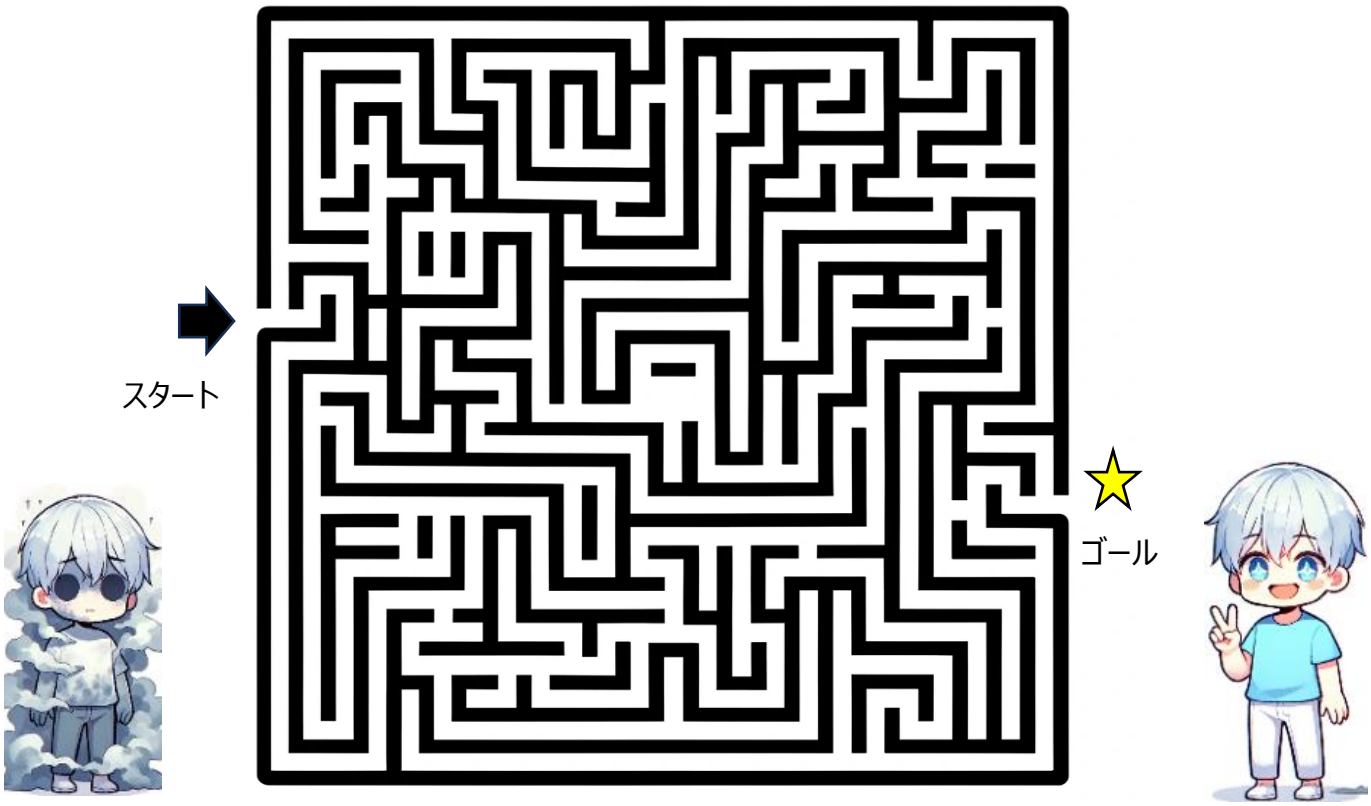


448 時間かけて分かった

セキュリティルールに感じる“もやもや”の正体とは？

独立行政法人　情報処理推進機構　産業サイバーセキュリティセンター
中核人材育成プログラム 7 期生　侵入と対策の研究プロジェクト
2024 年 7 月

目次

こんな人に読んでほしい 2
免責事項 3
はじめに 4
本書の読み方 5
第 1 章. 「もやもや」の正体 6
第 2 章. 「もやもや」を解消するために行ったこと 9
第 3 章. シナリオ演習 11
　シナリオ①：ばらまき型メールと電話詐欺を併用した攻撃 12
　シナリオ②：正規のソフトウェアを改ざんし機密データを流出させる手口 16
　シナリオ③：BadUSB 経由の遠隔操作ウイルス(RAT)感染 20
第 4 章. 納得できなかった禁止事項の考察 23
第 5 章. 「もやもや」に対する筆者らの結論 27
あとがき 29
謝辞 30
用語集 31
画像の出どころと引用元について 32

こんな人に読んでほしい

本書は次のような方々を想定読者として作成しました。

・自社の IT ルールを**守ることに疑問**を持ったことがある人

・情報セキュリティ教育や **IT ルールの作成**をしている人で、どう伝えるかを悩んでいる人

＜想定読者の例＞

想定読者	説明	イメージ
USB メモリ利用者	『USB メモリは原則使用禁止。どうしても必要な場合は申請・登録をして使用すること』という規則に疑問を抱き、USB メモリくらい使わせろ！と思ったことのある従業員の方。	
システム設計者	情報セキュリティの重要性は理解しているが、その対策のために発生するコストアップや、制限に対し疑問を感じている生産現場担当者の方。	
資産管理業務従事者	情報資産の棚卸を行っている際に、台帳にない情報資産を発見し、その登録手続きが面倒だと考えて、登録を避けたことのある担当者の方。	
IT 担当者	一般の従業員が納得して実施できるよう IT 施策に関して丁寧に説明したいが、その理解には専門的な前提知識が必要で、分かりやすく納得感のある説明方法が思いつかずに困っている IT 担当者の方。	

免責事項

(本研究の目的)

本書は、筆者らが情報処理推進機構(以下、IPA)の中核人材育成プログラムにおける卒業プロジェクト「侵入と対策の研究」の活動(以下、本プロジェクト)を通じて、実際に疑似攻撃コードをテスト・評価し、その対策を行うことで得た学びや気づきを、同じ悩みをもつ方々にも共有することを目的としています。サイバー攻撃の手口を広めるために、記載したものではありません。

(情報の出典)

本プロジェクトの演習シナリオは、サイバー攻撃事例やインシデントの報道を参考にしました。また、攻撃テクニックやプログラムについては、各国のセキュリティ機関・組織が Web 上に公開している情報をもとにしています。

(責任)

本書に記載の対策例は、本研究の実施時点での演習環境においては有効と考えられますが、サイバー攻撃や情報セキュリティは日進月歩で進化しており、将来においても有効とは言えません。本書の対策例に基づいて生じたいかなる損害に対しても、筆者ら及び IPA は一切の責任を負いません。

(本書の見解について)

