見ていきましょう。

まず、攻撃者から何を守ればよいかを考えます。攻撃者のターゲットになるものはパソコンであったりその中のファイルであったり、会社の評判であったりとさまざまです。こういった会社の財産のことを、セキュリティの世界では資産と言います。セキュリティ対策とは、**資産**を守るための活動なのです。

さきほど例に挙げたケースでいうと、攻撃された資産は次のようになります。

- **ケース１（不正メール送信）：会社の信用**
- **ケース２（ファイル暗号化）：パソコンのデータ**
- **ケース３（情報流出）：パソコンのデータ**
- **ケース４（不正アクセス）：会社の秘密情報**
- **ケース５（SNS炎上）：会社の評判**

そしてセキュリティ問題にはかならず原因があり、これを**脅威**と言います。自然災害なども脅威ですが、本書では攻撃者がいて、その人が悪意のある行動をとること。つまり、犯罪かそれに準じる行為を脅威とします。

さきほどのケースにおける脅威は次のようになります。

- **ケース１（不正メール送信）：コンピュータウイルスをばらまいた攻撃者**
- **ケース２（ファイル暗号化）：コンピュータウイルスをばらまいた攻撃者**
- **ケース３（情報流出）：紛失物の窃盗と分析を実施した犯罪者**
- **ケース４（不正アクセス）：クラウドサービスを狙う攻撃者**
- **ケース５（SNS炎上）：ライバル企業の社員**

そして、これらの脅威が資産に被害を与えたということは、どこかになにかしらのスキがあったはずです。攻撃者から見ると、カモにしやすい**問題点**があったのです。セキュリティの世界ではもろくて弱い部分という意味で**脆弱性**などともいうこともありますが、場合によっては狭い意味で使われることもあるので、本書では主に問題点という言葉を使います※10。

５つのケースでは、次のような部分に問題点があったと考えられます。

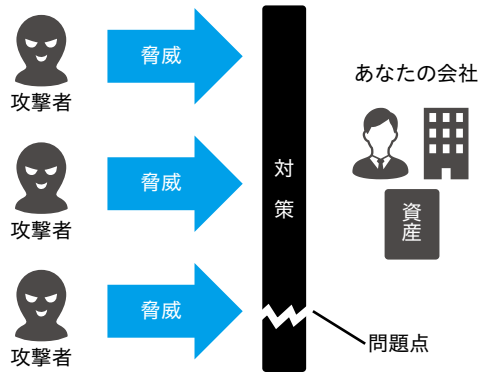
- **ケース１（不正メール送信）：パソコン、またはその利用者のウイルス対策**
- **ケース２（ファイル暗号化）：USBメモリ内のプログラムのウイルス対策**
- **ケース３（情報流出）：パソコンのハードディスク暗号化**
- **ケース４（不正アクセス）：クラウドサービスの欠陥、またはパスワードの管理**
- **ケース５（SNSの炎上）：社長の行動**

こうしたことが起きないようにセキュリティの**対策**が必要になります。例としては、次のようなものがあります。

- **ケース１（不正メール送信）：ウイルス対策をする**
- **ケース２（ファイル暗号化）：USBメモリは利用しない**
- **ケース３（情報流出）：パソコンのハードディスクを暗号化する**
- **ケース４（不正アクセス）：クラウドサービスにログインするためのパスワードは使いまわさない**
- **ケース５（SNSの炎上）：問題行為を慎むよう教育をする**

これらはあくまで例なので、やれば必ず問題が起きなくなる、というわけではありません。また、現実的には難しいという場合もあるでしょう。しかし、どうすれば問題が起きなくなるかを一度は考えておくべきです。

これまで見てきた資産、脅威、問題点、対策という４つの考え方は、本書にこれから何度も出てきます。図にまとめると**図1-1-6**のようになります。必ず覚えておいてください。



