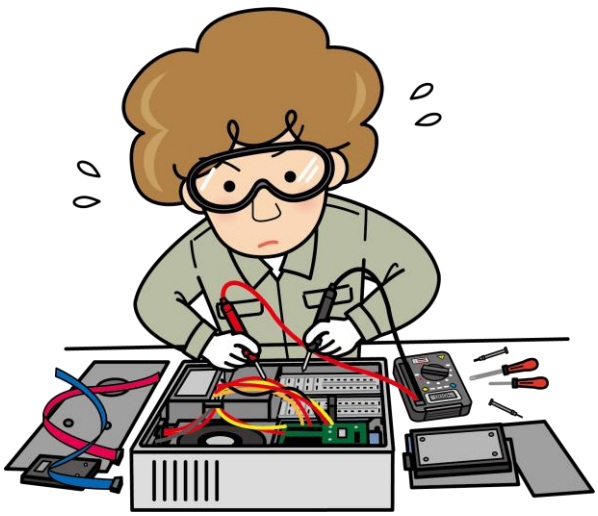
また、これを読んでいる皆さんにおいては、サイバー攻撃やサイバー犯罪を行わないというのはもちろんのこと、サイバー犯罪に巻き込まれるということもないように、情報を取捨選択する能力を身に付けていただければと思います。

お話を聞いた人

小松 奈央さん（株式会社ラック）

分解好き集まれ

IoTデバイスペネトレーションテスター



あらゆる技をもつ調査部隊

ゲーム機やラジカセなどの機械が、どのような仕組みになっているのかなと思ったり、実際に家にある古いラジオを分解して中身を調べたりしたことがあるという人はいませんか？このように中身を調べることを仕事にしている職業があります。それがIoTデバイスペネトレーションテスターです。

「IoTデバイス」とは、エアコンや自動車、コンピュータなど、インターネットにつながっている「もの」のことです。実際に目に見えるものであるハードウェアと、（ハードウェアを動かす役割をする）目には見えないソフトウェアで構成されています。

ペネトレーションテストとは「侵入テスト」のことです。ですから、IoTデバイスペネトレーションテストでは、IoTデバイスの中のハードウェアとソフトウェアがどうなっているかを詳しく調べるだけでなく、IoTデバイスに本物の攻撃に似せた偽のサイバー攻撃を行います。

IoTデバイスペネトレーションテスターは、通常、得意なことが違う人たちが集まって3〜5人でチームを組みます。まず、依頼を受けた会社から、テストをするIoTデバイス2台を受け取ります。1台はバラバラに分解して、基板（コンピュータなどに入っている部品）の攻撃されやすい弱いところを探します。もう1台は、偽のサイバー攻撃ができるかどうかや、設定に問題がないかを確認します。そして、二つの結果をまとめて、依頼者に報告します。場合によっては、報告会を行うこともあります。

実際の IoT デバイスペネトレーションテスターのお話

この仕事のやりがい

テストをする IoT デバイスは、家電（テレビや冷蔵庫など）、車の部品、スマートフォン、工業用機械、病院で使う機器など、さまざまです。これらの中身を確認して攻撃されやすい弱いところを探し、偽の攻撃を行うことは大変ですが、「いろいろなものを知ることができるチャンス！」と思っています。本物の機械に触れて中身を理解することは、好奇心をくすぐられるので飽きることがありません。

この仕事の難しいところ

テストする IoT デバイスの種類によって、中に入っている部品が大きく違うため、普段使わない言葉や仕組みなど、勉強すべき範囲がとても広いことです。そのため、さまざまなことを深く知る必要があります。

1 か月でテストを終わらせなければならない依頼がありました。そのときは最初の 2 週間は中身が複雑で何も分からず、「これで終わるのかな？」とプレッシャーを感じました（でも、ちゃんと弱点を見つけ出しましたよ）。

お話を聞いた人

高橋 信雄さん（株式会社ラック）

矢谷 春樹さん（株式会社ラック）

この仕事でうれしかったこと

お客様から「そんなことが分かったの？」「そんな攻撃方法があるの？」と言われたときは誇らしいです。

無理だと思っていたことができたときもうれしいですね。いつもとは違う形の IoT デバイスを分解してから、どのように元に戻せばよいか分からないことがありました。でも、やり方を工夫すればできることが多いので、楽しんでやっています。

