第7章

中小組織向け

セキュリティ向上が利潤追求につながることを理解しよう

人材・体制・資金などが限られた中小組織にとって、通常業務をこなしながらセキュリティ対策を講じるための負担は少なくありません。しかし、企業経営においてセキュリティ対策を省くことはできません。セキュリティ対策に投資すべき理由、テレワークを安全快適に利用するために必要なルール作り、企業だからこそ気を付けたいサイバー攻撃、そして最低限把握しておきたいセキュリティ関連の法律などを学びましょう。

1 社内・社外のセキュリティを向上しよう

1.1 セキュリティ対策を実施して負のコストを発生させない

業績を圧迫するコストとは、どうやって発生するのでしょう。1つは業務を遂行する上で支払わなければいけないお金が増えるときです。もう1つは、イレギュラーな事態が発生して、そのリカバリ▶用語集P.203のために人、お金、時間を割くときです。

この後者のロスというのは、なにか問題が発生してそれに誰かが掛かり切りになり、その期間中「利益を生む」ことができなくなることで発生する完全なる負のコストです。

ただ、トラブルを根本的に防ぐことは難しいので、その発生を予期して備え、利益を生まない負のコストによる業績の下ブレをなくす努力をするわけです。

サイバー攻撃▶用語集P.196による突発的なトラブルは、まさしくこの例に当てはまります。したがってサイバーセキュリティを強化して備えるメリットはここにあるのです。

「セキュリティを強化する」といわれても「正直うちが攻撃されるなんて万に1つもないだろう」というのが小さな会社やNPOの運営者の本音ではないでしょうか？

しかし、現在の攻撃者▶用語集P.196は、業種や企業規模に関係なく無差別に攻撃してきます。サイバー攻撃の数も被害額も年々増加傾向にあるのです。

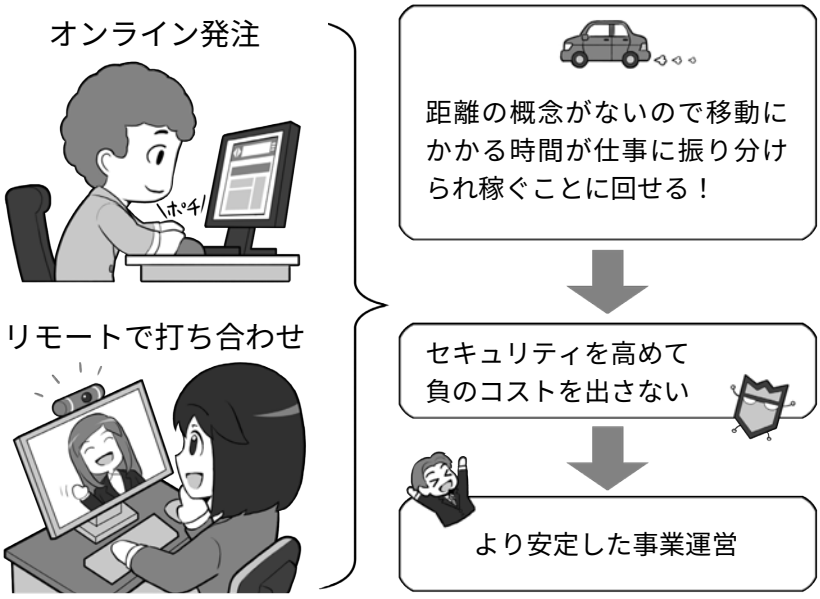
近年では「セキュリティ・バイ・デザイン」▶用語集P.198という考え方が一般的になりつつあります。企業のITシステムや業務プロセスなどを設計する段階でセキュリティ対策を組み込んでおき、サイバー攻撃による不測の事態に備えるのです。

小さな会社やNPOも例外ではありません。持続的な運営を行うために、きちんと備えましょう。

負のコストの発生例

利益を生むためのコストは必要ですが、備えをしなかったために発生し、そのリカバリのために多大なるマンパワーを割くことは「利益を生まない」完全なる負のコストです。そういったことが起こらないように準備するコスト（費用）は、実は利益を生むための投資なのです。

インターネットの利点を生かしてコストを減らす



せっかくのIT投資が、セキュリティの事故が原因で負のコストを生むこともあります。セキュリティもIT投資の一部として捉えることが重要です。

1.2 セキュリティ対策に必要な投資資金を確保する

しかし、「セキュリティに事前に備えるといわれてもそんな資金ないよ…」という経営者の方も少なくないのではないでしょうか？

セキュリティ対策が不十分なIT投資は、不必要な「負のコスト」を発生させる可能性があり、予期しない下ブレを起こす原因を抱えていますので、健全な投資とは言えません。また、セキュリティ対策不足によるトラブルは自分たちへの影響だけでなく、顧客や投資家などの関係者にも迷惑をかける可能性もあります。企業や団体の経営姿勢も問われますので、セキュリティ対策を後回しや後付けにせず、セキュリティ対策を含めたIT投資を検討してください。

また、近年では企業の業務システムをクラウド業務スイートに切り替えるケースが増えています。クラウド業務スイートは、業務用ソフト▶用語集 P.198、クラウドストレージ、ウェブサーバ▶用語集 P.194などが1つのパッケージとして提供され、どこからでもノートパソコンなどでアクセスして業務が行えます。これにより従来は会社に縛られていた従業員がテレワーク▶用語集 P.199環境で仕事ができるようになったり、スマホを利用して安全に業務連絡を行ったりすることが可能になります。

アウトソース▶用語集 P.193できることも増えています。自前で対応するよりも外部に委託する方がコストが安く実現できる場合もあります。

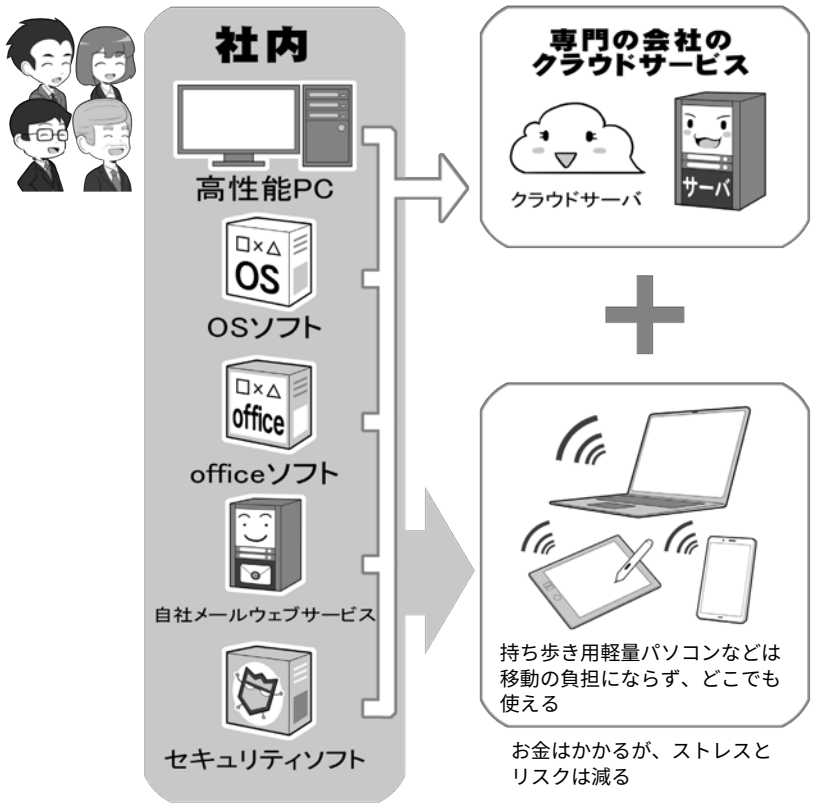
こういった新しいシステムや環境は、セキュリティ対策も込みで提供される場合や、これまでバラバラだったコストが集約・整理されて軽くなる場合があり、総コストが従来より安く済むこともあります。ただし、逆にコストがかかる場合があるので、導入前にしっかり確認しましょう。また、クラウドサービスは設定次第で誰でもアクセスできる場合がありますので、設定に注意して利用する必要があります。

その他、ある程度計画的に時間と費用を取れるのであれば、企業の業務システム構成に、ゼロトラスト▶用語集 P.198の考え方を採用することで、テレワーク環境下でより使いやすいシステムにできる可能性があります。

ゼロトラストに即切り替えは難しいことが多いですが、将来を見据えるのであれば検討の価値はあります。

そのようにセキュリティを後回しや後付けにしないIT投資によって業務効率改善が実現すれば、事業運営と高いレベルのセキュリティを両立できます。それが企業や団体にとっての生存戦略の1つになるのです。

面倒なことをアウトソース（外部委託）するのも1つの手



先進的なIT企業では、デスクトップパソコンを廃し、パッケージ版のソフトウェアを廃止し、軽量なノートパソコンと携帯電話回線、そしてクラウドベースのソフトウェアやシステムに活用することで、固定的な机も、オフィスも、出勤すらもなくしているケースもあります。また、社内や団体の業務もアウトソースすることで、一層身軽になることもできます。

総務省では「クラウドサービス提供・利用における適切な設定に関するガイドライン」を公開しているので、詳しくは以下をご覧ください。
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00149.html

2 災害時の会社のために事業継続計画(BCP)を作ろう

2.1 打たれ強くあるために、どこでも作業できる能力

激しい天災に見舞われる我が国では、災害時にどのように事業継続を行うか、人・モノ・金などの面から事業継続計画(BCP)▶用語集P.190を、きちんと考えておかなければなりません。その備えがないと、災害時に廃業の憂き目にあう可能性も高くなります。

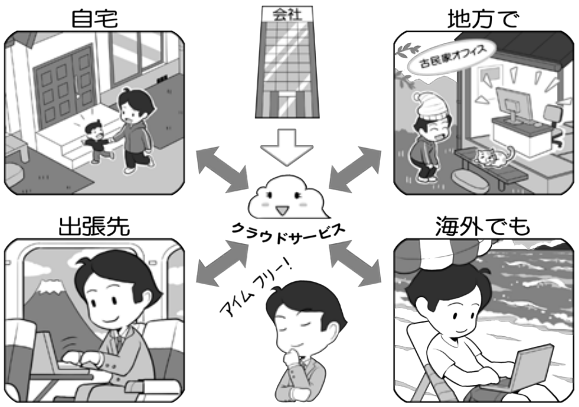
中小企業庁では、「中小企業BCP策定運用指針」のウェブサイト*内で、20項目による「BCP取り組み状況チェック」項目を設けています。ここではIT関連のアイデアから、その項目を達成するのに役立つと思われるものを紹介します。

最も役に立つのは、ネットがあればどこでも仕事ができるスキルや環境作りです。

生産設備などがあってその場で離れられない職種ではなく、オフィスでの作業を行う業種・職種の人は、インターネットの利点をフルに生かせます。データを主としてクラウドサービス上に保存し、あとはアクセスするパソコンなどの機器とネット環境があれば、基本的にはどこからでも作業を行うことができます。

また、作業に利用するソフトを、パッケージ版ではなくクラウド版で購入しておくと、災害にあってパソコンが壊れてしまっても、避難先でノートパソコンを購入して、ネットからソフトをダウンロードすれば、かなりのレベルで作業環境を復旧することができます。

クラウドを活用できれば打たれ強くなる



インターネットとは「距離の概念がない世界」です。これはイコール「どこにでもあるが、どこにでもない」と、少し哲学的な考え方になりますが、うまく使いこなせば、物理的な世界の制約を受けないだけでなく、物理的な世界の災害のダメージを受けにくくなることでもあります。

その1つのポイントは、クラウドをうまく使いこなした仕事の仕方だといえます。

最近ではこういったソフトは、クラウド上のデータの閲覧や軽微な修正に関しては、タブレットやスマホからブラウザ▶用語集P.202を使って行えるようになっているので、スマホさえ手元にあれば、とりあえずは手も足も出ない状況にはならないでしょう。

注意するべき点は3点。1点目はそういったクラウドのデータにアクセスしての作業は、ネットカフェなどでも可能ですが、不特定多数の人が触るパソコンは攻撃者が触っている可能性も高いので、そういった場所でのID▶用語集P.191やパスワード▶用語集P.200を入力する作業はやってはいけないこと。

