第6章

中小企業等向け

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企業等にとって、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
1.2 自組織の情報セキュリティの状況を確認する
1.3 セキュリティ対策に必要な投資資金を確保する
1.4 セキュリティ対策の適宜見直しを図る

2 災害時やサイバー攻撃時に会社を守る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
2.2 社員や家族の安全確認をしましょう
2.3 人的損失をリカバリする能力

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
3.2 効率的なアウトソーシング

4 ファイルの権限設定や情報の公開範囲を見直そう

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
5.2 より能動的に情報収集しよう

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によるリスク
6.2 オフショア開発や海外委託によるリスク
コラム.1 サプライチェーン攻撃のパターンと対策
コラム.2 サプライチェーンに対する攻撃事例について
6.3 問題が起きると事業継続に影響を及ぼす

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 サイバー攻撃の脅威を知ろう
7.2 不正アクセスの傾向
7.3 ランサムウェアの傾向
7.4 標的型メール攻撃の具体例
7.5 フィッシング攻撃の傾向
7.6 不正送金の傾向
7.7 ウェブサービスへの不正ログイン
7.8 ウェブサイトの改ざんやSNSの乗っ取り
7.9 DDoS攻撃
7.10 従業員・職員等の利用者に対する情報教育等を怠らない

8 個人情報は法律に則り適切に取り扱おう

9 取引先の監督を徹底しよう

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.189 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.182 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一つもないだろう」と思われている人もいるではないでしょうか？しかし、現在の攻撃者▶用語集 P.182 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。

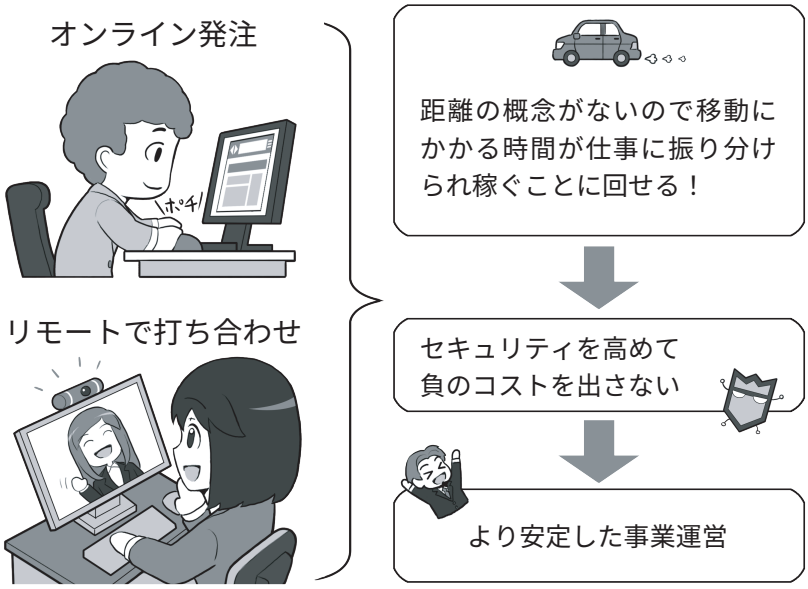
近年では「セキュリティ・バイ・デザイン」▶用語集 P.183 という考え方が一般的になりつつあります。企業のITシステムや業務プロセスなどを企画・設計する段階でセキュリティ対策を組み込んでおき、サイバー攻撃による不測の事態に備えるのです。

本章1.3(P.137)でも触れますが、適切なセキュリティ対策には一定の財源も必要です。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 自組織の情報セキュリティの状況を確認する

セキュリティ対策を実施するとしても、具体的な対策の内容は、各組織の実態によって異なります。例えば、インターネットとは全くつながっていないシステムしか使っていない組織と、何らかの形で外部と接続している組織では、セキュリティ対策の内容が違ってきます。

そのため、セキュリティ対策の前提として、自組織のセキュリティの状況を把握する必要があります。これを行うためには、

- 利用する情報資産・システム（以下情報資産等）の棚卸
- 情報資産等に対するリスク確認の実施
- リスク確認を踏まえたリスク管理の実施
- リスク管理に基づく具体的なセキュリティ対策の実施などが求められます。

利用する情報資産等の棚卸は、組織が業務で用いるために保有する情報資産とこれを取扱うシステム等を把握し、棚卸を行うことです。保有している情報資産等の実態がわからないと、何に対してセキュリティ対策をすればいいのかわからないですし、棚卸の結果、実は不要であったり、あるいは保有期間を制限したりするなどの見直しの機会にもなります。システム等についても同様で、業務上利用するシステムやサービス、機器等の棚卸を行うことで、セキュリティ対策の対象を整理することができます。