必要な資格や能力

必要な資格はありません。

一番は、ものを作ったり分解したりすることや、修理したりすることが好きであることです。また、深く知りたいと思う気持ち（探求心）も必要です。例えば、パソコンの画面が壊れた場合、同じ部品を探し出し、その部品を交換して直すというような人が向いています。

最後に一言

いろいろなものを分解して中身を調べることは、デジタル化された社会の縁の下の力持ちだと言えます。そんな仕事をしているのが、IoT デバイスペネトレーションテストです。

一緒に守りが強くなる方法を考えます

セキュリティコンサルタント

IT の相談役

何かをするとき、「どうすればいいのかなあ」「分からないなあ」「困ったなあ」と思ったことがあると思います。そんなときに、相談できる人がいれば心強いですよね。コンピュータやインターネットなどの IT（情報技術）を使うときも同じです。セキュリティの専門家でない限り、「安心して IT を利用するにはどうすればよいのか」「個人情報など大切な情報をどのように守ればよいのか」を考えることは、なかなか難しい問題です。

そんな時に頼りになるのが、セキュリティコンサルタントです。セキュリティコンサルタントの主な仕事は、依頼者（お客様）のコンピュータのセキュリティ対策（守り）に問題がないかどうかを確認して、もし問題があれば、依頼者と一緒に考えていく仕事です。

少し詳しく言うと、コンピュータやシステム（情報の保存・取り扱い・伝えるための仕組み）がどのくらい安全であるかをレベル付け（段階付け）したり、守りの弱いところを見つけて守りを強くしたり、どのように依頼者のセキュリティを守り続けていくかを考えます。

他にも、IT を安心して利用するためのルールや教育などの仕組みを作ることもあります。また、作ったルールや仕組みがきちんと機能しているのか、計画が順調に進んでいるのかを見直すなど、サポートを続けながら依頼者と一緒に考えていきます。

セキュリティコンサルタントは、基本的に何人かのコンサルタントでチームを作って取り組みます。依頼者の抱える問題によっては、他の専門部門から情報をもらったり、ときには一緒になってチームを組んだりしながら、協力して解決します。

実際のセキュリティコンサルタントのお話

この仕事のやりがい

お客様の問題を解決することや、役に立っているのが実感できることです。難しい問題をチームで解決できたときも面白いですね。そして、お客様独自の工夫やセキュリティについての考え方など、お客様の話を聞くことが学びとなり、自分の成長にもなります。

この仕事の難しいところ

セキュリティの問題はお客様によって違います。また、似たような問題であっても、会社の大きさや業種、会社の文化やシステムが異なれば、解決するやり方も変わってきますので、お客様に合った提案やアドバイスをすることです。また、いつも質の高い結果（信頼される結果）を出さなくてはならないことが難しいです。

重要な情報を守る側の技術は進歩していますが、盗もうとする側の技術も進歩しているので、お客様の守備力を高めるためどのように組み合わせるのかが難しいです。

ですから、お客様といつでも気軽に話せる関係を作り、どれだけ仲良くなれるかが、仕事の成功を決める大きなポイントと言えます。お客様の顔を見て声に耳を傾けながら柔軟に対応していくことが大切だと思います。

この仕事でうれしかったこと

感謝の言葉やお褒めの言葉が一番うれしいです。「すげー」「早！」「さすが！」など、その時の感情を直接もらえると特にうれしいです。また、問題を解決できたときは、セキュリティコンサルタントの仕事の本当の面白さだと思います。

必要な資格や能力

特に必要な資格はありません。でも、システム・ネットワーク（コンピュータやサーバを繋ぐ技術）の設定や開発などの実務経験があると、セキュリティコンサルタントの仕事に入りやすいです。

能力としては、責任感や道徳性、洞察力などの「コミュニケーション能力」があることです。お客様と仲良くになるにはよく観察しなければならないので、観る（意識して見る）・聴く（意識して聞く）ことです。

最後に一言

セキュリティコンサルタントは、悪いことをする人を探して見つけることではなく、お客様と共に成長していく仕事であり、夢がある仕事です。

お話を聞いた人

内田 昌宏さん（株式会社ラック）

三嶋 美季さん（株式会社ラック）

過去から未来を予測します

脅威情報アナリスト

サイバー攻撃予報士

脅威という言葉を知っていますか？脅威とは、「何か困ったことになりそうなもと」です。例えば、地震や台風などですが、皆さんにとっては宿題を忘れてしまうことなどです。台風が起きると、風でいろんなものが飛ばされたりして危険です。宿題を忘れてしまったら、学校の休み時間に宿題をやらなくてはならず、友達と遊んだりおしゃべりをしたり、ゆっくり過ごす時間がなくなってしまいます。