2点目。災害時には被災者が通信を円滑に行えるよう暗号化▶用語集P.194されていない無線LAN▶用語集P.203が各所で提供されます。これも攻撃されやすいポイントなので、使用する場合はVPN▶用語集P.193を使うこと。

3点目として、専門用語ではBYOD(Bring Your Own Device)▶用語集P.190というのですが、災害時であっても個人が所有する機器で業務を行っていると、うっかりマルウェア▶用語集P.203に感染すれば仕事の情報も漏えいする可能性があります。複数台持つのは面倒ですが、セキュリティを鑑み、業務用には別の機器を用意しましょう。

なお、「このどこからでも作業できるというスキル」は、別段災害時のためだけのものではありません。テレワークといって在宅でも作業ができるようにしたり、出産子育て時にも離職しないで仕事を続けられるようにしたり、あるいは地方に出かけて現地のコワーキングスペースを利用することで自由度高く働き、社員や会員のクオリティオブライフを向上させることもできます。

勿論、ためらいなく出張できるフットワークの軽い企業・団体になるには環境作りが重要です。

* 中小企業庁 中小企業BCP策定運用指針ウェブサイト https://www.chusho.meti.go.jp/bcp/index.html

2.2 人的損失をリカバリする能力

もう１つの備えは、社長や代表者、従業員や会員に人的被害が発生した場合にどう対処するかです。

例えば、社長や代表者が事故で亡くなってしまった場合のことを想定してみましょう。

小規模の企業や団体では専任のIT担当者がおかれておらず、社長や代表者が管理者を兼ねているという例は決して少なくありません。そうした企業や団体では、業務用のIDとパスワードなどの管理をどうするかが、事業継続の鍵になる可能性があります。

このため、普段から社長や代表者の他にデジタルデータなどの副管理者を置くなどの手段を取っておくとよいでしょう。いわば人的なバックアップ▶用語集P.201体制です。

そのなかで大切なのは、上記のとおり業務に使われるウェブサービスのIDやパスワードなどの管理です。

もし代表者が管理している場合、そのデータがスマホに保存されていて、その人しか解除するPINコード▶用語集P.191を知らなかったとすると、場合によっては事業継続が困難になります。

先ほども述べましたが、そういった意味では管理用の機器は、個人の機器と分離するということが重要ですし、そのPINコードなども複数人が持つことが重要です。

また、それが難しい場合は、例えばクラウドでもアクセス可能なパスワード管理アプリ▶用語集P.200を利用し、そのマスターパスワードやPINコードを、弁護士に託し、なんらかの理由で本人による事業継続が困難であると判明した場合は、弁護士に情報を開示してもらうのです。それは昔、貸金庫の鍵を弁護士にも持っていてもらったのと同じです。

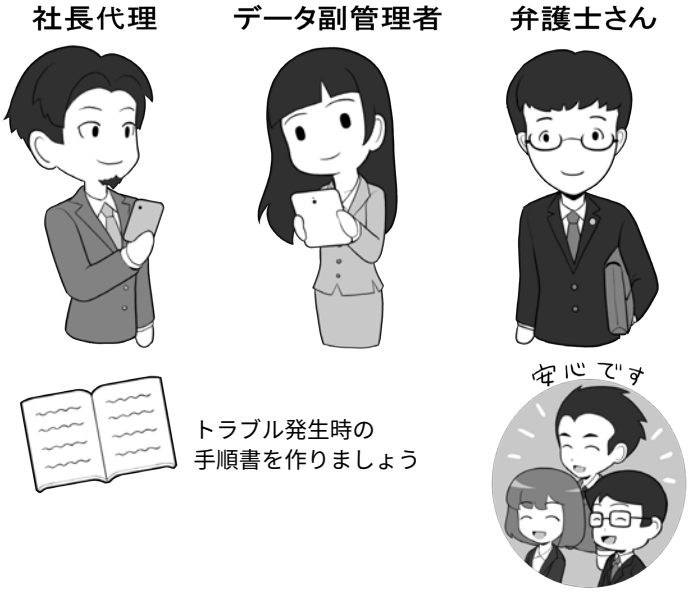
このように災害に遭った場合、どのように事業継続するか、そのバックアップ体制を考えましょう。

具体的に事例をあげ、それにしたがってどのように解決するか、シナリオを作り、それを社内や団体の中で共有しておくとよいでしょう。すべては「想定外」にならない想像力がものをいいますから。

１人しか管理者がいないと…

デジタル化のメリットは、逆に管理者になにかあった場合「物理的な手掛かりがない」ことにもつながります。また、セキュリティをきっちり固めることは、その入口の鍵をなくすとすべてにアクセス出来なくなる可能性もあります。したがって、トラブルが起こったらどうやってリカバリするか、あるいはデータのバックアップだけでなく、人的なバックアップをどうするかをきちんと考えておかなければなりません。

万が一に備えて人のバックアップ



トラブルに対処する手順書は、物理的な災害による建物や機材の棄損、サイバー攻撃の対処などだけでなく、人的な損害に対するリカバリも定めましょう。また、人的なバックアップをすることで、重要なデータへのアクセスする資格を複数の人が持つ場合は、だれがアクセスしたかが明確に分かる仕組みにするか、外部の信頼がおける弁護士さんなどに業務を依頼することなどを検討しましょう。

3 テレワークとアウトソーシングをうまく利用しよう

3.1 テレワークとBYOD-Bring Your Own Device

テレワーク、リモートワークという働き方は昔からありましたが、2020年以降のコロナ禍により全国的に普及しました。

職種や企業などの方針にもよりますが、デスクワークの作業の多くはオフィスに出勤せずとも可能です。現在はクラウドサービスが発達しているので、安定したインターネット環境が整備できれば世界中のどこからでも同じデータを共有しながら業務に従事できます。テレワーク普及によって、BYOD（Bring Your Own Device）という、企業から貸与される端末を使うだけではなく、従業員が個人で所有している端末を業務に使う動きも広がりました。

BYODは、従業員が所有している端末を業務に使うようになるため、従業員が使い慣れた環境で効率的に業務を遂行できたり、企業も端末を配布する費用負担がなくなったりという長所がある反面、端末側に業務情報や認証情報が残ったり、企業が貸与する端末と比較してセキュリティレベルが劣ったりする短所、懸念もあります。

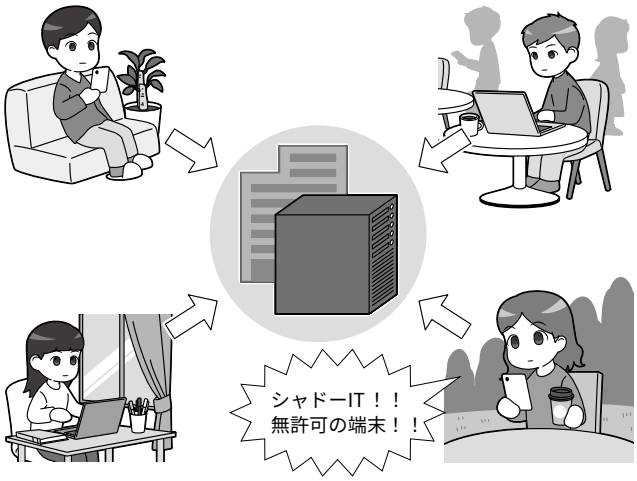
BYODの実施にあたっては、従業員が端末を盗難された場合など、想定されるセキュリティ上のリスクを企業側が事前に把握しておく必要があります。

BYODの実施には企業が運用のルールを設定すべきですが、このルールを理解しない一部の従業員が「シャドーIT」という問題を起こすことがあります。シャドーITとは、企業が許可していない端末やサービスのことを指し、従業員が許可していない端末から社内のシステムを利用してしまうケースがたびたび生じるようです。例えば、業務連絡にLINEなどを使用していたら、従業員の転職後、図らずとも自社の秘密情報が他社に知られてしまった、といったリスクもあり得ます。

しかし、シャドーITは従業員が社内の環境や端末に不満を感じているからこそ生じがちな問題であり、従業員がシャドーITを使わなくても効率的に業務が遂行できるよう、企業側で社内の制度や設備を整備する、というアプローチも考慮しましょう。

総務省もテレワークの環境を整備しやすくするため、ガイドラインや手引きを公開しているので、積極的にチェックしてください。

BYODと気を付けたいシャドーIT



シャドーITはBYODを実施する企業でよく起こる問題です。企業側は、従業員が端末を盗難された場合など、想定されるセキュリティ上のリスクを企業側が事前に把握して、従業員が効率的に業務を遂行できる環境を整備しましょう。

テレワークにおけるセキュリティ確保｜総務省
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

テレワークセキュリティガイドライン（第5版）（令和3年5月）｜総務省
https://www.soumu.go.jp/main_content/000752925.pdf

中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）｜総務省
https://www.soumu.go.jp/main_content/000816096.pdf

3.2 効率的なアウトソーシング

もう1つのインターネット時代のメリットは、気軽に専門的な業務をアウトソーシング(外部委託)できることです。

従来であれば、なにかモノを発注する、業務を委託するといった場合、物理的な距離に縛られました。しかし、現在では、自分が望むサービスをインターネット上で検索すると、さまざまな専門の業者を、オンラインで見つけることができます。

例えば、例えばチラシやパンフレット、および印刷物全般などは、オンラインの印刷業者がウェブサイトを設けており、そこで目的のものを探して紙質などを指定すると、どれぐらいの部数がどれぐらいの印刷日数で、いくらぐらいでできるかが明確になっています。

あとは発注側が、業者が受け付ける形式のデータを作るスキルがあれば、24時間365日印刷物が発注できるわけです。

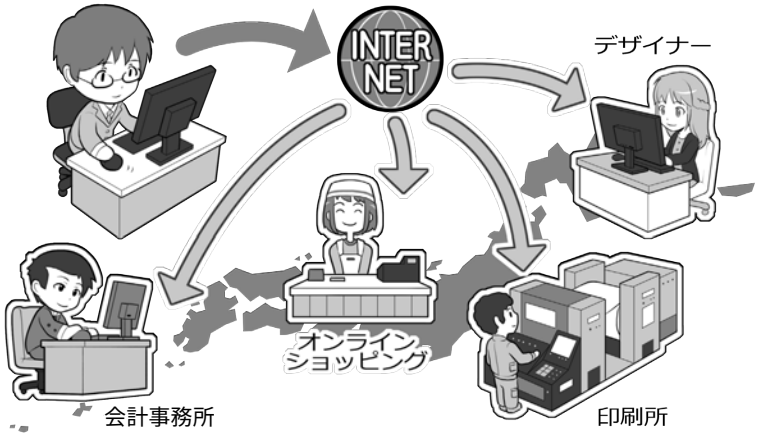
また、経理処理なども会計ソフト会社がオンライン対応になることで、取っておいたレシートをスキャナやスマホの撮影機能経由で提供されているクラウドサービスにダイレクトにアップロードすると、基本的な伝票入力が行われた状態で会計ソフトに返ってくるようになっているものもあります。

仕事で使う資材でも、図面を送信すれば、金属板をレーザーでカットして穴開けまでしてくれたり、簡単な折り曲げ加工をしてくれるもの、あるいは従来ならば専門店でしか購入できなかったものが、オンラインで購入できたりします。

そうすることで、いままでの業務の効率化が行え、必要だったコストや時間を省くことができます。

一方、近年は悪質な業者も増えてきているため、見つけた業者の評判をインターネット上で探してみることもお忘れなく。

どこにいる人とでも仕事ができる



社員がどこにいても仕事ができるのと同様に、地方に住んでいる専門分野の人たちと仕事をする制約も少なくなります。場所ではなく求める技術を基準にフリーランスの人を探して仕事を依頼することもできますし、自社で原稿だけを作り、制作や印刷といった後工程の業務を、遠方のプロにオンラインで発注することもできます。場合によっては特定の業務を行う自分の手間と発注のコストを計算して比較して、それをアウトソーシングすることで、自社や自団体が自らが得意とする分野に注力して能力を向上し、逆に選んでもらえるプロになりましょう。

セキュリティ系業務もアウトソースできる

日常的なサイバーセキュリティに関する業務も、専門業者にアウトソースすることが可能です。どういった企業に依頼したらよいか判断しにくい場合に備えて、経済産業省とIPAでは一定の基準を設け、これを満たした企業のリストを公開しています。詳しくはP.181を参照してください。