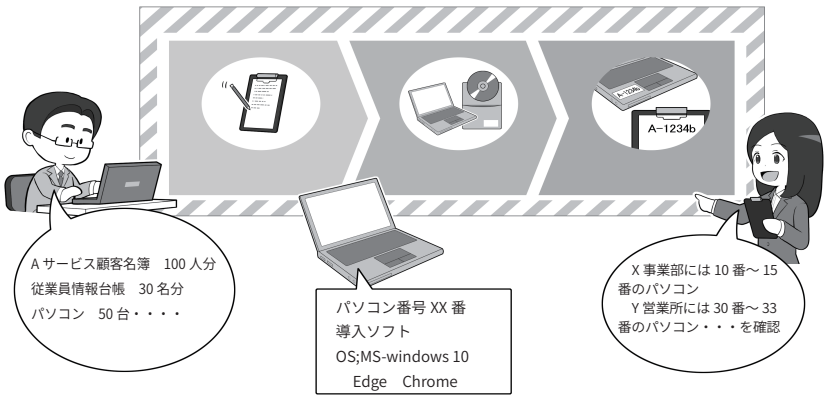
次に棚卸した情報資産等を業務上用いるにあたって、想定されるリスクを確認します。例えば、災害によりシステム等が破壊されるリスク、組織内外の要員により情報が外部に流出するリスク、システムの異常により業務が停止するリスクなどが想定されるものを確認します。リスクの確認は、組織が利用する情報資産等や、業務、管理状態の実態を踏まえて行います。

リスクの確認結果を踏まえたリスク管理の実施は、例えば内部要員による不正な情報漏えいのリスクに対してはリスク低減を図る、業務への影響の小さいリスクについては、リスク低減策をしないままにする等、リスク管理の対応方針を決定します。

そのうえで、具体的なリスク低減に資するセキュリティ対策などを講じることになります。例えば従業員等による不正な情報漏えいのリスクを低減するため、情報資産等へのアクセスを最小限の範囲にするため利用者や権限を限定する、アクセスできても媒体による持ち出しをシステム上制約するなどの対策を実施することになります。なおセキュリティ対策を講じても生じうる損害等に備えて、サイバー保険などにより、サイバー攻撃からのダメージを軽減する等も一案です。

このように情報資産等の棚卸は、これを踏まえたリスク確認、リスク管理などのセキュリティ対策を講じる前提となります。

自組織のセキュリティ状況の確認は、IT資産の棚卸から



組織のセキュリティ状況を把握するために、組織の中でどのような情報や機器などを保有し、管理しているのかを確認する、IT 資産の棚卸が必要です。
業務にどのような情報をどのように取扱っており、これを適切に管理できるような対応をとることがセキュリティ対策の前提となります。

1.3 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用語集P.181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.184、クラウドストレージ、ウェブサーバ▶用語集P.180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.185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.179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。

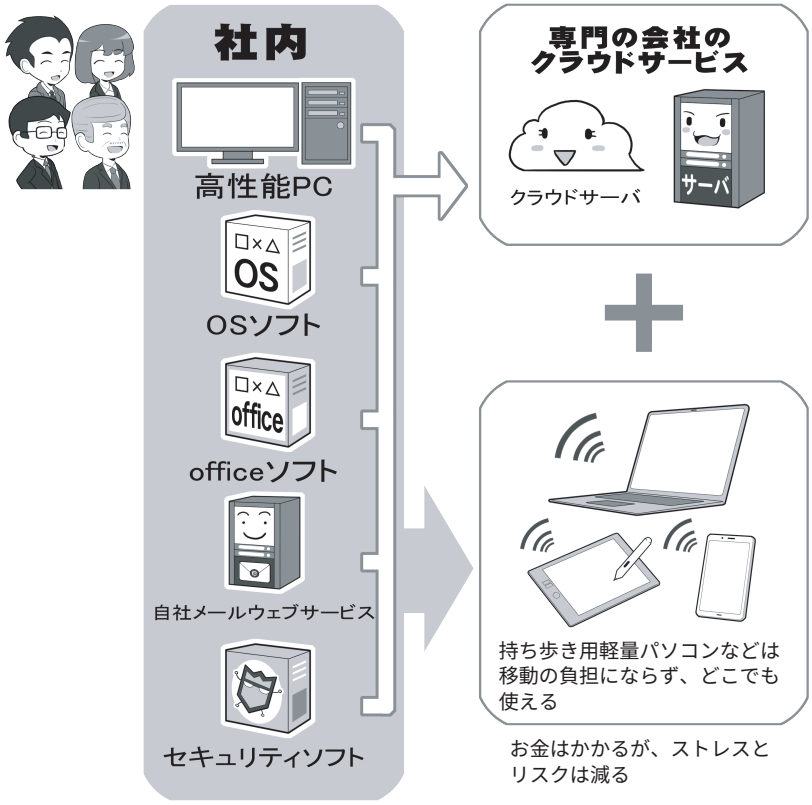
こういった新しいシステムや環境は、セキュリティ対策も込みで提供される場合や、これまでバラバラだったコストが集約・整理されて軽くなる場合があり、総コストが従来より安く済むこともあります。ただし、逆にコストがかかる場合があるので、導入前にしっかり確認しましょう。また、クラウドサービスは設定次第で誰でもアクセスできる場合がありますので、設定に注意して利用する必要があります。