サイバー攻撃もそれと同じで、困ったことになる前に、さまざまな情報（脅威情報）をもとに分析して将来に役立つように活用するのが、脅威情報アナリストの仕事です。「アナリスト」とは、分析する人という意味です。

脅威情報アナリストは、どこからどのような攻撃が起こったという情報を集めて、そこから未来にどこからどのような攻撃が起こるかを予測します。脅威情報は、「スレットインテリジェンス」なんていうカッコいい呼び方もあります。

まず、インターネットで「攻撃コード（どのような動きをするかが書かれたコンピュータへの命令）」や「攻撃の痕跡（足跡）」を探して、集めることから始まります。実は、集めたものを一つ一つ見ても、何のことだかほとんど分かりません。そのため、独自に準備した分析システムを使って、自動的に組み合わせて新しい情報にします。その結果、例えば、攻撃コードがインターネットに公開された日や、攻撃されやすい弱点かが分かるように付けられた番号などをまとめて、見やすいように表示してくれます。これをもとに、これから起きるであろう攻撃を自動的に予測できるようにすることが目標です。

このような攻撃予測は、インターネットを使った生活や大切な情報をサイバー攻撃から守る人たちが、「どのような守りが必要か」を考えるために使われます。そのため、サイバー攻撃専門の予報士と言っても過言ではありません。

実際の脅威情報アナリストのお話

この仕事のやりがい

やりがいは、情報システムペネトレーションテストやIoTデバイスペネトレーションテストと同様に、攻撃者の動きを予測して、サイバー攻撃に合わせて守りを固めることができることです。

私はゲームで戦う場合、すぐ攻撃するよりも、相手の情報に合わせて装備を整えてから攻撃する方が好きです。例えば、相手が火を使う敵だという情報があれば、戦う前にこちらも火から守る装備を準備します。このように情報を生かして戦う前に優位な立場になれることがとてもワクワクします。

この仕事でうれしかったこと

脅威を予測することは、情報を守る仕事の中でも新しい領域であるため、とても面白いです。いつも新しい何かを生み出すチャンスに恵まれていると思っています。

この仕事の難しいところ

「どのデータを使うのか？」「データをどういう形に作り替えるのか？」「AI（人工知能）を使うのであれば、どの種類のAIを使うか？」など、何度も試しては考え直してやり直します。長い時間がかかってしまうため大変ですが、根気とアイディアで乗り越えています。

必要な資格や能力

能力として大事なのは、チャレンジする気持ちです。新しいことにチャレンジすることが、脅威情報アナリストの仕事だからです。また、あらゆる知識が必要なため、好奇心もあるといいですね。

最後に一言

脅威情報アナリストは、データ分析と情報セキュリティを同時に経験できる仕事です。

お話を聞いた人

庄司　勝哉さん（株式会社ラック）

プロをたばねて問題解決

リスクマネジメント（リスクマネージャー）

サイバー事件の火消し役

リスクマネジメントという仕事は、さまざまな役割をしなくてはなりません。例えば、サイバーセキュリティの事件が起きたときは解決したり、他に守りの弱いところがないかをチェックしたりすることもします。一番大切な役割は、事前に問題を見つけて、守りを強くする戦略を立てることです。

たくさんある役割の中で、サイバーセキュリティのオールスターをたばねるリーダー役をすることがあります。学校では学級委員、チームを組んで行うスポーツではキャプテンのような職業です。

「なぜ、先生や監督ではなく、学級委員やキャプテンなのだろう？」と思いませんでしたか？リスクマネジメント担当は、サイバーセキュリティの事故が起こったときに、今まで紹介してきたインシデントハンドラーやコンピュータフォレンジックなどの仕事をしている人たちをまとめて、先頭に立ち、一緒に問題を解決するリーダーだからです。

サイバーセキュリティにおけるリスクマネジメント担当は、いつもは別の仕事をしています。ですが、サイバーセキュリティの事件を想定した訓練をしたり、事件が起きたときに何をするかをまとめたりして、実際の事件で慌てないように万全に準備をしています。

事件が起こったら、リスクマネジメント担当の腕の見せ所です。まず、サイバーセキュリティのプロの中から誰を集めるかを決め、特別チームを作ります。そして、チームメンバーと一緒に何が起こっているかを確認します。ここで確認することは、いつ、どこで、誰が（何が）どのような攻撃を受けているか、どのような影響が起きているのかなどです。ダメージ（被害）が広がることを防ぎ、事件の原因を突き止めることができたら、解決に向けて動きます。