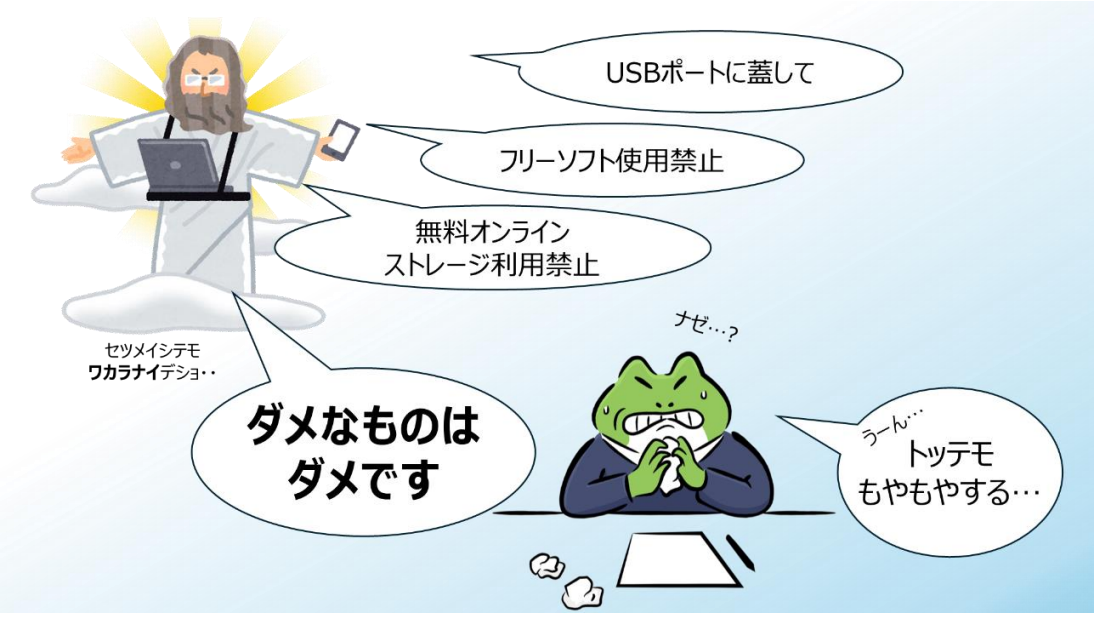
本書は IPA および産業サイバーセキュリティセンターの意見を代表するものではなく、本プロジェクトの見解に基づいています。

(注意事項) ※サイバー攻撃は犯罪です(＝真似しないでね)

本研究では具体的な情報セキュリティ対策を検討する目的で、疑似攻撃コードを作成し、シナリオを検証しています。これらの行為を評価環境以外で実行した場合、悪意の有無にかかわらず、**「不正アクセス行為の禁止等に関する法律」(不正アクセス防止法)等の法律により処罰される**可能性があります。

はじめに

みなさんは、会社の情報セキュリティルールに**「どうしてこんなルールに従わなければいけないの？」**と思いながらも従わされ、**「もやもや」**とした、なんだか負の感情が湧き上がってくることはありませんか？



実は筆者らも中核人材育成プログラムに参加するまでは、この**「もやもや」**を日々感じながらルールに従う一般の従業員でした。今回、このプログラムに参加し、そこでサイバー攻撃とその防御を自分で再現するという体験を通して、**「もやもや」**を感じながらも従っていたルールの真意が分かり、**「もやもや」**を**「納得感」**に変えることができました。不可解なルールの裏に、そんな背景があったのか・・・まさに**目からうろこの体験**でした。

そこで筆者らは、読者の方々にもこのような感動を味わってもらいたいと考え、本書の作成を企画しました。これまで感じていた**「もやもや」**が何に由来していたのかを最初に示したうえで、**もやもや解消**のヒントとすべく行ったシナリオ演習と、そこで得られた気づきを紹介していきます。筆者らが中核人材育成プログラムにおいて、**通算 448 時間のハンズオン演習から得た知識・経験をギュッと凝縮しています。本書を読むことで、時間をかけずにそれらを学べるお得な内容になっています！**

本書を読むことで、セキュリティルールに納得し、**積極的にルールを守ろう**とする理由が見つかると幸いです。

本書の読み方

本書はセキュリティルールに感じる**もやもや**について、なぜ筆者らの**もやもや**が解消したのかを5章に分けて説明していきます。

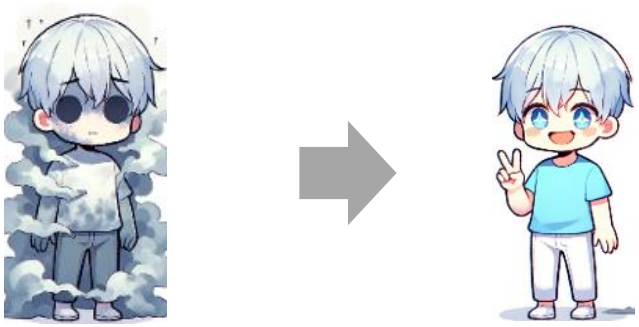
まず第1章では、**「もやもやの正体はこれだ！」**と考えた内容と、そう思うに至った経緯を説明します。

続いて第2章では、**もやもや**のもとになっている「情報セキュリティ担当者から言われて**納得**できなかったこと」について説明します。どうやってそれらを**納得**しようとしたのか、本プロジェクトを始めるに至った経緯と共に紹介していきます。

第3章では、具体的に行った本プロジェクトのシナリオ演習内容を説明します。どんなことをして、何を学んだのか。みなさんも一緒に演習している気持ちになって読み進めてもらえたら嬉しいです。

第4章では、シナリオ演習から学んだことを踏まえ、著者らが**「もやもや」**を感じていたルールが妥当だったのかについて検証していきます。**「もやもや」が一つずつ納得感**に変わるまでの過程を共に体験して頂ければと思います。

そして第5章では、**「もやもや」に対する著者らなりの結論**を簡潔にまとめたいと思います。みんなが**スッキリ**した気持ちで、ルールを守れることを願って・・・。



第 1 章. 「もやもや」の正体

現場の従業員が情報セキュリティルールに対して感じる**「もやもや」**の正体とは何でしょうか？

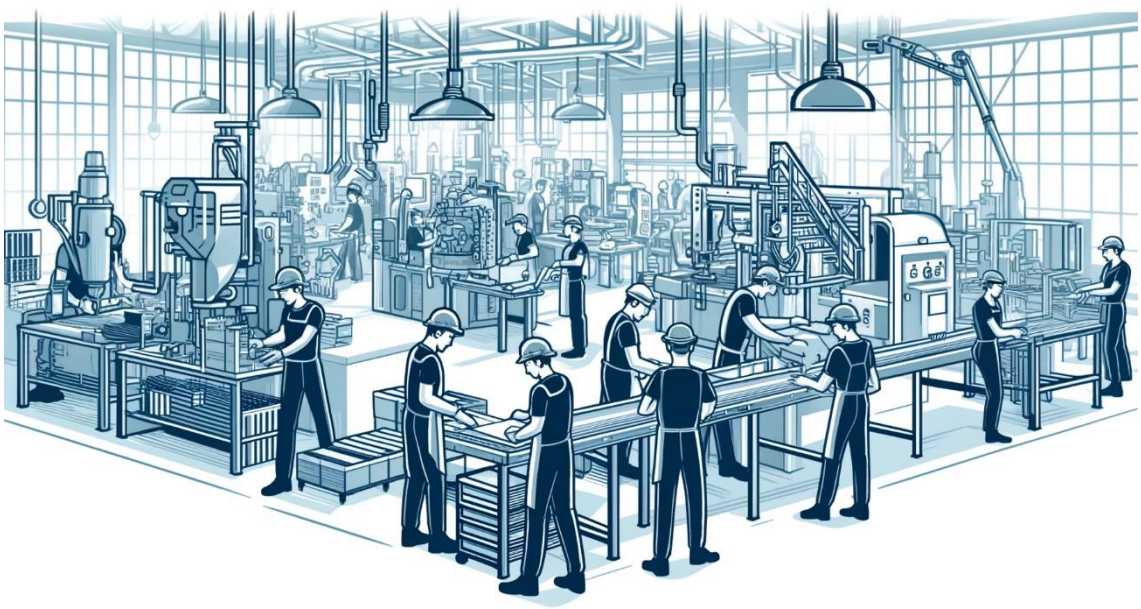
セキュリティルールを守ると、時に不本意にも作業の効率が落ちる、使いたい製品が使えないなどの不利益を被ることがあります。理由が分かり、**納得**して従っていれば特に気になりませんが、**納得**できないままこの不利益をこうむり続けると、内心では**納得**できず**もやもやとした感情**が残ってしまいます。筆者らは、これが**「もやもや」**の正体だと考えています。