製品を扱うなら全世界が市場

自社や自団体が何かの製品や物品をつくって販売や提供する場合も、ネットを活用すればその対象が全世界になるといっても過言ではありません。昔であれば距離の壁に阻まれ小さなマーケットに閉じ込められていた地方都市の小さな会社でも、ネットの時代の特性を活かして、世界的にビジネスを行えるようになった例もあります。

もちろん発信する情報を翻訳したり、時には海外の方とコミュニケーションする必要もありますが、そういった言語的な問題はいずれIT技術で解決されるでしょう。とくに伝統技術などは「存在が知られていない」ことが、海外でのチャンスを逃がしていることもあるのです。

4 ファイルの共有設定や情報の公開範囲を見直そう

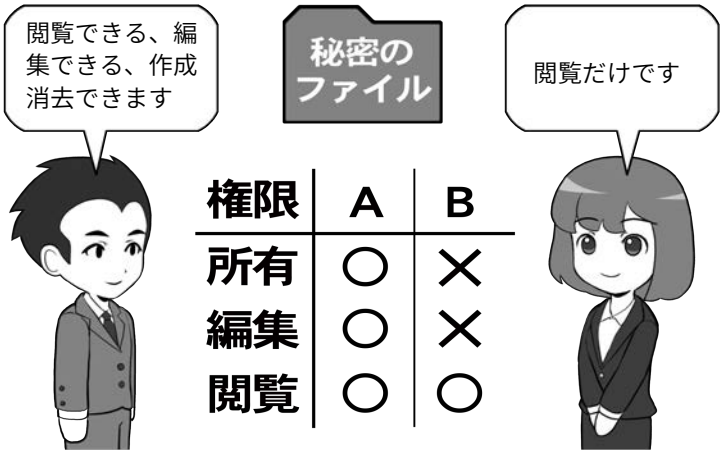
共有設定とは、私たちがIT機器上やインターネット上で使用するファイルや情報、あるいは機器そのものに関して、自分だけでなく誰かと共同で利用するときに、機密性を保つために必要な設定です。

共有設定には、ファイルの管理を例にあげれば、単純に見られるか見られないかを意味する「閲覧」、そのファイルを編集して内容を書き換えることができる「編集」、そしてファイルそのものを作ったり削除したりできる「所有」などの、大まかに3つの権限▶用語集P.196があります。

会社内でファイルをUSB▶用語集P.193メモリのような媒体にコピーしなくても受け渡しをしたりすることを可能にするために、社内にネットワーク(LAN:Local Area Network)を引いている企業であれば、ファイルを管理する「NAS」(NAS: Network Attached Storage)というサーバ上にある文章ファイルなどを見られる人を制限したり、あるいは誰かがうっかりファイルを消してしまわないように、こういったファイル毎の所有者設定や、同様の意味を成す資格設定をしっかりしておく必要があります。

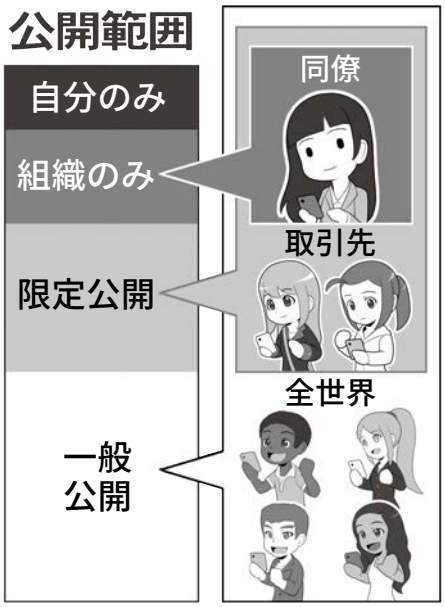
クラウドストレージサービスのようなインターネット上のサービスにも共有設定があり、「公開範囲」▶用語集P.196と呼ばれることが多いようです。インターネットのサービスの公開設定を一般公開にした場合、インターネットにアクセスする世界中のすべての人に公開することになりますので、注意が必要です。

共有設定ってなんだろう？



物理的な手帳は、それが誰の持ち物で誰にも見せてよいかといったことは、とくに意識せずに使っています。しかし、ネットワーク上にあるファイルなどは、とくに設定しない場合は、「基本的に誰でも見られる」状態になっているので、それでは困る場合、これに対してアクセスを制限する権限を設定する必要があります。それらが「所有」「編集」「閲覧」の権限です。

クラウドストレージの公開設定



企業がクラウドストレージを用いて自社内や取引先と業務上必要なファイルのやりとりをする際には、公開設定・公開範囲に注意しましょう。自社内に公開を留めておきたい情報を誤って一般公開すると、意図しない人にまで情報が閲覧されてしまう可能性があります。サービスによっては初期設定が一般公開になっている場合があるので、公開範囲は注意しましょう。

この公開設定の初期設定が一般公開になっていたり、誤って公開範囲を変更してしまったりした場合、情報が外部から閲覧できる状態になります。何者かに情報を持ち去られたり、公開された情報が原因で報道や

SNSで話題になり炎上▶用語集P.195したりした企業の事例もあります。

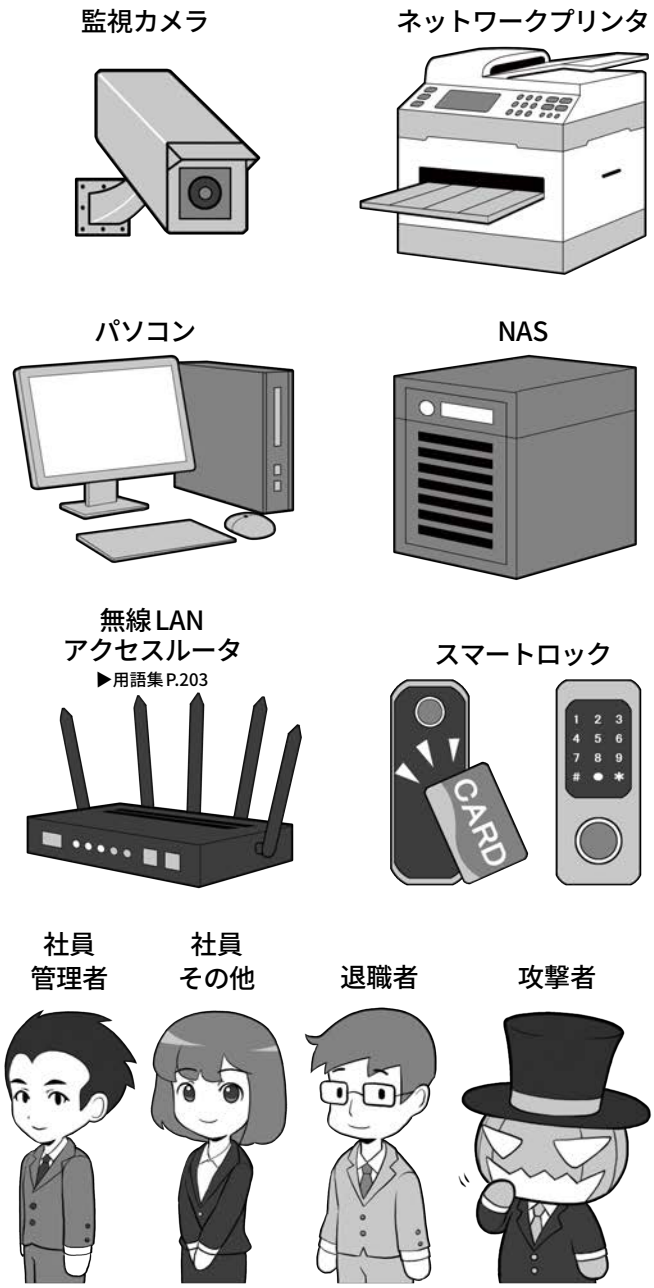
LAN上のNASでもストレージサービスでも、共有設定はファイル単位やフォルダ単位で設定できるので、その整合性に気を付けないといけないことと、例えば臨時で誰かに特定のファイルを公開したい場合、設定ではなく「見たり編集したりできる」リンク▶用語集P.204を送信することで共有することができるものもあり、この場合、そのリンクを知っている人は誰でも同じ権限を持つので、送信後の管理にとくに注意が必要です。

IT機器そのものの利用にも、同様の設定があり、こちらの場合は共有というよりも利用できる権限設定です。機器を管理し設定を変更できる「管理者」や、利用するだけの「利用者」や「ゲスト」などがあり、これらは機器に対してログイン▶用語集P.204するときのIDとパスワードで管理されるので、資格管理をしっかり行って下さい。

権限設定つながりでいえば、会社の建物や特定の部屋に入るための権限を設定している場合も、同じようにきちんとした管理が必要です。例えば人事情報がある場所は人事の人間しか入れないようにしておく必要がありますし、社員の異動や退職が発生した場合、資格の無い人が立ち入りできないように、きちんと設定変更をしたり、入出用にICカードや鍵などを使っている場合は、回収する必要があります。

また、こういったシステムもIT機器を使っている場合は他のシステムと同じように、常にアップデート▶用語集P.194する必要があり、それを怠ると攻撃者がシステムをクラッキング▶用語集P.196した上で建物に物理的に侵入することもあります。なお、攻撃者は人間の心の隙を突くソーシャルエンジニアリング▶用語集P.198で社員をだまし、例えば建物管理や防犯システムの業者のふりをして、堂々とやってくるかもしれないのでそちらも注意しましょう。人間の心理も攻撃の対象なのです。

機器の共有設定



会社や団体の事務所で使用する機器も、ネットワークにつながっている場合、基本的には誰でも利用できる設定になってることが多いのです。したがって特定の人のみが利用できるようにしたい場合は、それぞれの機器および利用者に対して権限を設定する必要があります。

建物などの立ち入りにIT機器による権限を設定している場合は、異動や退職などによってその人物の権限が変更されたり失ったりした際に、それに合わせてきちんと権限を変更するか、権限を執行するためのカードなどを回収しなければなりません。

これを怠ると、退職者が勝手に建物に立ち入ったり、あるいはなんらかの方法で攻撃者がそのカードを入手すると、なんの工作もしないで建物に侵入してしまえます。

また、機器に対する資格設定をしていない場合、攻撃者が無線LAN経由などで建物内のLANに侵入した場合、各種機器やファイルを管理しているNASなどに、なんなくアクセスしてしまえます。複数の人が働く職場ではこういった権限設定はとくに重要です。

5 企業が気を付けたいサイバー攻撃を知り、情報収集に心掛けよう

5.1 脅威や攻撃の手口を知ろう

「敵を知り己を知れば百戦危うからず」という孫子の諺（ことわざ）がありますが、サイバーセキュリティ上、危うい状況に陥らないためには、自らのセキュリティ環境が脅威にきちんと対応できてるか知り、また、攻撃者の手口を知ることが重要です。知らないことが、サイバー攻撃による被害がなくならない本質でもあるのです。

それを理解できれば、なにが必要かがわかり、さらにどのような情報が必要か地図が描けます。そうやってサイバー攻撃の危険性（ソーシャルエンジニアリングのような人間の心の隙を突くような攻撃を含め）を知ることが、一番の対策となるのです。

では、どのようにしたら情報を入手できるのでしょう？まずはセキュリティソフトを提供している企業の発信に注意を払いましょう。そうした企業はSNSなどで最新の攻撃情報をいち早く配信していることが多いので、著名な企業のアカウントを複数フォローするとよいでしょう。

次にOS▶用語集 P.191を作っているメーカーなどのアカウントです。ただし、そのアカウントが発信するのは自社製品に関する情報のみですが、有益な情報も多くあります。

もっと横断的な情報が欲しい場合は、IPAやNISC▶用語集 P.191などの政府機関のアカウントやメールマガジン、セキュリティや詐欺関連の対策機関の公式アカウント、セキュリティ系雑誌の記事を追いかけるようにしておけば、大規模なサイバー攻撃の兆候やセキュリティホール▶用語集 P.198の発覚をいち早く察知することができ、その対策を立てることが容易になります。

攻撃者の攻撃手段を知ることで学ぶ

仕事のメールに偽装したマルウェア

セキュリティ企業のブログやセキュリティ系のウェブ記事を見ていると、攻撃者の新しい攻撃手段について、かなり素早く教えてくれます。ニュースをキャッチする他に、それがどういった意味を持つのか知りたい場合は、セキュリティー系ブログや記事が参考になります。