●図 1-1-6：資産、脅威、問題点、対策の関係

※10 本書では脆弱性の厳密な定義やCVE、CVSSに関しては説明しません。脆弱性は「アタック・サーフェス（攻撃対象となる部分）に存在する悪用され得るバグ」という定義を使う場合が多いと思いますが、これも読み進める上で意識する必要はありません。

クラウドから統合管理できる、企業向けの製品か

会社向けか個人向けかで一番違うポイントがここになります。特にエンドポイント系の場合、セキュリティソフトをインストールしたパソコンやスマホ、その他の機器をまとめて管理（統合管理）できるかは確認しましょう。統合管理ができると、何か問題があったときにその機器を使っている人だけでなく管理者にも通知メールを送ることができ、各利用者が勝手にソフトウェアをアンインストールしたり設定を変えたりしても管理者の側から確認できます。

また、その管理ツールがクラウド型であるかも重要です。かつては社内に管理用のサーバーを作る方法が主流でしたが、不便なので現在は減っています※4。**図3-1-3**のようにクラウドから管理できることを確認しましょう。

なお、製品によっては統合管理が必要ない場合もありますので、詳しくはITサービス会社に確認してみてください。

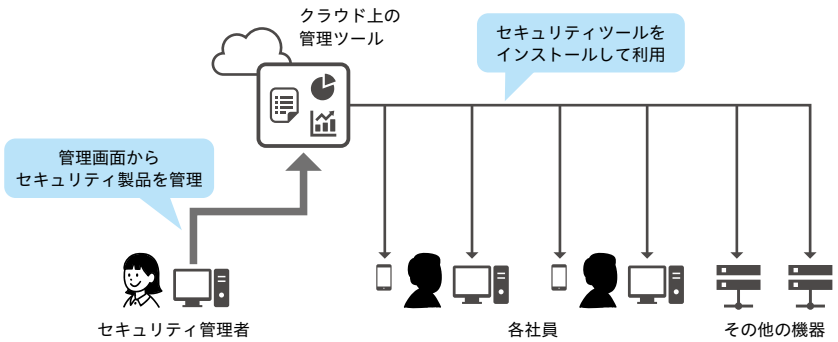


図 3-1-3：クラウドからの統合管理

競合製品やサービスにはどのようなものがあるのか、それらの製品とは何が違うのか

どのセキュリティ製品・サービスにもそれぞれのコンセプトがあり、どの部分が強みなのかは異なります。買おうとしている製品・サービスが自分の会社に合っているかを確認しておきましょう。

※4　インターネットや社内ネットワークに接続できないコンピュータの場合、こうした管理をすることはできませんので、統合管理をあきらめる場合もあり得ます。

採用事例はどの程度あるのか

国内未導入の製品を勧められることはめったにないと思いますが、一応注意しておきましょう。新製品・新サービスはバグが多いこともあるので、特に小さな会社では手を出さないほうが無難です。大企業向けの事例しかなく、小さな会社で使ったことがない、という製品やサービスにも注意が必要です。

価格はいくらか

最後に値段です。重要性や相場に合ったものか、しっかり相談しておきましょう。多機能だと値段は上がりますが、複数製品を買わなくてもよくなります。２年以上利用する契約にしたり、パソコンと一緒に買ったりすれば、安くなることもあります。

評価テストのときにチェックすること

どのセキュリティ製品・サービスを検討するかを決めたら、次は評価テストに入ります。その際に意識したいポイントについて解説します。セキュリティを強化するという意味では役に立つものでも、実際に会社で使うのは難しいということもあるので、確認しておくべき部分をしっかり確認しておきましょう。

法人向けの製品・サービスはたいていの場合評価テストに２週間～１か月程度の期間をもらえますし、そうでない場合は無料版を用意しているものもあります。下記の項目をチェックしながら検討してみてください。インストールしたり機器を設置したりするのが面倒かもしれませんが、ここが山だと思って乗り切りましょう。