では、何故納得感が欠如したままだといけないのでしょうか？筆者らは、ルールを守らせる人たち(セキュリティ担当者)と守る人(一般の従業員)との間に溝ができ、それが会社の情報セキュリティレベルを下げてしまうからだと考えています。

たとえば、セキュリティ担当者と生産現場との人間関係に溝ができると、生産現場の情報セキュリティ対策も遅れがちになり、情報セキュリティの問題が起こりやすくなります。一旦問題が起こると、生産現場の仕事が滞り不利益を被ることに加え、セキュリティ担当者にとっても通常の業務を行いながら緊急対応をしなくてはならず、お互い非常に大変な思いをすることになります。

また、このほかにも生産設備を導入する際に、計画の初期段階から情報セキュリティの部署と上手く連携できていれば、最初から情報セキュリティレベルの高い設備を導入でき、時間も予算も抑えられるのに・・・といった事例も発生します。

結果として、**「もやもや」**を放置すると、両者共に得しない状況が生じます。**それは会社にとってもよくないですよね**。



もやもや（パスワード使いまわし編）

作 Mr.もやもや

第 2 章. 「もやもや」を解消するために行ったこと

筆者らの一人が自社の生産現場にいた時に、情報セキュリティ担当者から指示されて**納得できなかった禁止事項**が 4 つありました。そのうち 2 つは、中核人材育成プログラムの前半で行ったハンズオン演習を通じて、**「もやもや」**を解消することができました。

そこで、攻撃のことをもっと勉強し、自分たちで作ってみることにしました。攻撃に対する理解が深まり、残りの 2 つの**「もやもや」も解消できるかもしれないと期待**し、後半の卒業プロジェクトにて本プロジェクトを立ち上げました。

No.	禁止事項	これまでどう思っていたか	なぜもやもやが解消したか
1	パスワードの使いまわし	元のパスワードが漏れたり、推測されたりすると、他も突破されるから危険。	パスワードを知らなくても、同じであれば突破される「パス・ザ・ハッシュ」攻撃があることを知った。
2	古い OS の利用	外部公開していないサーバは、古い OS を使っていても問題ない。	一旦社内に侵入されると、脆弱性がたくさんある古い OS は簡単に乗っ取られると知った。
3	会社が許可していないソフトウェアの使用	便利なソフトウェアがいっぱいあるので、自由に使いたい。	※もやもや
4	許可されていない USB デバイスの使用	個人の USB メモリを使いたい。未許可のデバイスでも、ウイルスチェックすれば問題ないよね？	※もやもや

攻撃手法を深く理解し、シナリオ作成の手がかりとするために、自分たちで一般的な企業のネットワーク構成を模した演習環境を構築し、その環境下で疑似攻撃コードを順に試してその効果を確認していくことを行いました。これに必要な情報は、サイバー攻撃の手口やその対策がまとめられ公開されている MITRE ATT&CK というデータベースと、さらに評価・テスト用に疑似攻撃コードが公開されているサイトを利用しました。

この結果、いくつかの攻撃を再現できるようになったので、まずはそれらと身近に起きたサイバー攻撃事例を組み合わせて 1 つ目のシナリオを作成しました。そして構築した演習環境で実際に動くように作り込みました。最後にその攻撃がどうやったら防げるかを考えて、その対策を評価しました。

これを２つ目、３つ目と繰り返すうちに、攻撃と防御の両面の知識が向上し相乗効果が働いて、侵入の手口に対する解像度が上がっていきました。次の章で具体的な３つのシナリオをご紹介しますが、回が進むにつれて技術レベルも上がっているのが分かり、筆者らの成長も感じてもらえるかと思います。

第 3 章.　シナリオ演習

まずはシナリオ作成の演習の流れを説明します。初めに、著者らみんなで攻撃のシナリオを考え、それにあう仮想企業とそのネットワーク環境を考案しました。その際、一般従業員になじみがあって、実際に起こりそうなもの、著者らの**「もやもや」**の解決に役立ちそうな、という要素を取り入れていきました。

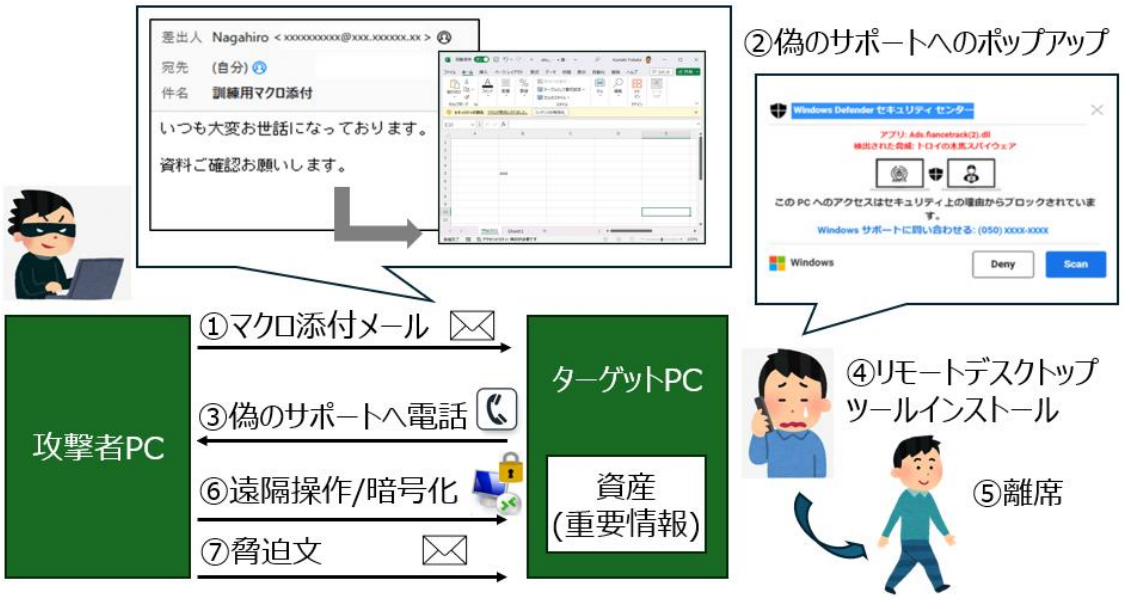
そしてシナリオが完成したら演習環境(ネットワーク環境)を作り込んでいきました。続いて手分けして攻撃のツールを作成し、シナリオに沿ってそれを再現してみました。そして最後にその攻撃をどうやって防げるかを検討して、その対策を演習環境に反映して攻撃が防げるようになったかを試しました。

今回作成した攻撃シナリオは 3 本で、大まかなテーマとしては、1 本目が**ヒューマンエラー**、2 本目が**ソフトウェアの改ざん**、3 本目が**不正な USB デバイス**がテーマとなりました。

