LAC

サイバーセキュリティ 仕事ファイル

～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 5

01 インシデントハンドラー 6

02 コンピュータフォレンジッカー 8

03 プラットフォーム診断士 10

04 Webアプリケーション診断士 12

05 サイバー犯罪捜査官 14

06 セキュリティインストラクター 16

07 ゲームセキュリティ診断士 18

08 情報システムペネトレーションテスター 20

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？ 22

09 IoTデバイスペネトレーションテスター 24

10 セキュリティコンサルタント 26

11 脅威情報アナリスト 28

12 リスクマネジメント（リスクマネージャー） 30

13 高校情報科の先生 32

14　大学教授　34

15　サイバーセキュリティ研究者（技術）　36

16　サイバーセキュリティ研究者（社会心理学）　38

コラム 2　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　40

17　弁護士　42

18　サイバー防衛隊（自衛隊）　44

19　サイバーセキュリティ会社の経営者　46

20　最高情報セキュリティ責任者（CISO）　48

21　セキュリティアナリスト　50

22　フィッシングハンター　52

23　アンダーライター　54

24　インシデントマネージャー　56

コラム 3　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？　58

コラム 4　CSIRT（シーサート）って何のこと？　59

用語集　60

困ったときの相談先 5 つ　70

自由メモ　72

はじめに

皆さん、こんにちは！ようこそ、サイバーセキュリティの世界へ！

株式会社ラック サイバー・グリッド・ジャパンです。

この『サイバーセキュリティ仕事ファイル』を作成したのは、コンピュータやインターネットの急速な発展によってサイバーセキュリティの仕事が増えているからです。

AI（人工知能）が簡単に利用できるようになったように、近い将来、私たちが想像していなかった新しいもの（特にインターネットを使って利用するもの）が次々に出てくることにより、今までとは違う生活になっていくかもしれません。そんな中、悪いことを考える人たちは、どうすれば悪いことができるかをいつも探しています。そうさせないように皆さんの生活を守っているのが、サイバーセキュリティの仕事です。

『サイバーセキュリティ仕事ファイル』では、代表的な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紹介しています。

左側には仕事の内容や魅力を簡単に説明してあります。	右側には実際に仕事をしている人のお話も載せて、仕事のイメージを持ってもらえるようにしてあります。

いよいよ仕事の紹介です。

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。

興味が持てるような仕事があったら詳しく調べてみてください。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、「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！

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、いつも攻撃するほうがいつも有利なため、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。持っているとよい資格は、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、会社で使っている他の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、常に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。

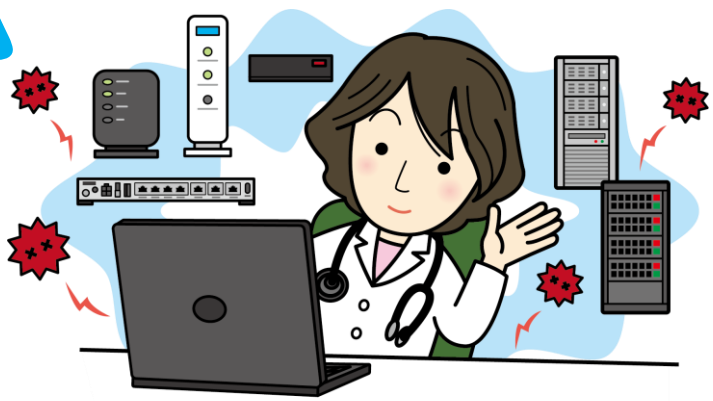
資格は特に必要ありませんが、情報セキュリティの資格、例えば、CISSP（国際的に認められた情報セキュリティのプロの認定資格）、GIAC（フォレンジックなど）、情報処理安全確保支援士（サイバーセキュリティの国家資格）、EnCE（EnCase Certified Examiner（デジタルフォレンジックの資格））は、コンピュータフォレンジックや情報セキュリティ全体の勉強になります。

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、それを動かす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全てチェックし、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。

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。

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。

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作業で診断します。

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損害（ダメージ）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）※インタビュー当時