ほかの仕事に問題が出てこないか

たとえばパソコンにアンチマルウェアをインストールしたら、Microsoft Excelやブラウザがまともに動かなくなった、といった問題です。最近はずいぶんマシにはなりましたが、ソフトウェアには相性がありますので、まったく使えなかったり、ほかのソフトウェアに影響が出たりする可能性はゼロではありません。ネットワークやコンピュータが遅くなるなども、実は珍しいことではありません。仕事ができないのでは話になりませんので、選択肢から外しましょう。

使っているマルウェア対策ソフトにはバンキング操作の際に他のサイトへ誤ってアクセスしないための保護システムが用意されていましたので、これも有効化しておきます。

これらを整理すると、次のような表（**表4-2-1**）ができました。

ヒグマ水産加工ではこうした対策をすでにやっているところもありましたが、未実施のものもありました。ここで、「未」となっているのがこれから実施する対策の候補です。これを今すぐやるかどうかはまだ考えませんが、恐らくはこの中からいくつかを選んで予定に入れることになるでしょう。

このような流れで、ほかの重要資産についても考えていきます。

資産	管理方法	攻撃者の観点	悪用の対策	実施
現金	XX銀行	ATM/銀行窓口から不正にお金を引き出す	カードは使うとき以外は金庫に入れる	済
現金	XX銀行	ATM/銀行窓口から不正にお金を引き出す	暗証番号を目立つところに書かない	済
現金	XX銀行	ATM/銀行窓口から不正にお金を引き出す	不審な人物にカードや暗証番号の情報を要求されたときの対策方法を教育する	未
現金	XX銀行	インターネットバンキングに直接アクセスする	パスワード管理ツールで複雑なパスワードを設定する	未
現金	XX銀行	インターネットバンキングに直接アクセスする	二要素認証を設定して、ログインには毎回スマホに送られる6ケタの番号を使うようにする	未
現金	XX銀行	インターネットバンキングに直接アクセスする	普段使っているパソコン以外からアクセスがあった場合はメールが通知されるようにする	未
現金	XX銀行	インターネットバンキングに直接アクセスする	一定期間自動で保管されるアクセスログを定期的に保存しておく	済
現金	XX銀行	パソコン・スマホを乗っ取ってインターネットバンキングを利用する	バンキング用の専用端末を用意する	未
現金	XX銀行	パソコン・スマホを乗っ取ってインターネットバンキングを利用する	銀行を名乗るメールのURLをクリックしてサイトアクセスすることは避けるか、銀行から来たと思わしきメールに対して電話で銀行に確認し、本当に送ったのかを確認する	未
現金	XX銀行	パソコン・スマホを乗っ取ってインターネットバンキングを利用する	パソコンやスマホのアップデート・パッチ適用を徹底させる	済
現金	XX銀行	パソコン・スマホを乗っ取ってインターネットバンキングを利用する	パソコンやスマホにマルウェア対策ソフトを入れる	済
現金	XX銀行	パソコン・スマホを乗っ取ってインターネットバンキングを利用する	OSへログインするときに複雑なパスワードを設定する	済
現金	XX銀行	パソコンを解体してハードディスクを抜き取り、アクセス方法を読み取る	パソコンのディスク暗号化を実施する	未
現金	XX銀行	パソコン・スマホを乗っ取ってインターネットバンキングを利用する	パソコン・スマホのブラウザなどに保存したバンキングの情報を消し、記録できないように設定する	未
現金	XX銀行	パソコン・スマホを乗っ取ってインターネットバンキングを利用する	マルウェア対策ソフトのバンキング保護機能を有効化する	未

表 4-2-1：現金のセキュリティ対策のまとめ

資産全体の対策を考えよう

重要資産の対策が終わったら、それ以外の資産を保護することについても考えてみましょう。ただし、重要資産を対策する中で、その他の資産も一緒に対策されることが多いため、特別に考えるべきものだけ検討しておきます。