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.184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。

外部依頼できる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止し、パッケージ型のソフトウェアも廃止し、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

1.4 セキュリティ対策の適宜見直しを図る

DXの掛け声とともに、新しいシステムやサービスの導入も進められています。一方でサイバー攻撃は巧妙化・高度化が進み、対策が求められています。

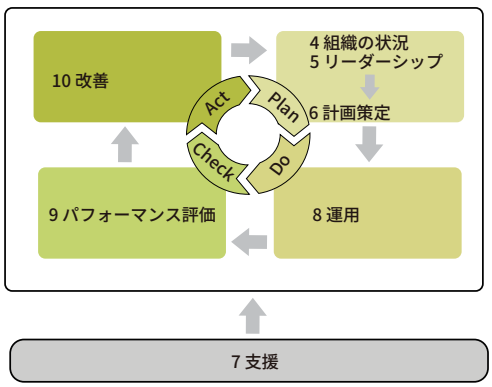
セキュリティ対策は一度、内容を決めればそれでよいというものではなく、情報資産等の変更や外部からの脅威の変化に応じて、その内容の見直しを図る必要があります。

このようなセキュリティの管理方法として、PDCAサイクルによるマネジメントが挙げられます。これは、P(Plan：計画策定)、D(Do：実施)、C(Check：実施内容の確認)、A(Act：実施内容の改善)から構成されるものです。このようにセキュリティ対策についても、PDCAサイクルに基づいて定期的に見直すことにより、実態に即しつつ、新たに求められる要請に対応したセキュリティ対策を運用することにつながります。

なお、情報システムのセキュリティに関するマネジメントシステムの規格としてJIS Q 27001(ISMS)があります。これは、組織のマネジメントシステムについて規格化し、その規格に沿った運用ができている組織に対して第三者認証するものです。ISMSの取得は、組織における情報システムの運用体制の信頼性を向上するため、必要に応じて認証取得することも、企業においては求められます。

組織の情報セキュリティにおけるマネジメントシステム

まえがき	
0 序文	0.1 概要 0.2 他のマネジメントシステム企画との両立性
1 適用範囲	
2 引用規格	
3 用語及び定義	
4 組織の状況	4.1 組織及びその状況の理解 4.2 利害関係者のニーズ及び期待の理解 4.3 情報セキュリティマネジメントシステムの適用範囲の決定 4.4 情報セキュリティマネジメントシステム
5 リーダーシップ	5.1 リーダーシップ及びコミットメント 5.2 方針 5.3 組織の役割、責任及び権限
6 計画策定	6.1 リスク及び機会に対処する活動 6.2 情報セキュリティ目的及びそれを達成するための計画策定 6.3 変更の計画策定
7 支援	7.1 資源 7.2 力量 7.3 認識 7.4 コミュニケーション 7.5 文書化した情報
8 運用	8.1 運用の計画策定及び管理 8.2 情報セキュリティリスクアセスメント 8.3 情報セキュリティリスク対応
9 パフォーマンス評価	9.1 監視、測定、分析及び評価 9.2 内部監査 9.3 マネジメントレビュー
10 改善	10.1 継続的改善 10.2 不適合及び是正措置
付属書A（規定）	情報セキュリティ管理策



組織の情報セキュリティマネジメントの国際規格として「情報セキュリティマネジメントシステム（ISMS）」（ISO/IEC 27001）が定められています。この中では上図のようにPDCAサイクルに従って、マネジメントを運用することが含まれています。なおこれを踏まえてわが国では国内規格として「JIS Q 27001」が発行されています。

出所：「ISO/IEC 27001(情報セキュリティ)」(一般社団法人日本品質保証機構)https://www.jqa.jp/service_list/management/service/iso27001/