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。

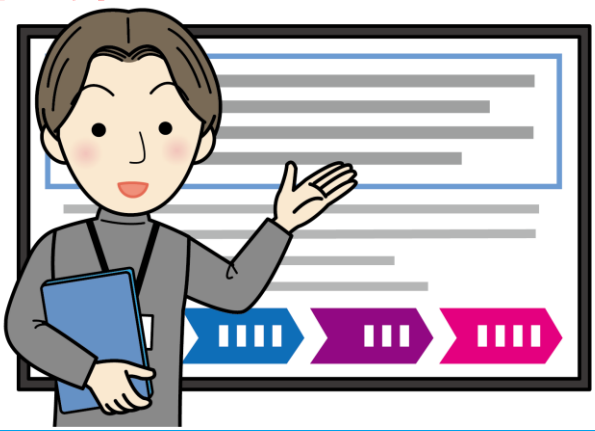
能力で一番必要なことは、「絶対に犯人を捕まえる」という強い意志と、粘り強さです。

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への取り組みを変えていきたい」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。

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。

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。

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。

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言います。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言います。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

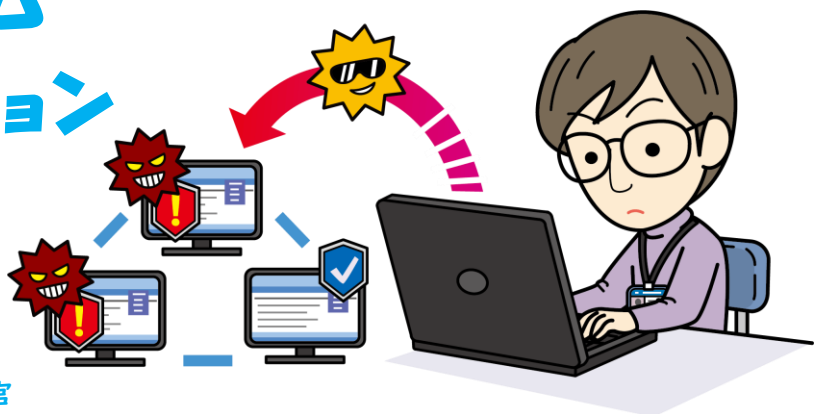
私は、大学在学中に会社を作りました。そのためにはさまざまな知識が必要でしたが、その知識は自分で勉強して得ました。そこで分かったことは、勉強する場所や環境は関係ないということです。

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）

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）をと持つIDやパスワードを探し出し、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）

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。

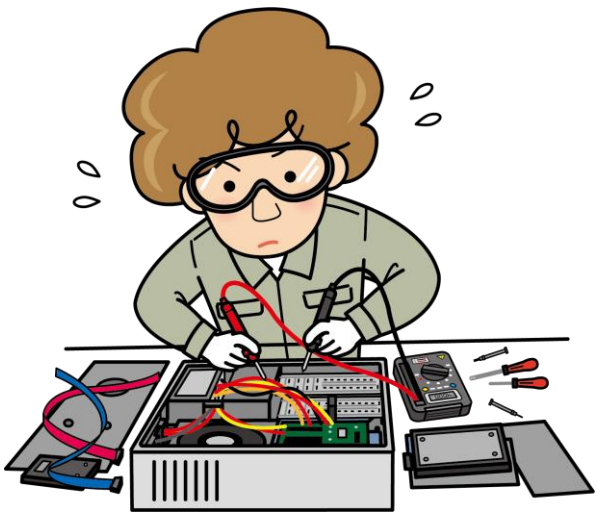
だから、怪しいメールは開かない、自分のIDやパスワードを他の人に教えない、分からないときや困った時は身近にいる人（家族や先生）に聞くなど、皆さんも気をつけるようにしてくださいね。

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）

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）。

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。

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）

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（インターネットやコンピュータなどを使う技術）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。

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。

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）※インタビュー当時
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。

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。

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。

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（インターネットやコンピュータなどを使う技術）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）

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。

13

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１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。