事件が解決しても、まだやることがあります。同じような事件が起こらないように、守りを今より強くする方法を考えます。これは大切ですね。

最後に、事件の原因や解決方法、守りを強くする方法を会社の上司に報告して、特別チームは解散し、いつもの仕事に戻ります。

実際のリスクマネジメント担当のお話

この仕事のやりがい

サイバーセキュリティの問題が起こったときに、たくさんの人の知恵を借りながら解決することが、一番のやりがいです。また、攻撃されやすい弱いところが見つかった場合など、事件を予防するためにたくさんの人に分かりやすく連絡することも私たちの仕事です。そのため、「何も事件が起きないことが仕事」と言えますが、日常を守るこの仕事にプライドを持っています。

この仕事の難しいところ

判断ミスが許されない仕事であり、さらに判断のスピードも求められます。そのため、判断とスピードのバランスが難しいです。サイバーインシデント（セキュリティの事件）が起きたときに悩むのは、必要な情報をいつ、誰に、どのように知らせるかを決めることです。

最後に一言

ぜひ、一緒にサイバー空間を守る仕事をしましょう。

この仕事でうれしかったこと

サイバーセキュリティの特別チームの活躍を間近で見ることができることが、とても面白く、うれしいところです。サイバーセキュリティで活躍している人の考え方や、最新のサイバーセキュリティの技術に触れられることが、この仕事の魅力です。

必要な資格や能力

情報処理安全確保支援士（サイバーセキュリティの国家資格）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）などのサイバーセキュリティの資格は、持っていた方がよいです。

能力としては、いろんな人と会話する仕事のため、コミュニケーション能力が必要です。また、専門用語を使うことがあるので、IT（情報技術）の仕事をいくつか経験しておくとよいと思います。

お話を聞いた人

菊池 完人さん（株式会社ラック）

コラム２　算数や数学が苦手でもサイバーセキュリティの仕事ができる？

コラム１で、サイバーセキュリティは「情報を守ること」であると紹介しました。読んで気づいたと思いますが、サイバーセキュリティに関わる仕事は、パソコンを使います（ぜひ、ページを戻ってイラストを見てみてください）。つまり、情報を守るために使う武器が、パソコンなのです。

そんなパソコンを使いこなす仕事は、どんな人が向いているのでしょうか？きっと、もともとパソコンが好きだったり、算数や数学が得意だったりする人を想像すると思います。

この『サイバーセキュリティ仕事ファイル』を作るために、サイバーセキュリティの仕事をしている人のお話を聞いてきました。そこで分かったことがあります。それは「興味を持つこと」が何かをするために、始めるために大切であるということです。そのため、きっかけは何でもよいと思います。

では、サイバーセキュリティの仕事は、算数や数学が得意な人だけがするのでしょうか？ 答えは、「いいえ」です。学校に通っているときにサイバーセキュリティやIT（情報技術）の勉強を始めた人は、他の人よりも数歩早いスタートを切ることができます。でも実は、学校を卒業してからサイバーセキュリティやITの勉強を始めている人も、たくさんいます。大切なのは、興味を持ってサイバーセキュリティやITの勉強を続けることです。

また、技術やトレンド（最新情報）はどんどん進化していきますので、普段から情報を集めることが必要です。最新の情報を得るため、英語のニュースや資料を読まなくてはならないことがありますので、英語が好きな人や英語を読めたりする人はそこから始めてもよいかもしれません。

もちろん、算数や数学の考え方が必要になるときもあります。そんなときは、分からないことを理解するために勉強したり、調べたり、人に聞いてみたりしてみてください。時間がかかるかもしれませんが、努力して覚えたことは忘れません。きっと、いつか役に立ちます。

皆さんの将来の夢や就きたい仕事に、サイバーセキュリティの仕事のどれかを入れてもらえたら、とてもうれしいです。もし、どれにするか迷ったら、ぜひ、このサイバーセキュリティ仕事ファイルを手に取ってくださいね。

（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Ⅰ（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/shigotofile.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Ⅰ　～みんなが知らない仕事のいろいろ～

2022年 2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
長崎県警察本部
株式会社Ninjastars
一般社団法人コンピュータエンターテインメント協会

株式会社ラック
サイバー・グリッド・ジャパン