2 災害時やサイバー攻撃時に会社を守る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.176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」のウェブサイト用語集P.180*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業務ではなく、オフィスでの作業を行う業務の人は、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業務を行うことができます。

また、業務に利用するパッケージソフトをオンライン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。

最近ではこういったソフトは、クラウドサービスとして提供され、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.187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やパスワード▶用語集P.186を入力する作業はやってはいけないこと。

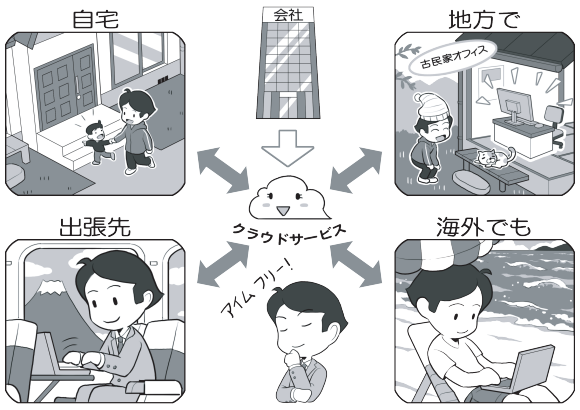
2点目。災害時には被災者が通信を円滑に行えるよう暗号化▶用語集P.179されていない無線LAN▶用語集P.188が各所で提供されます。これも攻撃されやすいポイントなので、使用する場合はVPN▶用語集P.178を使うこと。

3点目として、会社などから支給されたものではなく、私物を業務で利用する場合(BYOD(Bring Your Own Device))▶用語集P.176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.188に感染すれば仕事の情報も漏えいする可能性があり、実被害も出ています。

組織のセキュリティレベルを下げないためにも、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。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ける形でテレワークを活用することによって、社員や会員のライフワークバランスを向上させることもできます。

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。

* 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 社員や家族の安全確認をしましょう

災害時は原則としては政府や各自治体・消防などの指示に従うべきですが、ときに徒歩帰宅をする選択肢を取らざるを得ない場合もあります。

スマホには学校や仕事場から自宅までの道中、災害時に役立つ情報を掲載した帰宅支援マップやアプリ▶用語集 P.179 を入れておきましょう。日没時や降雨時の避難場所などもわかります。

その場合に備え、家族と落ち合う集合場所や、帰宅手順を話し合っておきましょう。長期大規模停電で通信できない状況まで想定して、プランを立てましょう。

避難場所に到着し、そこが安全であると確認できたら、安否確認の連絡や情報収集をしましょう。

安否確認サービスはさまざまなものがあるので、事前に家族や同僚たちと、どのサービスを利用するかを決めておきましょう。例えばNTTが運営する災害伝言ダイヤル(171)*1や災害用伝言版*2を利用するのも一案です。

また、災害時は電話やウェブサイトの閲覧などは混み合ってつながりにくくなります。スマホアプリの通話機能も通信容量を多く使うため、災害時に通話が優先される公衆電話や、なるべくデータ通信量の少なくてすむ、メールやSNS▶用語集 P.178 のメッセージなどのサービスを使いましょう。

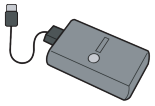
なお、スマホアプリの通話機能もメールなどより通信容量を多く使います。譲り合い、少ないデータ通信ですむ手段を優先しましょう。

万が一災害が起こった場合、緊急時の安否確認などが速やかに行える　連絡手段(SMS▶用語集 P.178 等)について　も周知しましょう。

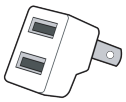
災害時に徒歩帰宅をする場合は

帰宅マップ

予備電池



ACアダプタ



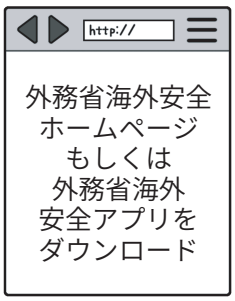
USB
カーチャージャー

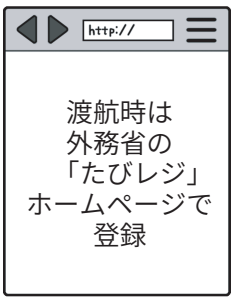
タブレット対応か
チェックする
(2Aなど)

注)「外務省海外安全アプリ」では、約120ページの「海外安全虎の巻」が同梱されていたり、海外安全にかかわる外務省のホームページなどを簡単に分類し、手早くアクセスできるようになっていたりするので、ぜひダウンロードしておきましょう。