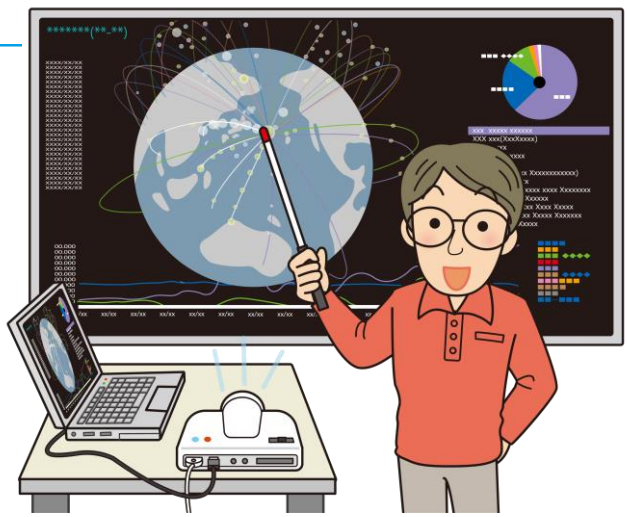
お話を聞いた人

阿南 統久さん（茨城県立IT未来高等学校）

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、48～49ページで紹介しています。

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(そうぞう)します

サイバーセキュリティ研究者(技術(ぎじゅつ))

インターネットの未来を守る職人(しょくにん)

「研究」という言葉で想像(そうぞう)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(なや)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(きょうみ)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(みな)さん以上に想像力を発揮(はっき)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(しょうかい)します。インターネット上のトラブルに巻(ま)き込(こ)まれないように危険(きけん)なWeb(ウェブ)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(こうげき)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(ため)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(しんぞう)と呼(よ)ばれるCPU(シーピーユー)（Central Processing Unit(セントラル プロセッシング ユニット)）でマルウェア（悪さをするプログラム）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(かいけつ)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(ろんぶん)（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(かくにん)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）

コラム２　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）

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』のもくじ（3〜4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。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）やCISA（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）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（深く知りたいと思う気持ち）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）

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。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。

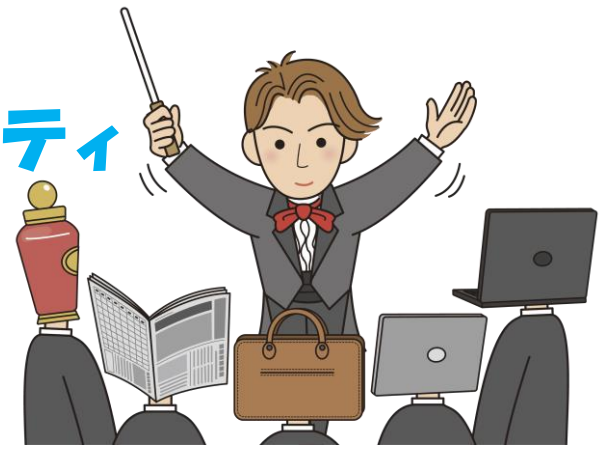
最後に一言

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。

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。

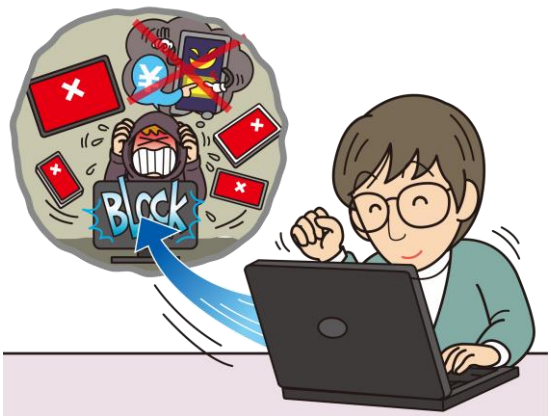
お話を聞いた人

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（アイディー）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（エスエヌエス）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。そして、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３　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（インターネットやコンピュータなどを使う技術）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（世の中の流れ）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）

コラム４　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。インシデントマネージャー（56 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。今まで出てき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、50～51 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）

用語集

この『サイバーセキュリティ仕事ファイル』に載っている難しい言葉や専門用語を説明しています。どのページに載っているのかが分かりますので、分からない言葉があれば確認してみてくださいね。