公的機関、OS企業、セキュリティ企業の情報を聞く

本当にヤバいサイバー攻撃が発生するとこんな感じに

上図に書かれているようにして、広範囲にアンテナを張ると、本当にヤバい攻撃が発生した場合は、各種ソース▶用語集 P.198がその性格にかかわらず、一斉に同じ話題について発信し始めます。記事を理解するだけでなく、こういった波を肌で知ると、攻撃の危険度を察知し身構えたり回避策をとったりできます。

5.2 より能動的に情報収集しよう

そうした必要最低限の情報だけでなく、世界で起きているサイバー攻撃のトレンドなどを知りたいなら、海外のセキュリティ関連企業や機関、サイバーセキュリティに関する情報を提供しているウェブメディア、セキュリティ識者のSNSやブログなど参照するとよいでしょう。

ただし、こうした情報は能動的に収集した上で取捨選択をする必要があり、さらに必ずしも毎日アップデートされるわけではありません。このため初めは熱心に情報を収集していても、だんだんと飽きてきてあまり見に行かなくなるかもしれません。

そこで、RSS▶用語集 P.192と呼ばれる仕組みを利用して、攻撃情報を楽に収集できるようにしましょう。RSSは気になるウェブサイトやブログを登録しておけば、記事の更新があれば時系列で情報を串刺しして表示してくれます。

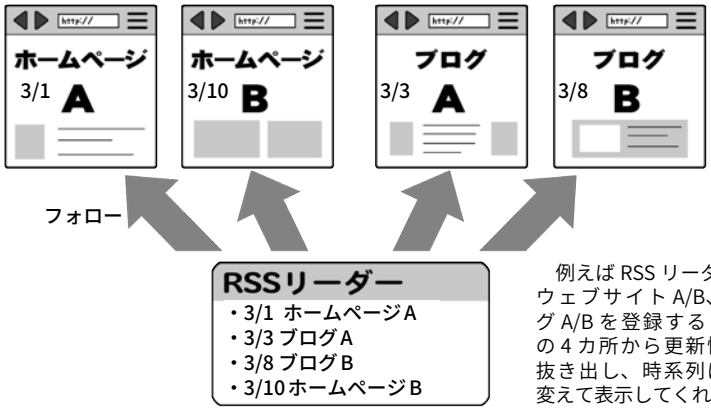
そうしたRSSを簡単に閲覧できるのが、RSSを管理できるウェブサービスとスマホ用のRSSリーダーと呼ばれるアプリの組み合わせです。それらを利用すると、まるでSNSを閲覧する感覚で、毎日世界中のどこかで起きているサイバー攻撃情報やトレンドが読むことができ、否が応でもセキュリティに関しての知識が蓄積されるでしょう。

その他、情報を選別するのに長けた企業や専門家が、重要そうな情報を選別・配布するサービスを提供していることがあります。必要に応じてそのようなサービスを受けることも視野に入れて、自身にとって必要十分な情報を取り入れましょう。

RSSってなんぞや

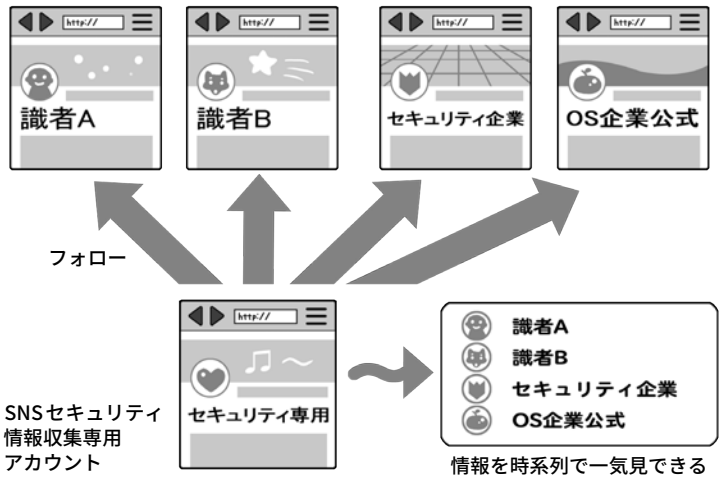
RSSとは平たくいえば、ウェブサイト上の更新情報を、見出し、もしくは概略付きで、時系列に、ウェブサイトの裏の見えない所で発信しているものです。規格（フォーマット）が決まっているので、RSSリーダーに登録すると複数の情報源を串刺しして見ることができます。

RSSは情報を串刺しして一気見できる



例えばRSSリーダーに、ウェブサイトA/B、ブログA/Bを登録すると、その4カ所から更新情報を抜き出し、時系列に並び変えて表示してくれます。

SNSも同様



RSSリーダーの感覚は、SNSで複数のアカウントをフォローすると、素の表示ではフォローしているアカウントの発信が時系列で並ぶのと一緒です。それと同じことをウェブサイトやブログでやると考えると分かりやすいでしょう。

なお、RSSリーダーはインターネット上のサービスで、それ自身がスマホアプリを出している場合もありますし、RSSリーダーに対応した個別のアプリも存在するので、それを導入すると、SNSの流し見と同じ感覚でセキュリティ情報をチェックできます。もちろんSNS上にある、セキュリティ関係のアカウントをフォローしてもOKです。セキュリティ情報収集専用のSNSアカウントを作ってフォローしておくと、個人的なSNS活動と混ざらないでよいでしょう。

よい情報源を集めこの2つを常時チェックしておくと、かなり情報を素早くキャッチできます。

なお、こういったウェブサイトやアカウントで発信される情報は、必ずしも一次情報ソースではないので、真偽を確かめたい場合は一次情報ソースを探すよう心がけて下さい。

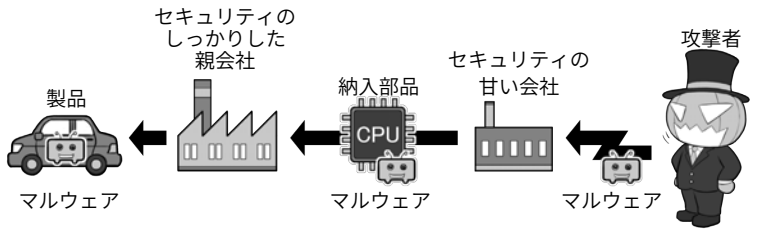
6 企業が気を付けたい乗っ取りのリスクを理解しよう

6.1 サプライチェーン攻撃やオフショア開発によるリスク

「サプライチェーン▶用語集P.197攻撃」による機器やアカウントの乗っ取りに注意しましょう。「サプライチェーン攻撃」とは攻撃者が、セキュリティが堅牢な大企業を直接狙わず、その企業の業務上や製品調達上の関係があり、かつセキュリティが堅牢でない企業を狙うなどして、攻撃を仕掛ける手法です。業務上つながりがある場合は、乗っ取った企業の従業員のアカウントから、メールをダウンロードして、取引先の相手の氏名やメールアドレスを盗み出し、日常的にやりとりしている文面を模倣して、マルウェア付きのフィッシングメール▶用語集P.201を送り付けます。場合によっては、その人物のアカウントそのものからメールを送る場合もあるため、受け取る側はフィッシングメールを疑う手掛かりがなく、引っかかってしまう可能性が高くなります。

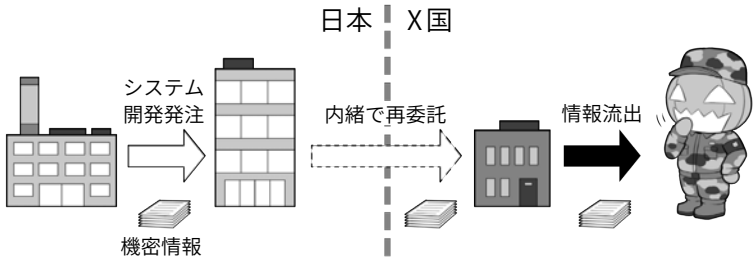
また電子機器を生産している企業などでは、生産しているIT部品にマルウェアやバックドア▶用語集P.201を仕込み、これを大企業に納入させることで、大企業が生産している製品を乗っ取る環境を整えるなどします。例えば大企業へ納入するのがネットワーク部品で、大企業が生産する最終製品がパソコンなら、最悪の場合、マルウェアやバックドアが仕込まれたパソコンが一般流通する事態になります。こういった攻撃に遭うと、サプライチェーンに関係する中小企業や団体にも責任が生じます。

①サプライチェーン攻撃とは



サプライチェーン攻撃とは、最終的な攻撃目標を生産している、セキュリティが堅牢な企業を狙うのではなく、そのサプライチェーン（供給の連鎖）の工程の、弱い企業や弱い場所を狙って攻撃を仕掛け、最終的な攻撃目標に、マルウェアなどを仕込む手法を指します。イラストでは車（ハードウェア）が狙われていますが、ソフトウェアであっても同様ですし、考え方として誰かのアカウントを乗っ取るときにも使われます。

②オフショア開発とは



オフショア開発とは、ソフトウェアの開発するときに、受託した企業が依り開発コストが安い海外の企業などに再委託することを指します。しかしこの再委託先が我が国と同じ倫理感や法治の概念を持たず、モラルが低い場合、サプライチェーン攻撃を仕掛けられる場合があります。問題は受託企業が発注企業に内緒で再委託している場合あり、発注者はセキュリティ上、開発がどこで行われるか、契約で定め、掌握する必要があります。

明示的なサプライチェーン攻撃以外にも、気付かぬ所で情報の漏えいを起こすケースにも気を付けましょう。使用するIT機器が、利用者の意に沿わぬ形で情報を勝手に国外に漏えいさせるケースもあります。

通信機器やドローンに関連したサイバー攻撃が取り沙汰されている他、外部から不正にIT機器へのアクセスが可能となるバックドアの設置も話題になっています。機器を購入するときは、当該の会社の製品が、類似のトラブルを起こしていないか、入念に調べてから手配しましょう。また外部にプログラムやIT機器の開発を委託する場合、詳細が開示されないうちに、情報の取扱が厳密でない外国に対して、「オフショア開発」で業務が再委託されるケースがあります。こういった場合、発注者のあずかり知らぬ所で、情報漏えいやシステム上にバックドアを仕込まれてしまう可能性があります。そのようなことを防ぐため、契約時には禁止行為や監査などを取り決めましょう。

6.2 問題が起きると事業継続に影響を及ぼす

攻撃者によるサイバー攻撃だけでなく、十分に気を付けなければならないのは内部の人間、およびそれに準じる人間によるサイバー犯罪です。

現実にあった例を下敷きに説明しましょう。

とある会社で営業機密や顧客情報の流出が発覚しました。その犯人は過去にその会社に在籍していた人物で、とくに複雑なハッキングをせずに、在籍時のアカウントを使ってアクセスし、情報を抜き取ったのでした。

退職者のアカウント管理をきちんと行っていなかったために発生したケースと言えます。

また、回線を使った侵入すら行わないケースもあります。

とあるサービス業から顧客情報が約数千万件流出するという事件が発覚しました。

その会社自身が流出に気付いたものではなく、流出した名簿を使って顧客にダイレクトメールが届くようになったことで、間接的に数千万件の顧客情報流出が発覚したものです。

情報流出は親会社から業務委託された情報処理系の子会社から、外部の派遣社員のエンジニアが顧客データを持ち出し、名簿業者に不正に転売した結果起きたものでした。

本件は、クラッキングなどを行ったサイバー攻撃によるものではありませんが、内部犯行者によるれっきとしたサイバー攻撃でした。

これにより親会社は顧客に数百億円相当の補償を行い、また、子会社は事業継続が困難となって翌年に解散。犯人は当然のことながら逮捕、責任を負うべき立場にいた役員が引責辞任となりました。

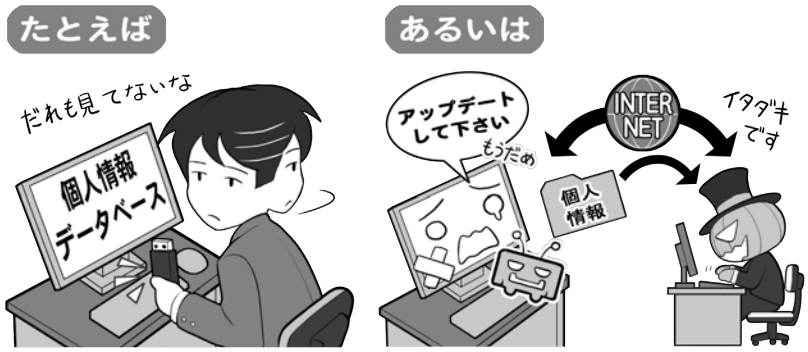
このケースでは親会社と子会社の関係でしたが、これが資本関係のない契約企業だった場合、損害賠償請求が行われたかも知れません。