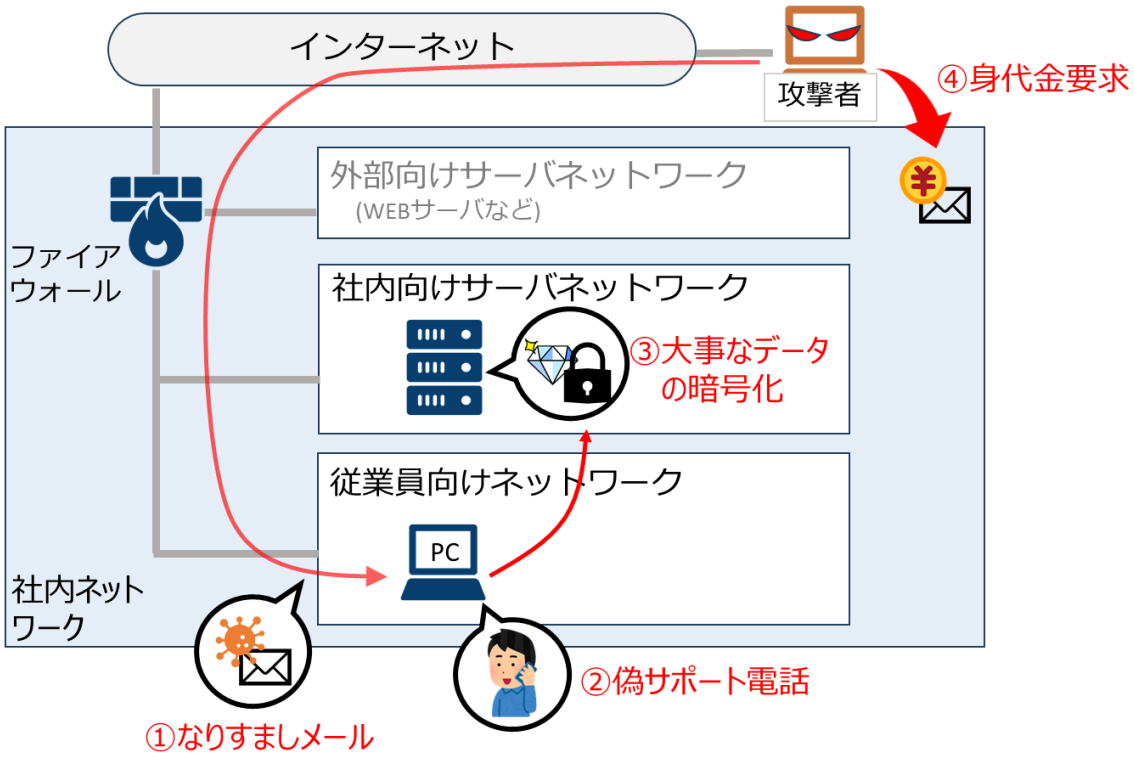
シナリオ①：ばらまき型メールと電話詐欺を併用した攻撃

このシナリオは、テクニカルサポートへの信頼を逆手にとった、ヒューマンエラーの要素が多いシナリオです。

このシナリオでは、従業員がなりすましメールに添付されたエクセルファイルを開いてしまい、更にマクロの有効化ボタンを押してしまうところから始まります。すると、翌営業日に PC 画面上に**「ウイルスに感染したので、テクニカルサポートへ連絡してください！」**というメッセージが表示されます。この連絡先は自社のテクニカルサポートではなく、攻撃者側の電話番号に繋がります。被害者が連絡すると「サポートに必要だから」と言葉巧みに遠隔操作ツールのインストールを促され、攻撃者が自由に操作できるようになると今度は**「作業に時間が掛かるので休憩に行ってきてください」**と離席を促されます。そして、不在の合間に PC 内の大事なデータが暗号化されてしまい、後日脅迫文にて身代金が要求される、という流れです。



今回の攻撃者の最終目的は身代金の取得です。脅迫文では**「支払いに応じればデータを復号する」**と記載されていますが、**その保証はありません**。また、身代金で金銭が得られなかった場合、大事な情報が不特定の誰かに売られ、更なる被害を招くことも考えられます。



この攻撃の特徴は、サイバー攻撃と特殊詐欺の手口を組み合わせていることです。さらに送られてくる**ばらまき型メール**は単純なプログラムであるため、特別な技術知識がなくても実行される可能性があります。また、一般的な遠隔操作ツールを使うので、相手の PC 環境を選ばずに実行できてしまうのです。この攻撃は従業員の焦り(心の隙)をついていますが、**このように焦っている場面で完璧な対応ができる人はなかなかいないですよね**。

この話を聞いて**「こんな雑なサイバー攻撃なんて現実には起こりっこない」**と思いませんでしたか？しかし、ばらまき型メールの手口は 2010 年代後半に大流行したウイルスである**「Emotet」**でも利用されています。また、後半の言葉による巧みな誘導は著者らの周りで**実際に起こったヒヤリ事例**がもとになっています。つまり、身の回りで起こってもおかしくない出来事なのです。

この攻撃に有効な対策は、まず**迷惑メール**の教育をして、メールを開く従業員を減らすことです。また、不審な添付ファイルを開いたら正しい情報システム部門(担当)にすぐに連絡することです。また不審な連絡先に誘導されないように、日ごろから**正しい連絡先**を見えるところに明記しておくことも有効です。更には侵入された場合を想定して、いち早く察知する仕組みの導入や、日ごろからデータの**バックアップ**を取っておくという当たり前の対策も重要です。

コラム①：バックアップしていれば暗号化されたファイルは何とかなる？

シナリオ①で記述した通り、暗号化に対して**バックアップ**は非常に強力な対策ですが、**バックアップからデータを戻せば全部解決**だと思っていませんか？今回のシナリオでは、侵入の原因となるものがリモート接続ツールでした。しかし、実際にはそんなに簡単に原因を特定できるのでしょうか？

筆者が昔、実際に遭遇した状況では侵入方法の特定に困難を極めました。なぜならネットワークやソフトウェア、PC を導入・管理している業者が異なっており、各業者による責任の押し付け合いや契約内容による調査期間の長期化が発生した結果、原因の特定に至ることができませんでした。結果、暗号化されたサーバを初期化して**バックアップ**から復旧させる対応をしましたが、同様の侵入経路を使用されて同じ被害に遭うという結末となりました。

この経験から、原因の特定をしないことには**バックアップ**も効果を発揮できないことを知り、侵入の検知や防御も**バックアップ**と同様に重要だと実感することができました。

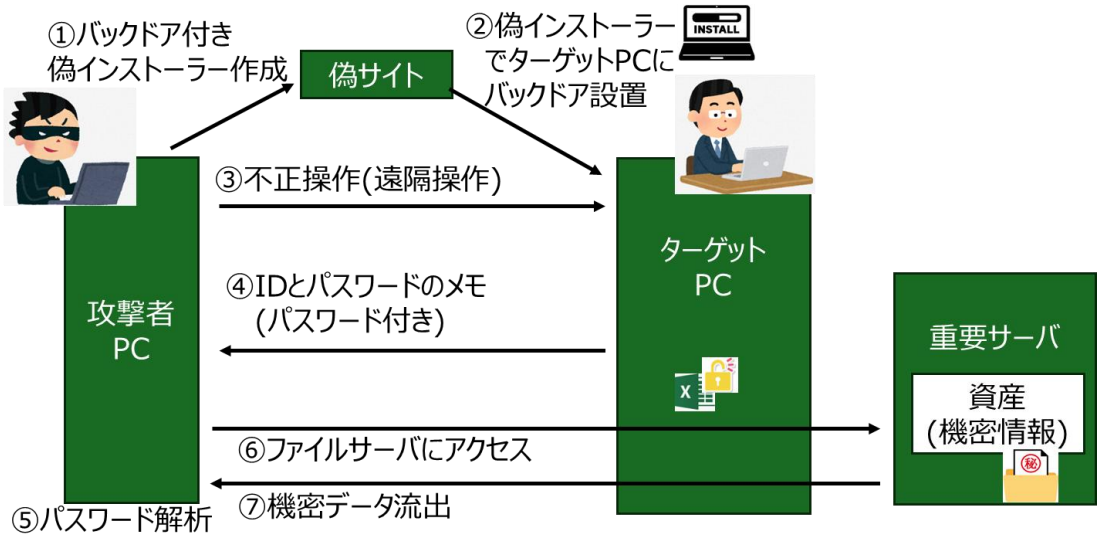
シナリオ② ：正規のソフトウェアを改ざんし機密データを流出させる手口

2 つ目のシナリオは「許可されていないソフトウェアの使用禁止」というルールの背景にある、**「ソフトウェアの改ざんなんて本当におこるのか？」**という**「もやもや」**を解決するために作成しました。