ヒグマ水産加工では、リストに挙げた資産のセキュリティ対策を以下のように整理しました。

- **業務用のパソコン**
  →今までの対策で十分と判断した
- **倉庫の商品**
  →入退出管理と定期的な在庫の棚卸を実施しているので、それ以上は対策しない
- **社外秘ファイルボックス**
  →鍵をかけられるケースを新たに購入してそこへ入れることにする

これらのサービスでは、大きめのデータも簡単に送れますし、メールサーバーがいっぱいになることもありません。誤送信の際には、まだ開いていないようであれば、元のファイルを消すことで解決できます。

しかし、セキュリティの観点からすると危険な場合もあります。転送サービスで使っているパスワードが漏えいしてしまうと、やりとりしているデータが攻撃者に奪われてしまうこともあるかもしれません。

また、そうしたサービスは送受信する両者が納得して初めて利用できるものなので、全く知らない相手の場合は、メールにファイルを添付することが多いと思います。重要な添付ファイルを送る方法としては、本書では以下を推奨しておきます。

- **情報を送る前に不要な情報／必要な情報を関係者に確認する。**
- **送信する前に宛先を全員確認する（BCCの設定漏れがないか、同姓や同名の間違いがないかなど）**
- **添付ファイルは暗号化しない**

まず、奪われたら困る情報を取り扱うわけですから、添付ファイルのついたメールを出す場合は相談してから送るようにしましょう。誰にどのような目的で、どのようなデータを送信するのか、周囲に確認するのが確実です。

それから、送信先を全員確認することも重要です。相手先を誤るのは非常に多いケースで、これはどんな技術的な方法でも対策できません。値引きした価格を間違った顧客に送ってしまった場合は最悪ですし、設計図を社外の人に送ってしまったら完全な情報漏えいです。現実的にはこちらのほうがセキュリティ的に重要ですので、確認を怠らないようにしましょう。

そして最後の項目では、暗号化「する」ではなく「しない」と書いていますが、これは次の項目で説明します。

ファイルを暗号化して添付することはやめよう

本項では、添付ファイルを暗号化することの是非について解説します。まず、日本ではかなり長いこと、以下のような方法が主流となっていました。

1. **添付ファイルをzipで圧縮してパスワードを設定する**
2. **パスワードを設定したzipファイルをメールに添付して送信**
3. **2通目のメールでパスワードを送る**

仕事でメールをよく使う人であれば、この方法を見たことはあると思います。特に官公庁などでは、この方法でなければ送付してはいけないという内規を作っている場合もあります。

ですが、この方法は面倒なだけでなく危険なので、本書ではおすすめしません。この方法はPPAPなどと呼ばれ、たいていは悪い意味で使われます（**図5-4-4**）。というのも、次のような問題があるからです。

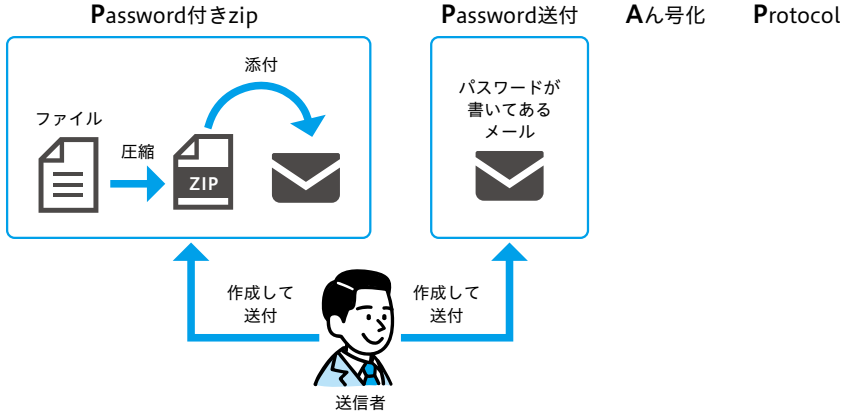


図 5-4-4：PPAP と呼ばれる添付ファイルの送付方法

情報が漏えいしたときに調べるのが大変

会社同士の約束ごととして、万が一関係しているメールなどが漏えいした場合は、その内容を報告することは重要です。しかしメールを暗号化していると、本文や件名から検索できないため、どの情報が漏えいしたのかを探すことがとても大変です。ウイルスに感染したパソコンから外部にメールが転送されることはよくあるので、それを考えると暗号化しないほうが正解です。