ましてやこれが、社員数名しかいない中小組織だったら、金銭的賠償は不可能でしょうし、NPO だった場合は、高い意識を持って始めた事業であっても、情報流出を起こしたことで信頼を失い、その目的の達成を断念せざるを得ない事態に陥ったでしょう。

受託事業の機密情報を流出させてしまった

受託事業で預かった機密情報や個人情報▶用語集 P.196 なども、IT 機器を導入していると、目立たずあっという間に持ち出されたり、流出してしまったりします。上記のイラストでは、外部から来た派遣社員の例ですが、ソーシャルエンジニアリングを使って会社に入り込んだり、社員を騙して送らせたり、あるいは外部からサイバー攻撃を行い社内や団体内のコンピュータなどを乗っ取って流出させたり、その可能性はいくらでもあります。こういったトラブルが発生したとき、相手先や顧客への不利益はもちろん、会社として受ける損害は計り知れません。

なぜこれがサイバー攻撃なのか？



誰でもさわれるPCに入れっぱなし　パッチあてずにつなぎっぱなし

外部の人間が機密情報の入ったパソコンに、USB メモリを挿して情報をコピーして持ち出した。ネットワーク越しに受けるサイバー攻撃だけでなく、こういった物理的な盗難も広義のサイバー攻撃です。サイバー攻撃とはネット経由に限らず現実世界も含むのです。

盗難されたデータはその先で、また、別のサイバー攻撃を生みます。例えば盗んだ名簿が現実世界の名簿屋やダークウェブ▶用語集 P.198 上のダークマーケットで販売されると、その名簿を買った別の攻撃者が、スパムメール▶用語集 P.197 などを使ったサイバー攻撃に用いる可能性があるのです。

7 企業が気を付けたいサイバー攻撃の具体例を知ろう

7.1 標的型メール攻撃の具体例

「お盆休み明けに出社して、すぐにメールを開くと、提携先の会社のAさんから、次回のミーティングに関してのレジュメが添付されてきていた。ミーティングは当分先だったのではと思いつつ、このファイルをクリックして開いたが、レジュメは表示されなかった。ファイルが壊れているのかな…。まぁいいか。」

はい。アウトです。こんな話は、どこの会社や団体でも見るありふれた光景でしょう。しかし、この話には3つのポイントがあります。

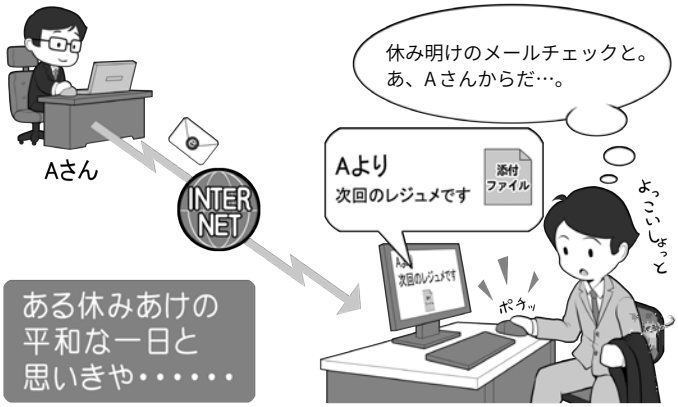
1つは、長い連休中にはセキュリティアップデートや、総合セキュリティソフトの更新が行われている可能性があります。日常的な業務を始める前に、まずアップデートして連休中に見つかったシステムのセキュリティホールや新しいマルウェアに対応できる状態にしましょう。

2つめに、どこかの会社のAさんが、本当にAさんか確かめるのは、ややレベルが高いとしても、少なくともこの時期にAさんからメールが来たことに疑問を持っています。そういうときは連休中にAさんのメールが乗っ取られた可能性を考えて、メールではない手段(電話やビジネスチャットなど)でAさんに添付ファイル付きのメールを送ったか確認しましょう。

3つめ、添付されているファイルをいきなり開き、きちんと見られなかった点で、マルウェアの可能性を考えていません。ひらけなければ疑問を持つべきですし、開いた場合でもなにかをインストール▶用語集 P.194しろとか、あなたに許可を求めるものは、総じて疑うべきです。

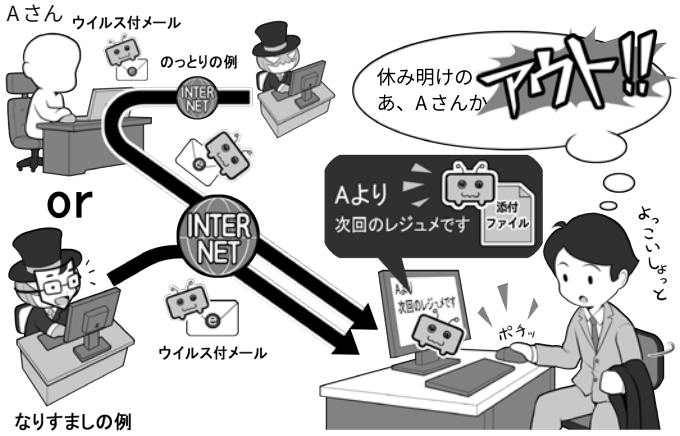
それに原則的なルールは、「メールを見ただけで完結しないものはすべて疑え」であり、「挙動が怪しい場合には、組織内にセキュリティ担当の窓口が設置されていれば、そちらに連絡する」です。それは添付ファイルでもメールの文中の外部ウェブサイトへのリンクでも同じです。

こんなシチュエーションだと思っていたら…



休み明けに出社して、普段どおりにパソコンを立ち上げ、メールを開いて読む。しかし、この一連の流れには攻撃に対する視点が欠けています。攻撃者だったらどう攻撃するかという視点です。休み明けということは、何日間かパソコンを立ち上げていない時間が存在し…

実はこんなシチュエーションかも…



その間には、新たなセキュリティホールが発見され、攻撃者が攻撃するためのマルウェアを開発して、取引相手になりすましたり、アカウントを乗っ取ったりして、そのマルウェアを送ってきているかも。標的型メール▶用語集 P.201に対処するには、メールを開く前にまず、アップデートしてシステムを最新の状態にします。

7.2 フィッシング攻撃の傾向

「オンラインショッピングの会社からメールで、『あなたのアカウントが攻撃され、一時的に利用停止になった。下記からログインして、停止を解除して下さい』という内容のものが送られてきた。リンクを開くといつもどおりのそのショッピングサイトのロゴとデザインのウェブサイトが表示されたので、IDとパスワードを入力して、停止を解除した。」

あなた宛に名指しで送られてくるメールなどと違い、個人名がなく不特定多数に送られることが多いのが、ばらまき型のフィッシングメールです。余談ですがフィッシングとは釣りFishingではなく、詐欺の意味のPhishingから来ています。

上記の話は有名なので知っている方も多いと思いますが、ねつ造された偽物のウェブサイトは、最近では本物と見分けが付きません。

あなたがIDとパスワードを入力すると、それをだまし取って勝手にオンラインショッピングサイトで買い物をし、商品を転売するなどしてお金を手に入れるわけです。

このメールも文面を見ただけで完結しないので疑うべきです。

なお、こういった警告が来た場合、メールのリンクは使用せず、ウェブブラウザで検索し直接そのショッピングサイトなどを訪れてみて下さい。本当にアカウントが停止されているならば、警告が表示されるでしょう。

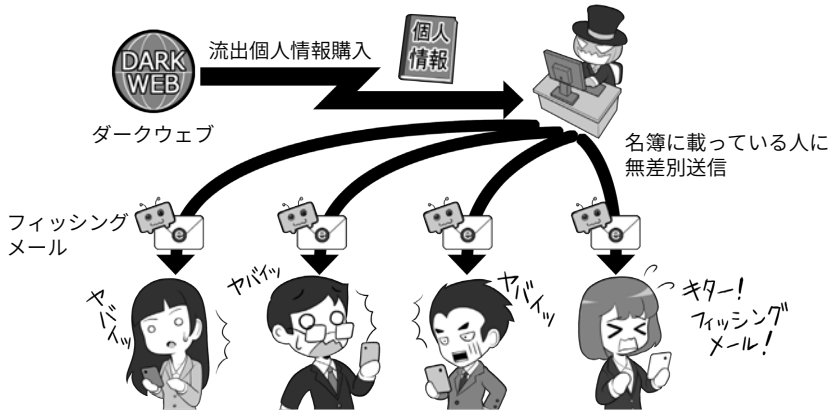
一方で、そのウェブサイトがショッピングサイト相当の暗号化(https://▶用語集P.191)に対応していて、一見そのショッピングサイトと同じ名前を掲示していても、実は「アルファベットに似た別の言語の文字」を使用している場合もあります。

具体的にはロシア語などで使われるキリル文字は、アルファベットと似た字形のものがありますが、インターネットでは別の文字として扱われるので、同じにURL▶用語集P.193に見えて別のウェブサイトを作れるのです。

すぐに対処しようと思ったら…

SMS▶用語集P.192やメールで「パスワードが流出しました。至急変更を！」という連絡がきても、ちょっと待ちましょう。それは本当に自分が使っているサービスから送られてきていますか？

実際はこういうワナだった！



攻撃者はどこかのウェブサービスなどから流出したメールアドレスなどをを買って、IDとパスワードを盗む攻撃をしかけてきます。反応するとアカウントを乗っ取られるかも。

それには解りにくくなる工夫も

この部分が見た目同じ文字を使う外国語だったりすると、一見、見分けが付かないことも

メールのリンクを開いて、飛んだ先のウェブサイトがそのサービスの本物のページとは限りません。似たような単語を使った別のウェブサイトの場合もあるのです。よく確認しましょう。

7.3 不正アクセスの傾向

「ある朝、会社に出社したら、取引先から『お宅に渡した当社の機密情報がネットで公開されているじゃないか、どういうことだ！』というクレームの電話が来ていました。それを受けて調べるみると、社員で共有用に使っていた社外のクラウドストレージサービスのIDとパスワードが何者かに破られて、社外からアクセスをされ、情報が流出していました……。でもなぜIDとパスワードが漏れたんでしょう…。」

この問題は複合的で、「①なぜIDとパスワードが漏れたのか」だけでなく、「②なぜ漏れたIDとパスワードでクラウドストレージサービスにアクセスできたのか」、最後に「③なぜクラウドストレージサービスから情報流出を許してしまったのか」の要素があります。

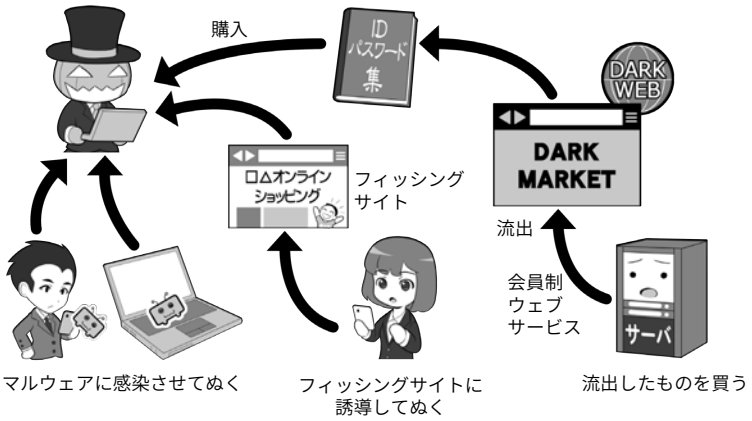
①のIDとパスワードの流出はマルウェアの感染やウェブサービスからの流出などがあり、自分で防げるものと防げないものがあります。自分で防ぐには、セキュリティをきちんと固めるだけです。一方、ウェブサービスからの流出は、多要素認証▶用語集 P.198を導入していないセキュリティ意識が低いサービスを避けるなど、消極的手段はありますが、最終的には自分でどうにかすることはできません。