難しい言葉	説明	載っているページ
サイバーセキュリティ	コンピュータやインターネット上の情報を守ること	5、7、9、11、13、16、17、18、19、21、22、23、30、31、32、34、35、36、37、38、39、40、41、42、44、45、46、47、48、49、50、51、52、53、54、55、56、57、58、59
AI（Artifical Intelligence）	人工知能と言われ、人が手を加えて作った頭、知恵のこと	5、29
インシデント	できごと、事件、事故	6、56
ハンドラー	あつかう人。 警察では警察犬や麻薬探知犬などをあつかう人	6
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	6、7、8、30、50、59
被害者	攻撃を受けた人	6、7、15、51
サイバー攻撃	コンピュータやインターネットを使った攻撃	6、7、16、20、21、22、23、24、28、29、34、35、36、37、40、41、44、45、46、48、50、51、54、55、56、57、59
フォレンジッカー	コンピュータやインターネット上にある証拠を見つけるため 鑑識調査や科学捜査をする人	6、8、9、59

セキュリティ	守ること、安全性	7、9、13、16、17、18、19、22、26、27、29、31、32、33、34、35、37、40、41、43、45、47、48、49、50、51、57、59
CISSP（Certified Information Systems Security Professional）	国際的に認められた情報を守る人のためのプロ認定資格	7、9、17、31、45、57
GIAC（Global Information Assurance Certification）	世界的に通用する情報を守る人のための資格	7、9
情報処理安全確保支援士	コンピュータやインターネット上の情報を守るための国家資格	7、9、11、13、17、19、31、47
EnCE（EnCase Certified Examiner）	コンピュータやインターネット上にある証拠を見つける調査道具を使うための資格	7、9
サイバー	コンピュータやインターネットを使った	7、14、22、30、31、40、44、45、54、55、56
証拠	たしかにそうだ、ということを相手になっとくさせるための材料	8、14、22
マルウェア	コンピュータに悪さをするプログラム、一般的にウイルスとも言う	8、20、36
痕跡	あと、あとかた	8、9、28
アップデート	最新のものにすること	9、19
診断士	調査するものを確認して、どのような状態であるかを判断する人	10、11、12、13、18、19
システム	組織や体系、しくみのこと。サイバーセキュリティでは、情報を保存・取り扱い・伝えるためのしくみ	10、20、21、26、27、28、29、32、44、45、52

プラットフォーム	駅のホーム、中心となるしせつのこと。サイバーセキュリティではシステムの中心部分	10、11
サーバ	テニスやバレーボールなどでサーブをする人。サイバーセキュリティではネットワークを通じてほかのコンピュータにサービスを提供するコンピュータのこと	10、11、19、20、27、50
ネットワーク機器	パソコンやスマートフォン、サーバなどのコンピュータをお互いにつなぐ機器	10、11
（本物の攻撃に似せた）偽の攻撃	（別名：疑似攻撃）	10、11、20、21、25
ツール	道具、工具	10、12、40
反応	はたらきかけに対する相手の動きや変化。サイバーセキュリティではリアクションと言う	10、17
攻撃されやすい弱点	（別名：脆弱性）	11、12、13、28、51
悪用	悪いことに使うこと、使って悪いことをすること	11、14
分析する	実験や機械を使ってそのものに含まれている成分の種類や量を求めること。サイバーセキュリティでは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	11、28、29、32、40、41、44、50、51、53
通信	郵便やコンピュータを使って情報やものをやりとりすること。サイバーセキュリティではコンピュータ同士のやり取りのこと	11、23、32、33、50、51、56
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組み立ててしあげること	11

防御	それが攻撃を受けるのを防ぎ、守ること	12
ソフトウェア	コンピュータ（ハードウェアと言う）を動かすためのプログラム	12、24、42
Webアプリ（Web アプリケーション）	インターネットで使えるソフトウェア（別名：Web サイト）	12、13
ブラウザ	ホームページを画面上に表示させるためのソフトウェア	12
損害	利益を失うこと、失われた利益	12、51
対策	それぞれの問題に応じた解決方法。サイバーセキュリティでは守りや戦略（守る方法）	12、13、16、26、38、39、43、44、56
情報処理	コンピュータに情報を入れて、役立つように手を加えること	13
サイバー犯罪	コンピュータやインターネット上で規則や法律にそむくおこないのこと	14、15、21、41、70、71
被害	害を受けること。 サイバーセキュリティでは、攻撃を受けること	14、15、35
違法	規則や法律を守らないこと	14、43、71
犯人	違法なことをした人（規則や法律を守らなかった人）	14、15、23
著作権侵害	他人が書いた文章や作った音楽、撮影した写真や動画などを勝手に使うこと	14
自炊代行	本を買った人から依頼を受けて、その本をスキャンしてデータにすることでお金をもらう行為	15
譲渡権侵害	他人が書いた文章や作った音楽、撮影した写真や動画などを勝手に売ること	15