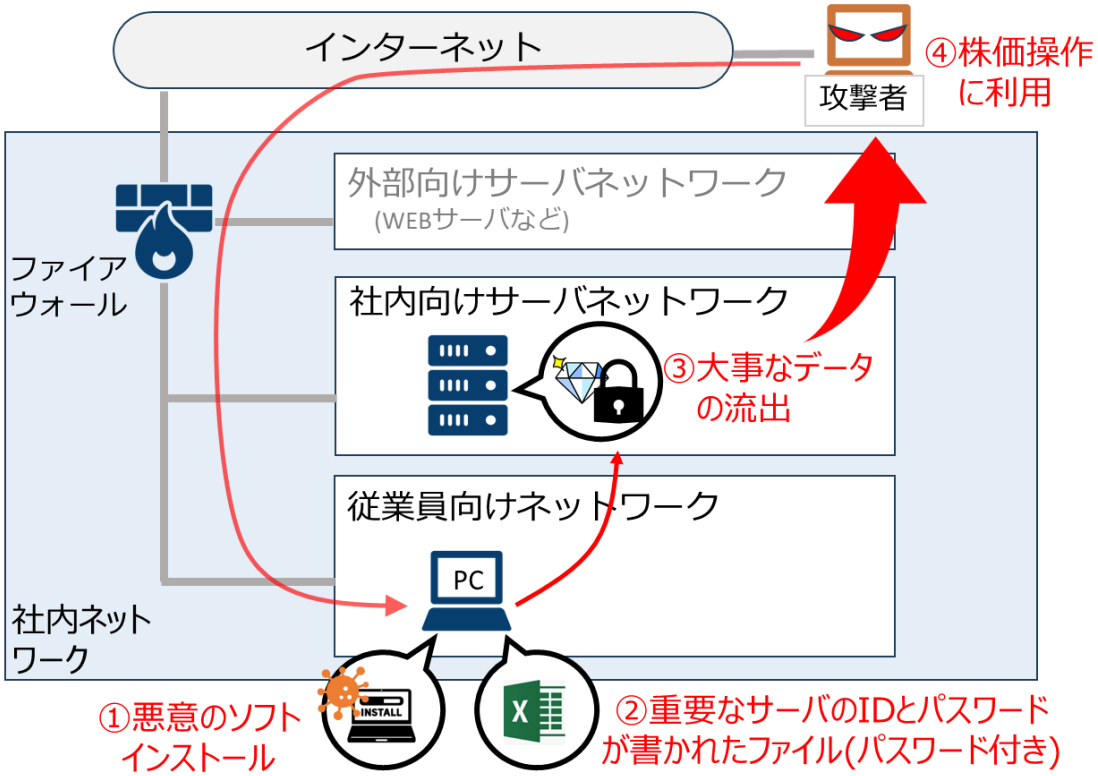
突然ですが、皆さんは**「バックドア」**というものをご存じでしょうか？これはざっくり言うと、会社のネットワーク内の PC にこっそり入り込むことができるようにする(つまり裏口のようなものを作っておく)というものです。今回の話でいうと、「会社のファイアウォールで止められることなく攻撃者が直接ターゲット PC を遠隔操作する」というものとなります。筆者らで偽のフリーソフトのインストーラーを作り、これにバックドアを仕込んでターゲット PC を遠隔操作できるようにすることが、技術的にどれほどの難易度なのかを確認したいと思い、本シナリオを考案しました。

このシナリオの具体的な流れについて説明します。まず、攻撃者はフリーソフトとバックドアを仕込むツールを 1 つにまとめた偽のインストーラーを作成し、用意した**偽のウェブサイト**を使用して、被害者が偽のインストーラーをダウンロードするように誘導します。このインストーラーを起動すると、本物のフリーソフトと一緒にターゲット PC に**バックドア**を作ってしまうプログラムもインストールしてしまいます。その結果、攻撃者がターゲット PC を遠隔操作し、その PC 内に保存されていた重要サーバの ID とパスワードが書かれたファイルが盗まれてしまうというシナリオです。

この時、被害者は用心深くファイルにパスワードをかけていたという想定ですが、今回の攻撃者は気づかれずに潜伏していますので、時間をかけてパスワードを解析し、その後得られた ID とパスワードを使って社内のより重要なサーバにアクセスし、情報を盗み出します。