この方法でマルウェアが送り込まれるとチェックできない

メールにマルウェア付きのファイルが添付されていても、それをチェックで

した上で多要素認証を使ってもらうことです。これらは徹底するようにしましょう。

オンライン会議ツールを使うときの注意点

新型コロナウイルスの流行以降、自宅やオフィス以外の場所でオンライン会議ツールが多く使われるようになりました。Zoom、Microsoft Teams、Google Meetなどをはじめ、様々なツールが販売、利用されています。これらは自分の会社で使っていなくても、取引先から指定されて利用が必要になることもあります。

こうしたツールは、たとえば会話の録音や映像などを関係ない人に奪われ、情報が流出することにつながる可能性があります。チャット欄などにファイルをアップロードできる場合は、それを盗まれてしまうこともありえます。また、退職した社員のIDが、元社員やそれを教えてもらった人によって悪用されることも考えられます。

こうした問題を防ぐには、次のような使い方を徹底してもらうことが考えられます。

- **暗号化機能を有効にして利用してもらう**
- **ミーティングIDを指定しておき、それを知らない限り入れないようにしてもらう**
- **招待者、参加者が適切かを確認してもらう**
- **物理的な使用場所（オフィスから入るか、自宅から入るかなど）を指定してもらう**
- **カメラを使って本人確認をする**

暗号化機能は通信を傍受されたときに、内容を奪われることを防ぎます。最近はたいていのツールに入っていますが、設定しだいで暗号化機能を解除できるものもあります。暗号化を使わない（意図的に解除する）理由はたいてい、通信の遅延を防ぐためですが、基本的には有効にすべきです。声が聞こえにくい場合は、一般回線の電話を併用することも検討します。

それから、参加者のみにミーティングIDを連絡し、そのIDを知らないと入れないように設定しましょう。YouTubeのような広く公開される動画サービスと違い、オンライン会議ツールはあくまで限定された参加者が使うことを意図して作られている場合がほとんどです。

また、Zoomであればパーソナルミーティングという、一人一人に配布されるミーティングIDがありますが、常にこれを使うことは、セキュリティ上の問題につながります。この番号が誰かに知られてしまうと、迷惑メールや迷惑電話のように不正な連絡が来る可能性があるからです。

複数の参加者が入る公開ミーティングを実施する場合は、都度新しくミーティングIDを作ったほうが安全です。これにより、招待された参加者だけがミーティングへの参加方法を受け取り、参加することができます。

会議を始めるときは、招待者と参加者が正しいかを必ず確認しましょう。見覚えのない人が入っていたら、その人はファイルを盗んだり話を盗み聞いたりしようとしているのかもしれません。招待を通知するメールなどを事前に送り合うと思うのですが、そこで参加が確定したメンバーが入っているか、招待したメンバーと違う場合は誰なのかわかっているかを確認してもらいます。

加えて、周りに仕事と無関係な人がいるようなカフェではオンライン会議は避けましょう。しゃれた新しいビジネススタイルに見えるかもしれませんが、恰好よりも会議の内容が聞こえないようにする方が重要です。シェアオフィスなどを利用しているのであれば、防音設備のある個室を予約しておきましょう。

最後の注意点として、参加者とその居場所を確認するため、**会議が始まったら、お互いに映像を一度はオンにしてもらう**ことはやっておきましょう。顔や服装、自室などを見せるのは気が向かない、という人も多いかもしれません。しかしセキュリティの観点からは、お互いに顔を見ておくのは重要なことです。自分以外の周囲の様子を見せたくない場合は、バーチャル背景を使いましょう。