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	15
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すること	15
受講者	講義や講習、授業を受ける人	17
CompTIA Security+	コンピュータやインターネット上の情報を守る技術者の資格	17
砦	敵の攻撃を防ぐ小さな建物	18
チート	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	18、19
チーター	ゲームで相手をだましたり不正行為をする人	18
キャラクターデザイナー	アニメやゲームなどのために人物や動物などをつくり出す仕事をしている人	18
サウンドクリエイター	ゲームをしているときに流れる音楽を作る仕事をしている人	18
シナリオライター	映画などの台本を書く人。 サイバーセキュリティでは、キャラクターのセリフやサブストーリーを考える仕事をしている人	18
スタミナ	体力、持久力、活力。 サイバーセキュリティでは、ゲームを続けるために必要なゲーム内の体力	18
プラス面	良い部分	19
マイナス面	悪い部分	19
ネットワーク	放送を利用して同時放送すること。サイバーセキュリティでは、パソコンやスマートフォン、サーバなどのコンピュータをお互いにつなげる技術	19、20、21、27、32、33、50、51

IT（Information Technology）	情報技術と言われ、コンピュータやインターネットなどを使う技術のこと	22、26、31、53、58
スペース	一定のあいている部分、空間	22
ペネトレーションテスト	本物の攻撃に似せた偽のサイバー攻撃を行い、攻撃されやすい弱点を見つけ出すこと（別名：侵入テスト）	20、21、24、25、29
テスター	検査をする係の人	20、21、24、25
最高権限	会社の社長や学校の校長などの役目として、好きなように処理していいという権利	20
知的好奇心	変わったものや、まだ知らないものを知りたがる心のはたらき	21
IoTデバイス	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」	24、25、29
ハードウェア	コンピュータなどの機械、または、目的のためにはたらくしくみの部分	24、37
基板	電子部品が組み込まれている、電気や熱をきわめて通しにくい板	24
家電	家庭電器の略。家庭で使う電気器具。アイロンやそうじ機、テレビなど	25
レベル付け	段階付け	26
質の高さ	人や物を形づくっているものの評価の高さのこと	27、39
洞察力	観察して、かくれた所や将来の様子まで見抜く力	27
観る	ながめる、見物する	27
聴く	くわしく聞く、注意して聞く	27

脅威情報	何か困ったことになりそうなもとのさまざまな情報（別名：スレットインテリジェンス）	28、29
アナリスト	ものごとを分析し、説明する人	28、29、50、51、59
脅威	自分にとって危険だというおそろしさ。サイバーセキュリティでは何か困ったことになりそうなもとのこと	28、29
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のこと	28
アイディア	計画や方法などについてのいい思いつき	29、42、47、55
領域	関係のおよぶ範囲	29
マネージャー	社長などに代わって、全体に指示を出したり責任をもって取り仕切る人	30、56、57、59
オールスター	選りすぐり	30、59
サイバーインシデント	コンピュータやインターネット上の事件、事故	31
データサイエンス	たくさんのデータの中から何か世の中の役に立つことを見つけて、問題を解決すること	32
教員免許状	学校（幼稚園、小中高等学校、特別支援学校）の先生になるための資格	33
採用試験	会社や学校などで働くための試験	33
CISO（Chief Information Security Officer）	会社のコンピュータやインターネット上の情報を管理するための権限をもっている人（別名：最高情報セキュリティ責任者）	35、48、49
博士号	大学院を修了するときに与えられる学位の中で、世界的に通用する最高レベルの学位	35