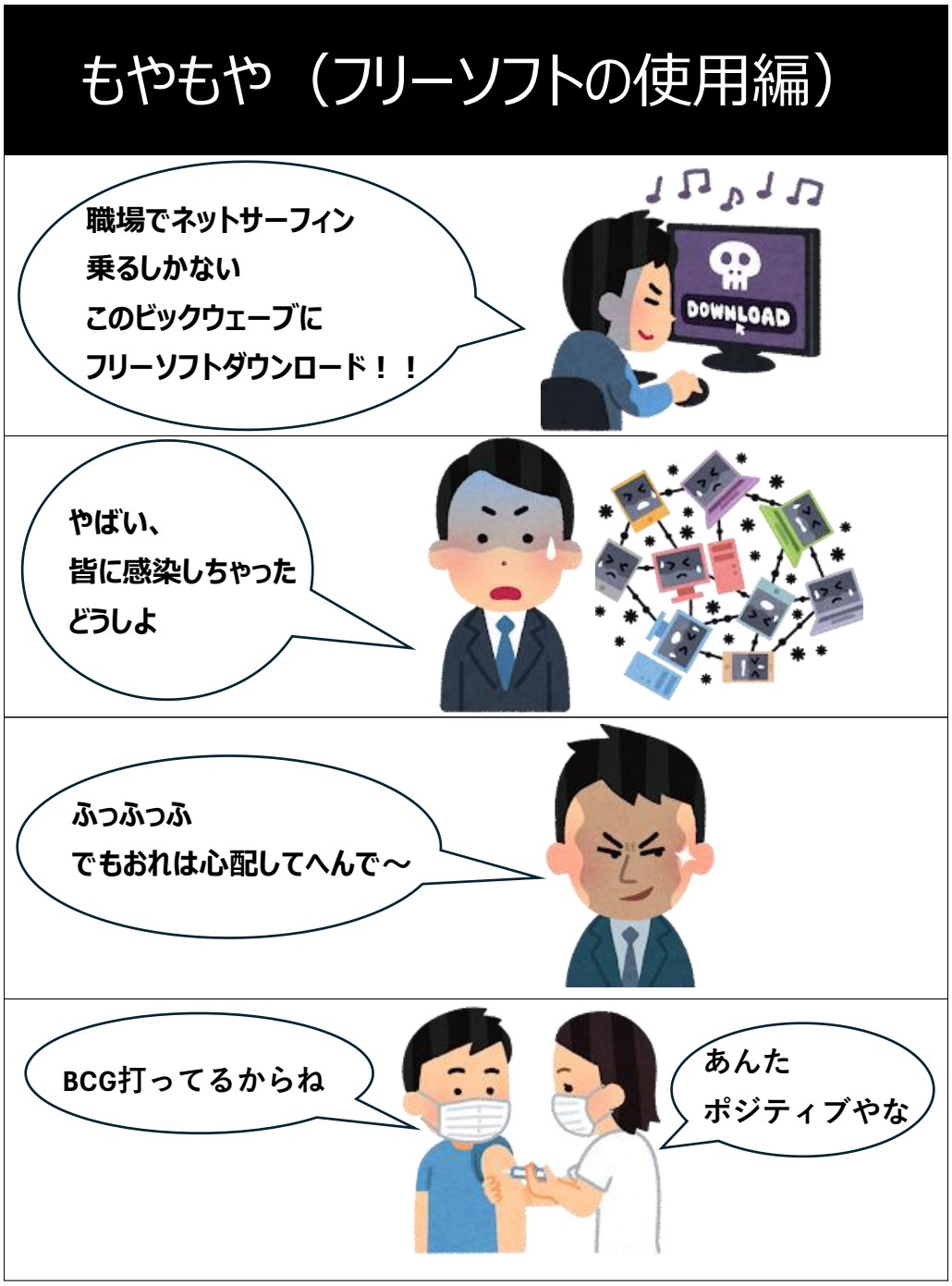


今回の攻撃者の目的は、機密データを流出させて企業の信頼を落とし、**株価を下げる**ことで不正な利益を獲得することと想定しました。最終的に攻撃者は重要サーバに保存されている個人情報や、営業機密情報を盗み、闇サイトに流出させます。そうなると、後日警察から**「大変です！あなたの企業の機密データがインターネット上で不正に投稿されています！」**と電話がかかってきて、事態が発覚し、大きな問題に発展することになります。



この攻撃は、インストール時にちょっと不自然な動きがみられるものの、インストールされるソフト自体は本物なので、**普通の人はなかなか気づけません**。またシナリオの中で、ターゲット PC 内の重要サーバの ID とパスワードをメモしたパスワード付きファイルを見つけられ、解読されてしまう場面が出てきますが、皆さんの中にも、重要な情報をファイルに保存していて、**パスワードを付けているから大丈夫**と安心している方がいませんか？近年コンピュータの性能向上に伴い、昔は安全と言われていた長さのパスワードでも、今は危険性が増しています。試行回数に上限がなく、バックドアに気づかれていなければ、攻撃者は十分に時間を使ってファイルのパスワードを解析し、突破することができてしまうので気を付けてください。重要情報の保管については、PC の中ではなくて、物理的に離れた場所に保存する、パスワードを一定以上に長くし、かつ大文字、小文字、特殊文字を混ぜるといった方法が効果的です。

このシナリオを通じて学んだのは、**改ざんされたソフトウェアを掴まされるリスクは意外と身近である**ということです。だから、ルールを守り、普段の行動で気を付けることで、**改ざんされたソフトウェアに遭遇する確率を下げることが大事なのです**。



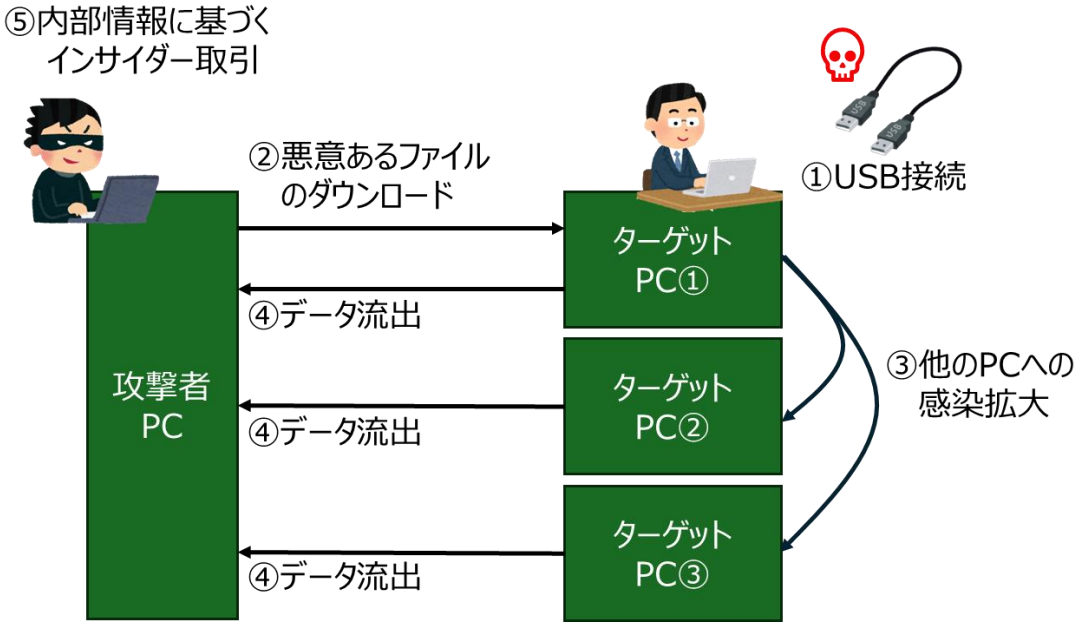
作 Mr.もやもや

シナリオ③：BadUSB 経由の遠隔操作ウイルス(RAT)感染

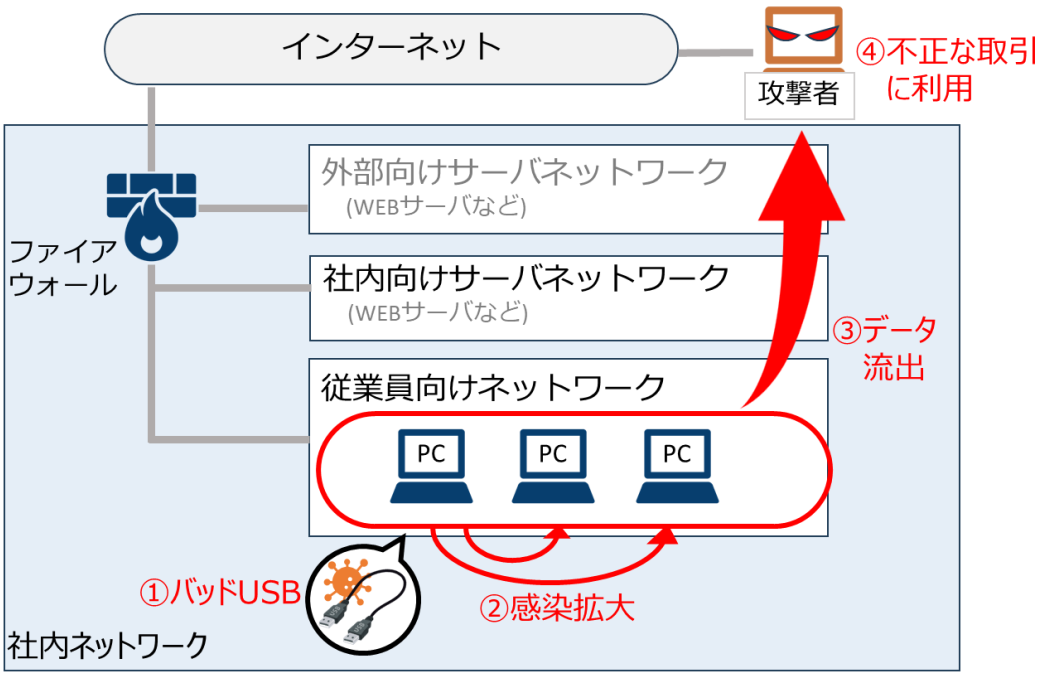
3 つ目のシナリオは、**「USB を接続しただけで本当にウイルス感染するのか？」**という**「もやもや」**を解決するために考えたものです。