どうにかできないをカバーするには、②のなぜクラウドにアクセスできたかの問題ごと封じます。この場合は個人と業務用でパスワードの使い回し▶用語集 P.201をしていたことが原因なのでこれを防ぐのです。たとえ漏れても被害が発生しないようにするには、1つはパスワードの使い回しを絶対にしないこと。もう1つは、多要素認証を導入して、漏れてもIDとパスワードだけではアクセスできないようにすることです。

③でさらにクラウドにアクセスを許しても情報流出を許さないためには、アクセスできる人間を限定することや、重要情報を見られる人間を共有設定で限定すること、そして、機密情報などは例えファイルとして流出しても、その内容を閲覧できないように、ファイルごとに暗号化を施すことです。

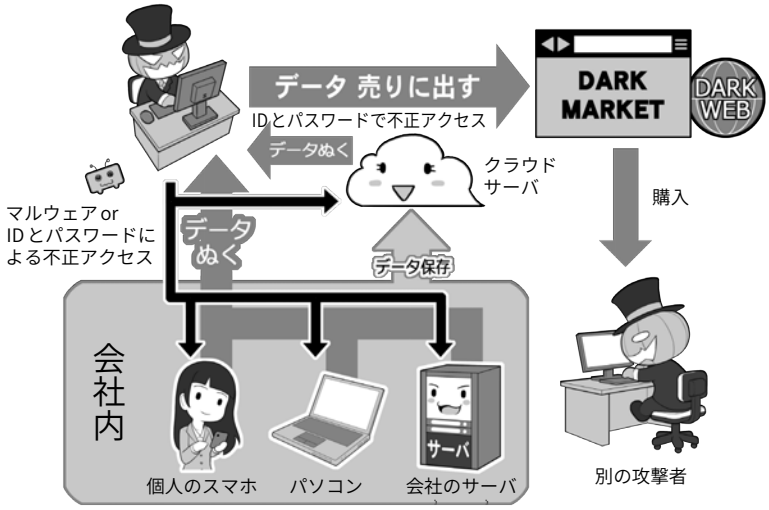
不正アクセスを行うために攻撃者は…

①IDとパスワードを狙う



攻撃者は不正アクセス▶用語集 P.202を行うために、IDとパスワードを収集します。前ページのように偽のウェブサイトに誘導して抜く方法の他にも、マルウェアに感染させて抜く、流出した情報をダークウェブにあるマーケットで購入して集めるなど、さまざまな手法があります。それを使って別のウェブサービスや業務上のサービスに不正アクセスを行おうとします。このとき、IDとパスワードの使い回しをしていると、侵入されてしまう危険性が跳ね上がります。

②データを狙う



不正アクセスができたら、今度はあなたが持っている機器、使っている機器から情報を抜き取ります。それをダークウェブのマーケットを経由して誰かに販売するかもしれません。クラウドサーバ上にあるデータも、アカウントを盗まれればアクセスされて、保管しているデータを盗まれるでしょう。盗まれたデータが受託した業務に関連するものだった場合、自社だけでなく発注元企業に被害が及び、また個人情報だった場合、顧客などに不利益を与える結果になります。アカウント情報を盗まれないように、細心の注意を払いましょう。

7.4 不正送金の傾向

お金を直接狙うサイバー攻撃は、取引先のふりをして振り込み口座を変更させるBEC▶用語集P.190や、不審なメールやメッセージから銀行にそっくりのウェブサイトに誘導して、IDとパスワードを抜いたり、実際にインターネット上で送金するときにその通信の中間に割り込んで、目的の口座に振り込ませる「中間者攻撃」▶用語集P.199と呼ばれるものなどがあります。

警察庁の発表によれば、令和元年の発生件数1872件、被害総額25億2100万円をピークに発生件数、被害総額ともに減少していましたが、令和4年は、発生件数、被害額ともに増加に転じています。また、その手口の多くはフィッシングによるものとみられています。

「会社の口座を確認したら、空になっていた。」こうなってしまっては回収できたとしても時間を要するでしょう。会社の運転資金までやられてしまえば、事業継続は困難になります。

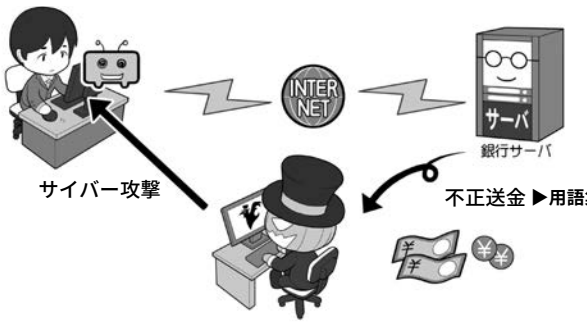
幸いにして情報の流出などと異なり、銀行の場合は過失が無いことが認められれば、銀行側が補填してくれることもあります。クレジットカードの不正利用なども同様です。

一方、場合によっては補填が行われないのが、暗号資産を奪取する詐欺です。暗号資産は通貨といいながら、平たくいえば暗号化された情報なため、不特定多数をフィッシングメールでマルウェアに感染させ、情報を奪取することも行われています。

これらに対処する特別な方法はなく、今までの3項目であるような基本的な対処方法と、もう1つは同様の手口の情報を、アンテナを高くしニュースやネットの記事、SNSなどから集めて、いざ攻撃されたときに、「似たような話を聞いたことがある。不信だ」と気付くようになることです。

なお、不正送金が疑われる事象があった場合は、速やかに銀行やクレジットカード会社に相談しましょう。

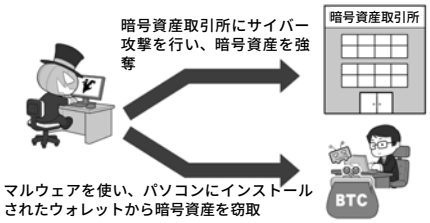
オンライン決済は常に狙われている



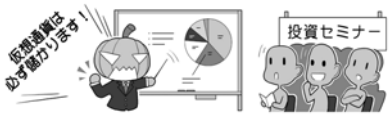
オンラインの銀行決済は常に狙われています。取引先になりすまして BEC だけで誤った口座に送金させる手口や、偽サイトで ID やパスワードを奪う方法、そしてなんらかの手段で決済の中間に割り込んで振込先を自分の口座にすり替えてしまう中間者攻撃。

多要素認証、パスワードなどの厳重保管、BEC やフィッシングメールに騙されないスキル、そして総合セキュリティソフトなどを導入している場合は、決済専用のブラウザを使うなどの防御手段があります。

犯罪者に狙われる暗号資産



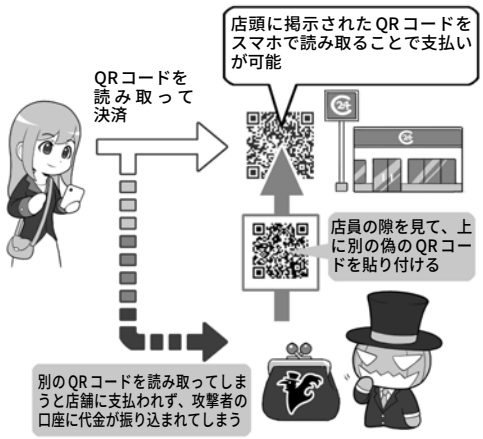
暗号資産を巡るサイバー攻撃も続発しています。実際、国内海外含め多くの暗号資産取引所がサイバー攻撃を受け、大きな金銭的被害が生じた事例がある他、暗号資産の窃取を目的としたマルウェアも登場しています。



題材を暗号資産にした「必ず儲かる」系のセミナーも開催されています。暗号資産に限らず、「必ず儲かる」という話は詐欺のケースが多いので、信用しないようにしましょう。

暗号資産をネタにした投資詐欺▶用語集P.199が増えています。どのようなものであっても「必ず儲かる」という話はありえませんので、くれぐれもご注意を。

QRコード決済▶用語集P.191の詐欺の流れ



まず犯罪者が店舗に掲示されたQRコードの上に、別のQRコードを貼り付けます。利用者がそのQRコードを使って決済を行うと、代金は店主ではなく犯罪者の口座に振り込まれてしまうという流れです。

7.5 ランサムウェアの傾向

「始業時間に会社に来てパソコンを起動すると、『このパソコンは乗っ取った。データはすべて暗号化したから、データを返して欲しければ身代金を払え』というメッセージが出て、送金期限までのカウントダウンが始まった……」

これがランサムウェア（ランサム＝身代金）▶用語集 P.203 と呼ばれるマルウェアの典型的な手口です。

ランサムウェアへの対処方法は、システムを常に最新の状態に保つことと、仮に攻撃されても、組織としての対応方針をあらかじめ策定し、感染したシステムを初期化▶用語集 P.197 しバックアップから復旧できる体制を整えることです。感染しにくくするためには、とくに外部からアクセス可能な機器について、地道にセキュリティ対策を施していく必要があります。

身代金を支払ってもデータが復元▶用語集 P.202 される保証はないですし、攻撃者を助長するだけなので避けましょう。

ランサムウェア感染はビジネスにも影響

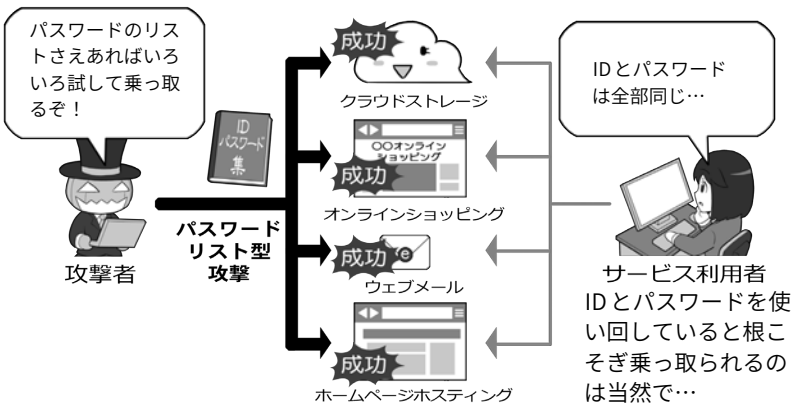
ランサムウェアはパソコンなどの中のファイルを勝手に暗号化するため、感染すれば仕事上の極めて重要なファイルも人質に取られてしまいます。大事なデータが入ったパソコンが使えなくなれば、業務停止、納期遅延など顧客に迷惑をかけ、その結果、会社としての信用を失う恐れもあります。バックアップは常にしておきましょう。

7.6 ウェブサービスへの不正ログイン

先ほどの情報流出の件でも登場しましたが、クラウドストレージサービス、オンラインショッピング、メール、ウェブサイト運用など、ウェブサービスと総称されるインターネットのサービスは、常に攻撃者からの乗っ取りの危険にさらされています。常にこれを阻むことを考えましょう。

IDやパスワードの使い回しをしないことと、さらにサービスを利用する際に、多要素認証などやUSBセキュリティキー▶用語集 P.193 などを用いて、攻撃者が不正ログイン▶用語集 P.202 しにくくなる環境を整備しておきましょう。

パスワードを使い回しをしていると攻撃に

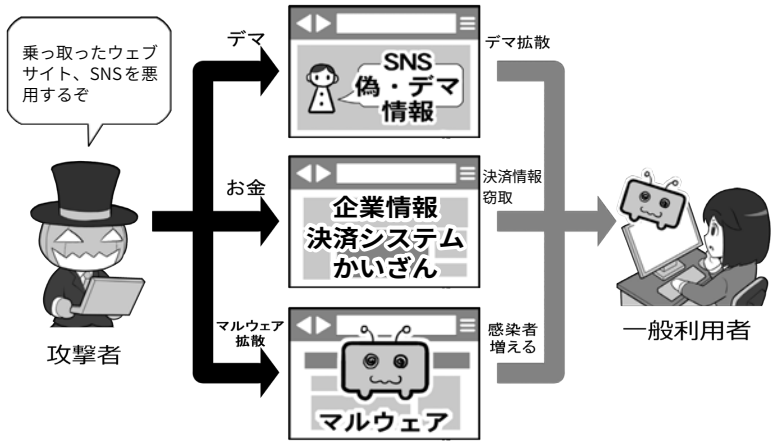


つい面倒くさがってIDとパスワードを使い回ししていると、どこか1つでも流出が起これば、同じIDとパスワードを使用しているサービスが根こそぎ乗っ取られる場合があります。また、別々のパスワードを使っていても、そのパスワードがよく使われるような簡単なものだった場合、そういったパスワードをまとめたリストが流通していて、それを使ってアカウントを乗っ取る攻撃が行われます。一部を変えただけなど、似たようなパスワードも非常に危険です。