創造	はじめてつくること	36
CPU（Central Processing Unit）	コンピュータの本体で、計算をおこなう装置のこと	36
論文	理由をあげて自分の意見をのべる文章	36、37、38、39
社会心理学	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	38、39
レポート	調査・研究の報告書、調査・研究をかんたんにまとめたもの	38
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わからない情報	39
新規性	これまでとは別の新しいことや新しさ	39
汎用性	何にでも使えることや使いやすさ	39
信頼性	まちがいないと信じて、たよりにすることやたよりやすさ	39
ウイルス対策ソフト	コンピュータに悪さをするプログラム（ウイルス）からコンピュータを守るソフトウェア	40
詐欺	自分が得をするために人をだまして損をさせること	40、52
転ばぬ先の杖	失敗しないように、よく考えて行動しなさいというたとえ	42
オリジナル	ほかとちがって、特別であるようす	42
知的財産	個人や会社の人たちの知恵によって、新しく考えられたことや新しくつくられたもの	42
裁判	うったえを聞き、法律にあてはめて、どうすべきかを定めること	42
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	42

防人（さきもり）	奈良時代に、近畿地方から東側にある地域から九州に行かされ、だいじな所を守った兵士。 サイバーセキュリティでは常に危機と隣り合わせにいて地域社会の安全を守る人たち	44
内閣サイバーセキュリティセンター（NISC）	日本における、コンピュータやインターネット上の情報を守る中心の組織	44
CISA（Certified Information Systems Auditor）	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	45
探究心	ものごとの本質をさぐって、くわしく知りたいと思う心のはたらき	45
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	41
在宅ワーク	自分の家にいながら会社の仕事をすること （別名：在宅勤務）	41
経営	計画を立てて事業を行うこと、会社を続けていくこと	46、47、49
契約	法律上の効果を持つ約束	46
トレンド	時代の傾向、世の中の流れ	49、58
警報	災害や事故が起こるかもしれないと知らせること、アラートとも言う	50
リアルタイム	録画などのように間をおかず、同時、即時	51
フィッシング（Phishing）	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	52、53
スペル	ことばのつづり方	52

保険	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そなえるしくみ。 病気や死亡、事故などにそなえてあらかじめ保険料をしはらい、もしもの場合に保険金を受け取る契約	54、55
治療費	病気やけがなどを治すためにかかるお金	54
修理代	機械や道具などのこわれた部分を直すためにかかるお金	54
インシデントマネージャー	コンピュータやインターネット上の事件や事故を管理して、事件や事故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	56、57、59
CSIRT（Computer Security Incident Response Team）	コンピュータやインターネット上の事件や事故が起きたときに立ち向かう専門チーム	56、57、59
情報セキュリティマネジメント試験	コンピュータやインターネット上の情報を管理するための国家資格のための試験	57
認証	本人であることを確かめること、本人であることを認めて証明すること。 その人やものにまちがいないと認めること	57
メンテナンス	整備、維持、管理	59
誹謗中傷	悪口や嘘を言われたり、SNSに書かれたりして傷つけられてしまうこと	71

困ったときの相談先 5つ

1 もし、インターネットで困ったことが起こったとき

すぐに身近な人（家族、先生、友達）や周りの大人、

警察などに相談しましょう！

2

身に覚えのないお金を払うよう

求められたり、インターネットで

お金のトラブルに巻き込まれたとき

■消費者ホットライン　電話番号：１８８

■国民生活センター https://www.kokusen.go.jp/map/

3

サイバー犯罪に巻き込まれたときや、

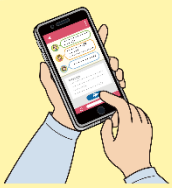
巻き込まれそうなとき

■各都道府県警察本部のサイバー犯罪相談窓口

ホームページ:

https://www.npa.go.jp/bureau/cyber/soudan.html

4



個人情報や写真が勝手に投稿された

■違法・有害情報相談センター

ホームページ：https://ihaho.jp/guide/index.html

5

インターネットで悪口や嘘を書かれて傷つけられ（誹謗中傷）たり、差別を受けたりしたとき

■法務省インターネット人権相談

ホームページ：http://www.jinken.go.jp/

■厚生労働省 まもろうよ こころ

ホームページ：https://www.mhlw.go.jp/mamorouyokokoro/

自由メモ

サイバーセキュリティ仕事ファイル（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/cybersecurityshigotofile.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　～みんなが知らない仕事のいろいろ～

2023 年 11 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）
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、
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

名前