今回の攻撃は、**USB ケーブル**に見せかけた悪意のある **USB デバイス**をターゲット PC の USB ポートに刺させるところから始まります。このようなデバイスは **BadUSB** と呼ばれるもので、USB に接続しただけで自動実行され、ターゲット PC に対して自由に操作できるようになるのです。

今回使用した **BadUSB** には、攻撃者が遠隔でターゲット PC 操作をすることが可能になる RAT というものが仕込まれています。そのため感染すると PC 内の重要ファイルや、キーボード入力情報、デスクトップ画面の写真が定期的に攻撃者 PC に送信されるようになり、使用している**従業員に気付かれることなくずっと情報を盗み続けます**。更にこの RAT は他の PC にも感染を拡散する機能を持たせたため、同じ状況が同一のネットワーク内にある PC も広がります。



攻撃者は集めた情報をどんな目的に使用するのでしょうか？目的の一つは、株価を操作して**お金を儲けること**だと言われています。そのため、多くの従業員のデータを盗み見て、株主総会で発表される前の情報や、新製品開発の情報などを手に入れようとします。それらの情報を使って**インサイダー取引などによる不正な利益獲得**を目指します。



この攻撃の特徴は、**USB デバイス**がキーボードやマウスをとして認識され実行されるため、いくつかの前提条件がそろうと、**USB デバイス**を挿しただけで攻撃が成立してしまうという点です。USB やマウスの接続を禁止している会社は少ない、という点を狙った手口ですが、新しいマウスやキーボードの接続まで禁止すると、キーボードやマウスが壊れたとき操作不能になってしまい、使い勝手が著しく悪くなってしまいます。また、感染後のデータ送信も、感染端末が正規の通信として外部に送っている形をとっているため、ファイアウォールがこの通信自体を悪いと判断することが難しい状況を作っています。

この攻撃に有効な対策は、まずは **BadUSB** の存在を従業員に知ってもらい、USB ポートにこれらを挿すこと自体に危険が伴うことを知ってもらうことです。そして、従業員に不審な **USB デバイス**を接続させないように教育するのが効果的です。技術的にはマウスやキーボードを登録制にすることも考えられますが、使い勝手がかなり悪くなるため、運用できる場面は限られます。

このシナリオを通じて学んだことは、**USB ポートに挿しただけで感染するような攻撃があり、そのため、担当者は「登録されていない USB デバイスの使用禁止」というルールを通して、従業員の PC を守ってくれている**ということです。今回の「ダメなものはダメなんです」も理由が分かると**「スッキリ」**しませんか？

もやもや（USBデバイス使用編）

作 Mr.もやもや

第 4 章. 納得できなかった禁止事項の考察

この章では 2 章で述べた**「もやもや」**について、第 3 章で分かったことを踏まえて考察をしていき、筆者らの**「もやもや」**が解消されるまでの道筋を説明していきます。

まず「会社が許可していないフリーソフトの使用禁止」というルールについてです。シナリオ②で起こったような、ソフトウェア改ざんに遭遇しないためにはどうすればよいのでしょうか？みなさんならどう対策しますか？偽のアドレスかどうかを確かめる？でも正しいサイト自体が改ざんされていて、そこでつかまされていたら？(水飲み場攻撃といいます)。セキュリティ意識の高いソフトウェアの企業では、正規のソフトであることを確かめるための番号(ハッシュ値)が提供されていたりします。しかし、バージョンごとに確認が必要です。**日々更新されていくソフトウェアの安全性を個人で毎回確認する根気が皆さんにはありますか？**

実はこれらを解決する最も簡単な方法があります。そう、**「会社が安全を確認しているソフトウェア以外は使わせない」**という選択肢です。何か聞いたことのあるフレーズですね。

また、もう一つ付け加えておきたいことが、**ソフトウェアの改ざん**に関する難易度についてです。私はソフトウェア改ざんには超高度な IT スキルが必要だと思っていました。しかし、理屈を知ってしまえば**実は簡単に実行できてしまう**ことが分かりました。そのため、**素人が思うより、ソフトウェア改ざんはより身近な危険**なのです。

次に「許可されていない USB デバイスの使用禁止」についてです。この**「もやもや」**は、**USB メモリくらい使わせてほしい！**という一般の従業員の要望が背景となっていました。ウイルスチェックをしっかりとすれば感染したものかどうか分かるのに、**ちょっと行き過ぎたルールじゃないのか？**と感じていました。

しかし、シナリオ③で出てきた **BadUSB** の存在を知り、自分たちの考えが甘かったことを実感しました。**BadUSB** は見た目が普通の **USB デバイス**なので、見分けるのが非常に困難です。いったん PC に接続すると、ウイルスチェックを行う前に意図しないコマンドが実行されてしまいますので、今回の**もやもや**の根底にあった**「USB メモリのウイルススキャンをする」という行為をおこなおうとした時点でリスクが発生する**、**ということです。**場合によっては USB の延長ケーブルや USB ハブに仕込まれていたりもしますので、USB メモリ自体が安全でも、延長に使ったケーブルに仕掛けられていて攻撃される、という場合もあります。**これって本当に厄介ですよね？だから、「許可していない USB デバイスの使用禁止」は結構理にかなったルールなのです。**

最後に触れたいのは、ヒューマンエラーについてです。

特にシナリオ①がそうでしたが、人間は不測の事態が起こった時、必ずしも最適な判断ができるとは限りません。また、大勢集まれば必ず一定の割合でミスをする人が現れます。攻撃者はそれが分かっていて、近年の攻撃の多くがヒューマンエラーを狙ったものになっています。

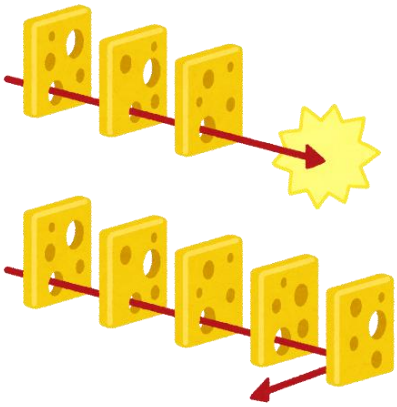
セキュリティ担当者は、不測の事態が起こっても大丈夫なように、社内のネットワーク内に多層の防御を敷いて安全を確保してくれていますが、そのヒューマンエラーの入り口となる一般の従業員の協力が無ければ、この対策は脆弱なものとなってしまいます。つまり、**「もやもや」**を残したままにすることは、会社にとっても従業員にとっても、非常に危険な状態なのです。

どうでしょう、みなさんの**もやもやはどこまで解消しましたか**？

コラム②：標的型メール訓練とスイスチーズモデル

「怪しいメールのリンクをクリックしてしまっても、責めないので IT 管理者に連絡してください」という指示されますよね。「これ絶対、怒られるやつだ！」と、思っていませんでしたか？筆者も中核人材育成プログラムに参加するまではそうでした。でも、真相は、一般の人が想像しているイメージとちょっと違うのです。

ところで、**スイスチーズモデル**というものをご存じでしょうか？これは、リスクマネジメントおよびリスク分析のモデルの一つで、不完全な安全対策をスライスチーズに見立て、複数枚重ねることで穴を塞ぐという考え方です。この考え方では、1 つの穴が突破されたかどうかよりも、全体で侵入を止めようとすることが重要なのです。



中核人材育成プログラムに参加するまでは、筆者もサイバー攻撃は誰かの PC がウイルスに感染して、そこで事象は終わりだと思っていました。しかし攻撃者の目的は、感染した PC を起点に他の PC を次々に乗っ取って機密データを奪い、それを用いて社会的影響を与えるところまでです。そのため、スイスチーズモデルのように多層防御で、攻撃者が目的を達成する前のどこかで、この流れを止めることが重要なのです。