7.7 ウェブサイトの改ざんやSNSの乗っ取り

会社や団体のウェブサイトは、ホスティングサービス▶用語集 P.203と呼ばれる、専用の業者のサーバを利用していることも多いと思います。これらのサービスはセキュリティを自分で管理する代わりに、ホスティングサービスに外注している形になり、特殊なカスタマイズを施さなければある程度のセキュリティは確保されています。一方、管理者アカウント情報を推測されたり、ウェブサイトなどの脆弱性▶用語集 P.197を突かれたりして不正アクセスされ乗っ取られると、改ざんされ偽の情報を発信したり、マルウェアなどを埋め込まれ、不特定多数にサイバー攻撃をしてしまったりします。認証情報はきちんと管理し、多要素認証などで容易に不正アクセスできないように設定し　ましょう。

ウェブサイトを乗っ取られると攻撃の拠点に



管理者アカウント情報を推測されたり、ウェブサイトなどの脆弱性を突かれたりして不正アクセスされ、自社や団体のウェブサイトを運用しているサーバが乗っ取られると、攻撃者はそのウェブサイトを使ってサイバー攻撃を行います。

例えば偽の情報を発信する、公開されている企業の情報を改ざんする、あるいはそのウェブサイト自身をマルウェアの発信元にして、ウェブサイトを訪問した人のIT機器をマルウェアに感染させ、乗っ取ったIT機器をどんどん増やしていくかもしれません。

一方、WordPressなどのウェブサイト作成ソフトは、それ自身をアップデートしないで使用すると、発見されたセキュリティホールを悪用されるので、きちんとアップデートしましょう。

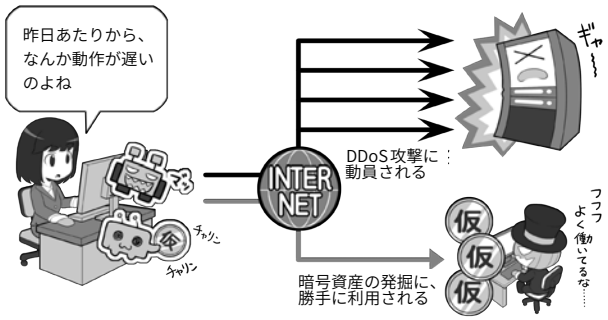
7.8 DDoS攻撃

DDoS攻撃▶用語集 P.190とは、複数のIT機器からウェブサーバに対して大量のデータを送りつけて応答不能にするサイバー攻撃です。DDoS攻撃を受けると、利用しているインターネットサービス、いずれもが処理能力オーバーで機能しなくなり、ウェブサイトならばアクセスできなくなります。これに関してはウェブサーバ側で対処できることが少ないのが実状です。事前にCDN（Content Delivery Network）▶用語集 P.190サービスを利用するようにしておけば、DDoS攻撃をある程度緩和できる可能性があります。

一方、自分の会社や団体のIT機器などが乗っ取られDDoS攻撃に利用されている場合は、利用停止、ネット切断、通報の判断、周りを含めマルウェアの駆除、バックアップからの復旧などをする必要があります。

DDoS攻撃に限らず、総合セキュリティソフトが反応しない場合、マルウェアの感染を検知するのは、「なにか動作が遅い。おかしい」といった、正常動作時との差なので、そういった点にも気を配りましょう。

乗っ取ったIT機器は直接的サイバー攻撃などに



マルウェアに感染させられたIT機器は、自分が被害に遭うだけに留まらず、他のIT機器やサーバに対して直接的なサイバー攻撃に駆り出されることもあります。例えば不正な情報リクエストを集中させ、相手のサーバが反応できない状態に追い込むDDoS攻撃などを行います。また、IT機器の動作がおかしいときには、気付かないうちに暗号資産の発掘に利用されている場合もあります。普段と比べて動作が遅い、不審な挙動をするなどといったときは注意しましょう。

7.9 サイバーセキュリティ以前の情報モラル教育を怠らない

顧客情報を狙う攻撃者の視点から、情報を手に入れる手段を考えると、狙った社員の心の隙を突くソーシャルエンジニアリング方法などが考えられます。例えばSNSで相手を見つけて「名簿高く買うよ」とそそのかす方法などが考えられます。

ただ、情報流出が起こるのは狙われたケースだけではありません。「列車内に鞄ごとパソコンを置き忘れる」「顧客情報の入ったUSBメモリを落とす」「車内に置き忘れた生徒の成績表の入った記憶装置▶用語集P.195を盗まれる」「全顧客にメールを送信しようとしたら全顧客の宛名が見える形で送信してしまった」など顧客情報の流出の報道は枚挙に遑がありません。

「それってサイバー攻撃なの？」といわれれば、直接的にはサイバー攻撃ではないかもしれません。しかし、流出したものがダークウェブなどで販売されれば、サイバー攻撃につながります。

こういった内部犯行や情報流出を防ぐには、防御手段をとった上で情報モラル教育▶用語集P.197をきっちり行うことです。

例えば内部犯行防止に、必要がないときに顧客情報を扱う部屋に人を入れないよう、部屋や建物に施錠をしているでしょうか。アルバイトや社員に、きちんと情報モラル教育をしているでしょうか。

あるいは、仮に置き忘れや紛失、盗難が起こってしまっても、完全な情報流出が起こらないようにするリカバリ手段を講じたり、問題が起こったらどう対処するか、その段取りを考え訓練したりしているでしょうか。

情報流出の可能性はたくさんある

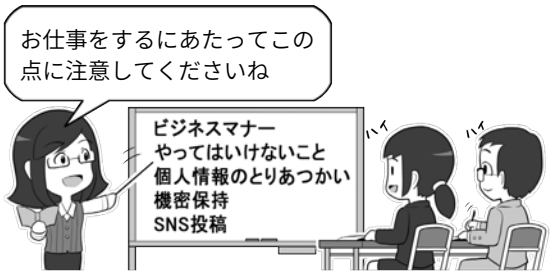
流出の可能性は情報を扱う人を狙ってそそのかすことだけではありません。機密情報を入れたパソコンをカバンごと電車やタクシーの中に置き忘れる、生徒の成績などが入ったUSBメモリを落とす、多数の人に一斉メールを送ろうとしたら、互いのメールアドレスが分からないBCC欄ではなく、見えてしまうTOやCC欄に入れて送信してしまった、などなど。パソコンやスマホ、IT機器は便利な反面、ミスを犯すときも一瞬で多量に失います。要注意です。

サイバーセキュリティにつながる予防策

内蔵記憶装置暗号化　暗号化USBメモリ　資格のない人にはさわらせない共有設定　必要ない人が立ち入らないように施錠

現実世界、ネットの世界、両者に共通する情報流出の防御手段は、機密情報を扱うパソコンや記録媒体は暗号化した上で、その部屋や建物には必要がない人が入れないようにすること、施錠をきちんと行うこと、パソコンなども使用しない場合はロッカーにしまって鍵をかけること、ハッキングを受けないようにネットワークには接続せずにスタンドアロン▶用語集P.197で使用すること、使用できる人の資格設定をきちんと行い、資格がない人には触れないようにすることなど、できる事はたくさんあります。

大切なのは情報モラル教育



こう言った機器やシステム的防御策だけでなく、同等に大切なのは、情報に触れる社員や会員に対する情報モラル教育です。機密情報の取扱だけでなく、最近ネットを賑わせる、問題のあるSNS投稿などを起こさないように、ネットリテラシーを含んだ勉強会や教育を行う事が、求められています。

情報流出というと、攻撃事例だけに注目をしてしまいがちですが、他にも情報流出は起こりえますし、一方で情報管理の基礎を守ればそれらを防ぎ、被害を抑え込むリカバリ手段も打てるのです。

そういったサイバー攻撃以前の備えの必要性を忘れないようにした上で、一般的なサイバー攻撃の事例を知りましょう。

8 個人情報は法律に則り適切に取り扱おう

個人情報の取扱に関することは、「負のコスト」を発生させないための重要な要素です。

個人情報保護法は、中小組織あるいは町内会・自治会、学校の同窓会などにも適用され、個人情報を取り扱う際のルールとして、その遵守が求められています。

個人情報保護法では、個人データを第三者に提供する場合、本人の同意を得る必要があります(第27条)。また、国外に個人データを移転する場合にも原則として本人の同意が必要とされる他(第28条)、令和4年4月の法改正により、外国にある第三者への個人データの提供時に、提供先の第三者における個人情報の取扱に関し本人に対して詳細な情報提供が求められるようになりました。外国に設置しているサーバーで個人データを取り扱う場合などは、当該外国の個人情報の保護に関する制度などを把握した上で安全管理措置を講じる必要があります。

個人情報保護法に違反しますと、個人情報保護委員会▶用語集P.196から指導などを受け、会社の社会的信用を損なう可能性があります。

個人情報の適切な取扱に関し、個人情報保護委員会では、「はじめての個人情報保護〜シンプルレッスン〜」として、「中小企業向け『これだけは！』10のチェックリスト」を公開しています。

その中で、パソコンでのデータの保管は、システムを最新に保つ、セキュリティソフトを入れる、ログインパスワード▶用語集P.204の設定やデータを暗号化するといった事項が掲載されています。より安全に保護するためには、個人情報を取り扱うパソコンを明確にし、不必要にネットにつなげないようにすることの他、USBメモリを使ってデータを抜き出すことができないようにすることが必要です。

また、使用していないときは、個人情報を記録したパソコン、もしくはデータが自動的に暗号化される外付け記憶装置を使っている場合はそれを、物理的に鍵がかかるロッカーなどに保管して、流出事故を起こして完全なる負のコストを発生させないようにしましょう。

気を付けたい個人情報の取扱

巻末資料 中小企業向け基本の10のチェックリスト

分類	No.	チェック項目	ポイント	関連ページ
取得・利用	□ 1	取り扱っている個人情報について、利用目的を決めていますか？	目的は具体的に。 ○「新商品のご案内の送付のため」 ×「当社の事業のため」	P3
	□ 2	その利用目的は、本人に通知するか公表していますか？	取得の状況からみて利用目的が明らかなら通知・公表は不要。	P3
保管・管理	□ 3	(組織的安全管理措置) 個人情報の取扱いのルールや責任者を決めていますか？	個人情報の保管場所や漏えい等発生時の社内の報告先は決まっていますか？	P4-6
	□ 4	(人的安全管理措置・従業者監督) 個人情報の取扱いについて従業員に教育を行っていますか？	個人情報の保管場所等のルールは周知できていますか？	P4-6
	□ 5	(物理的安全管理措置) 個人情報が含まれる書類や電子媒体について、誰でも見られる場所・盗まれやすい場所に放置していませんか？	不要になった情報は適切に廃棄・削除することも大切。	P4-6
	□ 6	(技術的安全管理措置) パソコン等で個人情報を取り扱う場合、セキュリティ対策ソフトウェア等をインストールして最新の状態にしていますか？	ログイン時にパスワードを要求したり、ファイルにパスワードをかけることも大切。	P4-6
	□ 7	個人情報の取扱いを委託する場合、契約を締結する等、委託先に適切な管理を求めていますか？	委託先にも安全管理を徹底してもらうということ。	P4-6
第三者提供	□ 8	本人以外に個人情報を提供する場合、本人に同意をとっていますか？	法令に基づく場合(警察や裁判所からの照会等)や、委託に伴う提供には同意不要。	P7・8
	□ 9	本人以外に個人情報を提供したり、本人以外から個人情報を受け取る際、相手方や提供年月日等について記録を残していますか？	法令に基づく場合(警察や裁判所からの照会等)や、委託に伴う提供には記録不要。	P7・8
開示請求等	□ 10	本人から自分の個人情報を見せてほしいと言われたり、訂正してほしいと言われた際には、対応していますか？	開示等の請求に対応する人は決まっていますか？	P9・10

※このチェックリストは、主に中小企業を対象に、個人情報保護法を遵守できているかどうか確認する際の参考に作成したもので、これ以外にも留意すべき事項があります。個人情報保護法のルールの詳細は、本シンプルレッスンの関連ページや、個人情報保護委員会のHP等をご参照ください。