これにより、見覚えのある相手か、名前と顔は一致しているか、その人は参加する予定があったか、背景に不審なところがないかなどがわかり、情報流出を防ぐことができます。お互いの表情がはっきり見えることで商談がうまくいくことにもつながります。

出先でWi-Fiを使う

外出先、たとえば空港やカフェ、ホテル、図書館などに設置してある無線LANを利用することは、現在のセキュリティ状況を考えると**おすすめできません**。

業務用品の調査シート

業務で使用している物品を確認して、右の欄に〇をつけてください。

持ち物	所属	社外利用	備考（修理中、紛失、複数あるなど）
（例）パソコン	(支給)・私物・不明	(有) 無	
	支給・私物・不明	有・無	
	支給・私物・不明	有・無	
	支給・私物・不明	有・無	
	支給・私物・不明	有・無	
	支給・私物・不明	有・無	
	支給・私物・不明	有・無	
	支給・私物・不明	有・無	
	支給・私物・不明	有・無	
	支給・私物・不明	有・無	
	支給・私物・不明	有・無	
	支給・私物・不明	有・無	
	支給・私物・不明	有・無	
	支給・私物・不明	有・無	
	支給・私物・不明	有・無	
	支給・私物・不明	有・無	
	支給・私物・不明	有・無	
	支給・私物・不明	有・無	
	支給・私物・不明	有・無	
	支給・私物・不明	有・無	

※リストになくても業務上ないと困るものがあれば書き足してください。
※個人の衣類や文房具、カバンなど、なくても簡単に替えが効くものは書かなくてかまいません。

パソコン・スマホの調査シート

普段の仕事で使っているパソコンやスマホ、タブレットについて質問します。１台あたり、１枚を使って答えてください。

■ **あなたの名前を書いてください。**

_____

■ **調査対象のパソコン／スマホ／タブレットの管理番号、またはシリアルナンバーを書いてください（不明の場合はわかるように書いてください　例：自席のパソコン）。**

■ **機器の種類を書いてください。**

パソコン ・ スマホ ・ その他（具体的に：　　）・ わからない

■ **OSを書いてください。**

Windows ・ Mac ・ iPhone／iPad ・ Android ・ その他 ・ わからない

■ **OSのアップデートはやっていますか。あてはまるものを選んでください。**

会社が実施 ・ いつもやっている ・ 気がついたらやる ・ やっていない ・ わからない

■ **自分だけが利用できるように、パスワード・パターンロック・顔認証などを設定していますか？**

やっている ・ やっていない ・ わからない

■ **パスワード・パターンロック・顔認証を設定している方のみ回答してください。何を設定していますか？**

パスワード ・ PIN ・ パターン ・ 指紋認証 ・ 顔認証 ・ その他 ・ わからない

■ **パスワード・パターンロック・顔認証を設定している方のみ回答してください。何回失敗したらロックされますか？**

（　　回）・ 設定はしていない ・ わからない

■ **アンチマルウェア（アンチウイルス・ワクチンソフトなど）を利用していますか？**

会社で購入 ・ 自分で購入 ・ やっていない ・ わからない

■ **データのバックアップをとっていますか？**

会社でとっている ・ 自分でとっている ・ やっていない ・ わからない

■ **ウイルスが見つかった、データが消えた、機器の盗難があった、その他の問題があったとき、誰に報告・相談しますか？**

（　　さんに報告・相談する）・ 決めていない ・ わからない

■ **機器の中に入っている、仕事上大事なデータは何ですか。1〜3個まで書いてください。ファイル名ではなく、何に使っているどのようなデータかを書いてもらうようお願いします。いくつかをまとめて書いてもかまいません。（例：契約書、設計書）**

1：
2：
3：