つまり、**「迷惑メールを踏んでしまったら連絡してください」**の真の意味は、犯人探しをしてその人に厳しく注意することではなく、1 つ目の穴を通ったことを IT 担当者が知り、その次の対応を素早く行うために**重要な情報を提供してほしい**、というお願いだったのです。

どうですか？こういう説明を受けると、助けようの精神で、連絡しようと思いませんか？

第 5 章. 「もやもや」に対する筆者らの結論

著者らは本プロジェクトの中でセキュリティルールに感じる負の感情を**「もやもや」**と表現し、その根源に関してと、これをどうすれば**「スッキリ」**にできるのかを考察していきました。

その過程で、**情報セキュリティルールの本質**を理解すれば、**納得感**を持てることが分かりました。しかし、その結論にたどり着くには、十分な学習環境と時間が必要で、情報セキュリティの専門家でない人たちが著者らと同じように、自分で手を動かしセキュリティルールの本質を理解して納得するのは非効率だと感じました。

今回のプロジェクトを通して、**「もやもや」**の原因になるような情報セキュリティルールの記載がつくられる背景には、「難しいルールの真意を理解していなくても対策ができるように」というセキュリティ担当者の**やさしさ**が入っているということを実感しました。

本書のシナリオでも示したように、最近のサイバー攻撃は非常に悪質で、それに対する対策も様々です。複雑な背景が省略され**ちょっと無骨な指示になっているだけ**なのですが、**直感的に合理性が感じられない**ため、**「もやもや」**してしまうのです。

先の章でも述べた通り、近年のサイバー攻撃はヒューマンエラーを狙ったものが中心となってきています。そのため、セキュリティ担当者と一般の従業員との間に**「もやもや」**がある状態は、攻撃者の思うつぼです。そのため、お互いが**「自分の知らない分野で日々戦ってくれているんだろうな…がんばってくれて、ありがとう！」**くらいの気持ちで交流できるのが理想ではないでしょうか？

つまり、最後に言いたいことは

みんな仲よく！

終わり

あとがき

私たちは本プロジェクトを通じて侵入と防御の方法を学んで、ルールを守ることの重要性を再認識できたのと、それまで感じていた**「もやもや」**が**「スッキリ」**に変わりました。
この本を読んでいただいた皆さんも、私たちと同じような感覚を得られますように・・・。そしてぜひ、この気づきを周囲の人たちにも広めてください！そしてルールを守る人と、守らせる人、みんな仲良く協力して、**サイバー攻撃に負けない会社を作っていきましょう。**

謝辞

本書の作成にあたりまして、産業サイバーセキュリティセンター中核人材育成プログラム講師の満永拓邦先生、並びに門林雄基先生には、本書の元となるプロジェクトのメンターとして、ご指導・ご助言、ご支援を賜りました。改めて御礼申し上げます。

そして、本書の作成や本プロジェクトをともに実施した、下記メンバーの皆様、研究に協力してくれたすべての方に感謝します。

最後に、本研究を支え、応援してくれた家族と友人たちにも感謝します。彼らの支持がなければ、この困難な道のりを乗り越えることはできませんでした。心からの感謝を申し上げます。

＜侵入と対策の研究プロジェクト＞
リーダー
・深田　訓章
サブリーダー
・茂木　亮太
メンバー
・渋谷　篤
・永廣　武士
・簇野　公嗣

用語集

用語	意味・解説
ヒューマンエラー	人間が原因となって発生するミスや事故
多層防御	サイバーセキュリティで複数対策、機密情報があるネットワーク内部への侵入を防ぐ手法
フィッシングサイト	ショッピングサイト装った偽のサイトでクレジットカード番号などの個人情報を騙し取るためのサイト
BadUSB	悪意のあるソフトウェアが仕組まれている USB デバイスを用いたコンピュータセキュリティ攻撃
インシデント	事件、事例、事案、事象、出来事といったことを表す単語
ファイアウォール	外部から企業内の PC への不正なアクセスを防ぐためのバリアのようなもの。安全な通信のみを許可し、危険なものをブロックする役割
インストーラー	ソフトウェアをコンピュータにインストールする(その PC で使える状態にする)ための実行ファイル。
バックドア	無許可で利用する目的で、コンピュータ内に（他人に知られることなく）設けられた通信接続の機能
スイスチーズモデル	リスクマネジメントおよびリスク分析のモデル

画像の出どころと引用元について

本書に使用している画像は、以下のサイトのものを使用しています。

(1)ChatGPT で生成したイラスト
これらのイラストは、OpenAI の DALL·E ツールを使用して生成されたものです。特定のプロンプトに基づいて作成されており、プロンプトの内容に従ったビジュアルを提供しています。

(2)Web のフリー素材
以下の Web サイトから提供されるフリー素材を使用しています。

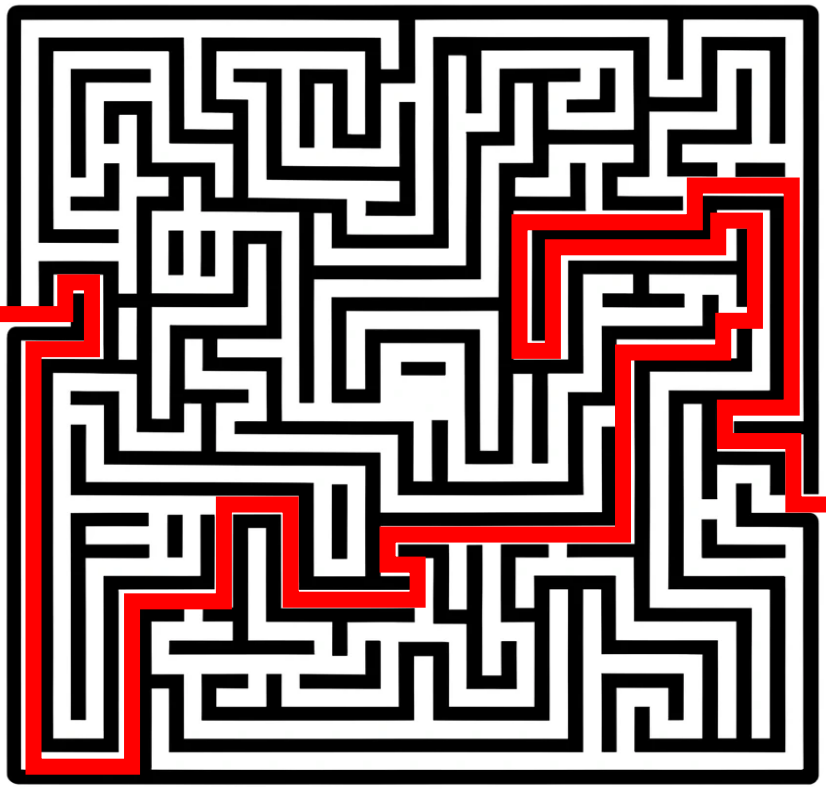
・名前:いらすとや
URL: https://www.irasutoya.com/
著作権の規定の範囲で使用しています。

・名前：SAKURA internet Inc「さくらのアイコンセット」
URL：https://knowledge.sakura.ad.jp/4724/
「クリエイティブ・コモンズの表示 4.0 国際ライセンス（Creative Commons Attribution 4.0 International License）（https://creativecommons.org/licenses/by/4.0/）」で提供されており、著作権の規程の範囲で使用しています。一部のアイコンは加工しています。

・名前:ダ鳥獣戯画
URL: https://chojugiga.com/
著作権の規定の範囲で使用しています。

迷路を解いて**「もやもや」**を**「スッキリ」**に

スタート



ゴール