出典：個人情報保護委員会ウェブサイトより https://www.ppc.go.jp/files/pdf/simple_lesson_2022.pdf

9 フリー素材の取扱と著作権について注意しよう

インターネット上の素材を利用する上で、知っておくべき概念として、いわゆる「フリー素材」とよばれているものがあります。

「フリー」といっても「著作権を放棄しているので勝手に使ってよい」ということではなく、「著作権者の厚意で、一定の条件の下に、無料で利用することが許されている」という意味なので注意しましょう。

この点を理解せず、利用条件をよく確認しないままコンテンツを勝手に使ってしまうと、著作権侵害▶用語集 P.199をしているとして、炎上したり、著作権者から損害賠償を請求されたりするなど、不必要な負のコストを生んでしまうことになります。

一口に「コンテンツ」といっても、その中身はプログラムや画像、映像、動画、音、音楽など多岐にわたり、コンテンツの種類によって利用条件が異なる場合があります。また、著作権者が認めている利用条件の内容も、完全な著作権フリー（著作権を放棄または一切行使するつもりはないため、著作者の明示も要求されず、用途も営利・非営利を問わず利用可能で、改変も許される）といったものから、著作者名は明記しなければならないもの、非営利目的での利用のみが許されるもの、改変が許されるもの・許されないもの、など、さまざまな条件があります。また、中には著作権の保護期間が満了したためパブリックドメイン（PD）となり、基本的に自由に利用できるものもあります。

クリエイティブ・コモンズ・ライセンスとは

すべての著作物には著作権があり、著作権は守られなければなりませんが、インターネットには著作権者によって「条件を満たせば比較的自由に使ってよい」とされているコンテンツが多く存在します。クリエイティブ・コモンズは、そのルールを簡単に示すための試みとして、クリエイティブ・コモンズという国際的非営利組織とそのプロジェクトによるクリエイティブ・コモンズ・ライセンスがあります。

クリエイティブ・コモンズ・ライセンスでは、その条件をわかりやすくするために特定の条件に関するマークを定めています。

クリエイティブ・コモンズ・ライセンスの表示であることを示し、すべての権利が留保されている（個別の許諾がなければ使ってはいけない）とする©All Rights Reserved から、著作権保護期間が終了しパブリック・ドメイン（自由に利用可能）になるまでの間の段階に位置する、Some Rights Reserved の条件を、マークによって示す。

パブリックドメインを意味し、著作権の保護期間切れを示す。つまり自由に使ってよいコンテンツである事を意味する。(PD) と表記される例もある

この場合、「表示ー非営利ー改変禁止」となり、クレジット表記をした上で、非営利目的で改変しない限りにおいては、再配布が可能、という意味になる。

「表示」(BY) を意味し、著作者のクレジット表記などをすることを条件とする。営利目的での使用可。改変も可。再配布可。

「非営利」(NC) と意味し、非営利目的の使用に限って利用が許可される。非営利であれば、改変、再配布も可。

「改変禁止」(ND) を意味し、オリジナルのまま使用することを条件とし、改変や切り抜きレタッチなどはできない。そのままであれば営利目的での使用も可。

「継承」(SA) を意味し、改変を行った場合は元のライセンス条件を継承することで再配布を認める。条件を守れば営利目的の利用も可。

参考：クリエイティブ・コモンズ・ジャパン　ウェブサイト
https://creativecommons.jp/
クリエイティブ・コモンズに関して、詳しくは上記ページを参照してください。

無断使用は著作権侵害で賠償も

インターネットでは「パクリ」▶用語集 P.200と呼ばれる著作物の無断使用が散見されます。無断で使ってもばれないだろうといった軽い気持ちで使ってしまっているのでしょう。しかし、私たちが普段インターネットの検索エンジンを使って、世界中のウェブサイトにある情報を検索できるように、画像などが使われている場所も検索できるので、他人の著作物を勝手に使った場合、それが判明してしまいます。そもそも、著作物を著作権者の許諾なく勝手に利用する行為は、著作権法に違反し、著作権者から無断使用に対する損害賠償請求を受ける可能性があります。きちんと著作権者の許諾を得てから利用するか、利用条件が明示されているコンテンツをその条件にしたがって使いましょう。

写真の著作権と被写体の権利の両方に注意しよう

自社サイトの広告や記事などを作るとき、「写真を掲載したい」と感じることはよくあるでしょう。その際、写真には、写真そのものの著作権だけではなく、被写体の権利にも注意をする必要があります。写真を撮影した人（＝写真の著作権者）から、写真を利用することについて許諾をもらっていたとしても、肖像権のある被写体である人から「ダメ」と言われたら、その写真を使うことはできません。写真については、「ストックフォト」など、被写体の権利について明記したサービスなどもあるので、目的に応じて使いやすいものを選びましょう。

このようなコンテンツの利用条件を簡単に示すものとして、「クリエイティブ・コモンズ・ライセンス」がよく使われています。

クリエイティブ・コモンズ・ライセンスではそれぞれ「どう使ってよいか」が、マークなどで明記されているので、その範囲で活用させてもらいましょう。

コンテンツの利用を許諾している著作権者の中には、自分のコンテンツをどこで使ったか教えて欲しいという方もいるので、その場合は、どこで使ったかを報告するとともにコンテンツを使わせてもらった感謝を伝えましょう。

著作権には保護期間があり、すでに述べたとおりこれを過ぎると基本的には自由に使うことが出来ますが、個人が著作者である著作物の保護期間は著作者が亡くなってから70年なので、いつ保護期間が終わったのか簡単に分からない場合もある点に注意が必要です。

また、自社のウェブサイトで、写真を利用したい場合などもあると思いますが、写真などを利用する場合には、写真そのものの著作権だけではなく、被写体の権利にも注意をする必要があります。例えば、人物を撮影した写真の場合には、被写体となっている人には肖像権があります。ですので、写真を撮影した人（＝写真の著作権者）から、写真を利用することについて許諾をもらっていたとしても、写っている人から「ダメ」と言われたら、その写真を使うことはできません。また、その写真に、絵画などの別の著作物が写っている写真を使おうとする場合には、原則その絵画の著作権者からの許諾も必要となります。したがって、写真やイラストなどを使おうとする場合には、その写真やイラストの著作権者の許諾だけではなく、被写体（描写されている人・物）についての許諾があるかどうかを確認する必要があります。

ネット上で見つけた写真を利用する場合には、そのような被写体の権利についても配慮し、例えば、被写体の人物からの許諾がきちんと得られているのか、または人物が特定できないようになっており被写体である人からの許諾なく使用してもよいものなのか、などについても確認してから利用するようにしましょう。

写真のコンテンツに関しては、「ストックフォト」といわれる写真素材があります。「ストックフォト」は、特定のシチュエーションでの使用が想定された写真素材では、被写体についての許諾のあり／なしが明示されている場合があります。ウェブ上で自社を紹介する広告や記事などを作りたいときに写真が必要になったら、許諾があることを明示された写真を選ぶとよいでしょう。ちなみに、ストックフォトは有償無償さまざまなサービスがありますが、被写体についての許諾は、人物の場合は「モデルリリース」、物の場合は「プロパティリリース」などという表記が使われているケースをよく見かけます。

10 取引先の監督を徹底しよう

自社のセキュリティは十分に高度にしていたのに、大事なデータを渡していた関連会社や取引先がずさんな管理を行なっていて、個人情報を流出させてしまった……。

そんなとき「関連会社がやったから……」といったとしても国民や社会の理解を得ることができないのは、これまでの情報流出の事例を見ても明らかです。

自社が持っている個人データの取扱を利用目的の達成に必要な範囲内において委託し、それに伴って取引先に当該個人データを提供する場合には、本人の同意に基づき取引先に提供する場合と異なり、記録義務はありません。しかし、その一方で取引先を監督する義務を負います。

具体的には

1．プライバシーマークを取得するなど、きちんと個人情報を取り扱える能力のある業者を選定すること

2．取扱の内容を契約書に明記すること

3．契約の内容が守られているか定期的に監査すること

4. 業務委託先が外国に設置したサーバーで顧客データを取り扱う場合は、どのような安全管理措置が講じられているかについて明示して監査すること

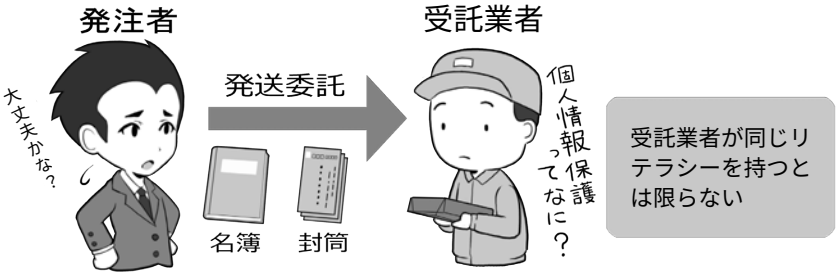
が義務づけられます。

詳しくは個人情報保護委員会のウェブサイトなどを参照して欲しいですが、こういったことをきちんと行うことが、個人情報を厳密に扱う姿勢を委託先に示すことになり、不正な個人情報の流出への抑止力になると考えて下さい。

P.161で紹介したように、企業のグループ内であっても同様で、問題が発生したときに「関連会社が」とか、「委託先が」といって責任を逃れることは許されません。個人情報を取り扱う者は、会社や団体の社会的な義務を果たし、また、流出した情報に関してはきちんとした責任を負わなければなりません。

流出がおきれば、実際のお金としての負のコストや、それに対処するためにマンパワー、信用喪失が見えないコストとして、自分たちに跳ね返ってくる点を十分理解して適切な措置を講じる必要があります。

取引先が自分と同じリテラシーを持つとは…



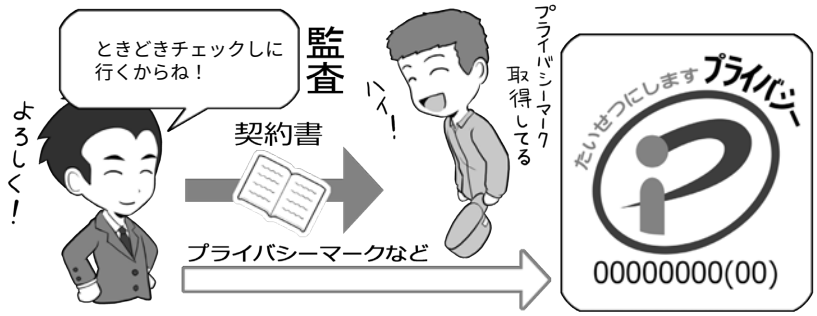
個人情報やプライバシーに関して、きちんと管理しなければならないことであるという意識は広がりつつありますが、それは自社や自団体の中だけにはなっていませんか？

その意識は取引先や委託用務先まで徹底されてるでしょうか？

自社や自団体と委託先は別ではなくて、例えば宛名を渡して発送業務を行う場合でも、その個人情報にまつわる監督責任が発生します。また、委託先が自社や自団体と同じリテラシーを持つと安易に考えないで、確認を怠らないようにしましょう。

専門性のある委託先に業務をアウトソースしてコストを抑えるのはよいことですが、抑えるべきポイントは抑えましょう。

自分たちも相手もトラブルにならないために



個人データを取り扱う業務を委託する場合は、委託先を監督する義務が発生し、プライバシーマークを取得しているかなど適切な取扱の体制が整備されているかを確認し、個人データの取扱に関して契約書に明記し、その内容が守られているか定期的に監査するなどの対応が必要となります。

なお、プライバシーマークに関しては一般財団法人日本情報経済社会推進協会 (JIPDEC) のウェブサイトの、プライバシーマーク制度のページに詳しく記載されているので、参照してみてください。また、実際に取得する場合は、職種によってはそれぞれの職種の団体を通じて取得申請をする場合があります。

日本国内であっても海外の方の個人情報を取り扱う場合は、EU の GDPR(一般データ保護規則) ▶用語集 P.190 など、さらに注意が必要な法制度がありますので、業務を行う前に精査しましょう。

・プライバシーマーク制度（一般財団法人日本情報経済社会推進協会）
https://www.jipdec.or.jp/project/pmark.html
・GDPR(General Data Protection Regulation: 一般データ保護規則) 個人情報保護委員会
https://www.ppc.go.jp/enforcement/infoprovision/laws/GDPR/