海外での災害やテロに備える場合は

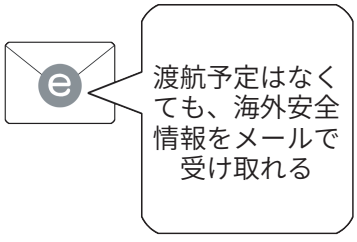
渡航前後に現地の情報を確認する　**外務省たびレジに登録する**





緊急時は
SMSで連絡

たびレジ簡易登録にメールアドレスを登録する



滞在国によっては
周波数に対応した
AM\FM\短波ラジオ

*1 災害伝言ダイヤル(171) https://www.ntt-east.co.jp/saigai/voice171/
*2 災害用伝言版 https://www.ntt-east.co.jp/saigai/web171/

2.3 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.177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。

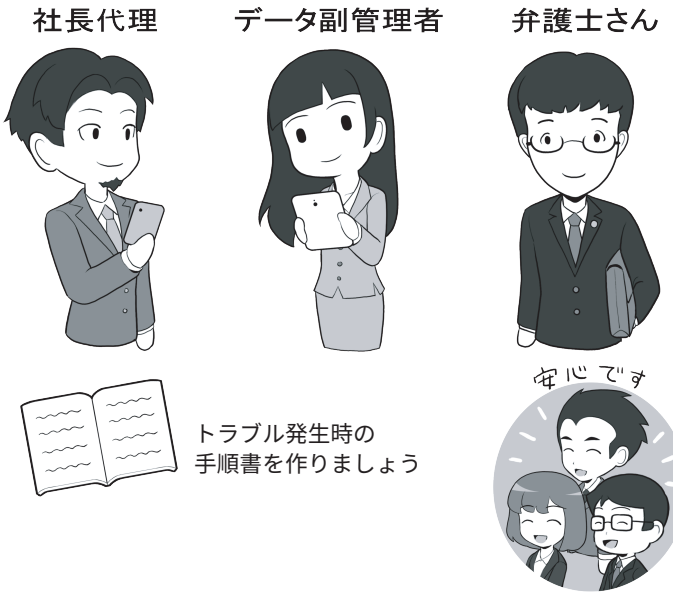
また、それが難しい場合は、例えばクラウドでもアクセス可能なパスワード管理アプリ▶用語集 P.186を利用し、そのマスターパスワードやPINコードを、弁護士に託し、なんらかの理由で本人による事業継続が困難であると判明した場合は、弁護士に情報を開示してもらうのです。それは昔、貸金庫の鍵を弁護士にも持っていてもらったのと同じです。

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。すべては「想定外」にならない想像力がものをいいます。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。

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

職種や企業などの方針にもよりますが、テレワーク、リモートワークという働き方により、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。

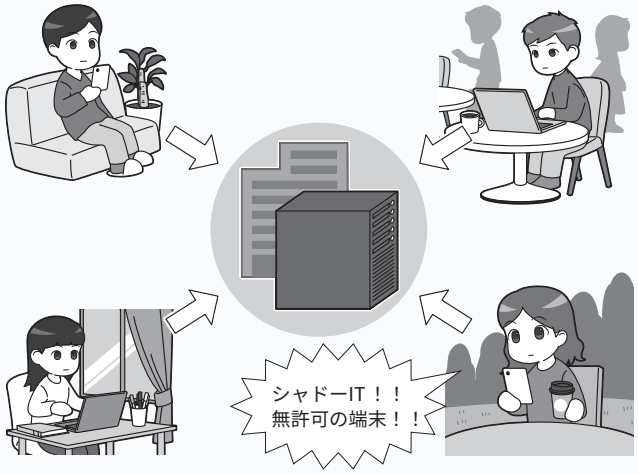
BYODの実施にあたっては、従業員が端末を盗難された場合など、想定されるセキュリティ上のリスクを企業側が事前に把握し、例えば端末にデータを残さない方式を採用するなどの対応をする必要があります。総務省では、BYODも含め、テレワークにおけるセキュリティ対策を示す「テレワークセキュリティガイドライン」を公表していますので、参考にしましょう。

BYODの実施には企業が運用のルール設定する必要がありますが、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、あるいは社内から許可されていない外部のサービスを利用するなどのケースが生じるようです。例えば、業務連絡にSNS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。

シャドーITは、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ことや、シャドーITが使えないような対策を講じること、従業員との良好なコミュニケーションを図ることなど、アプローチも考慮しましょう。

一般社団法人日本テレワーク協会もテレワークの環境を整備しやすくするため、「テレワーク導入ガイドライン*」などを公開しているので、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

* テレワーク導入ガイドライン https://japan-telework.or.jp/tw_info/suguwakaru/guide/

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、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。

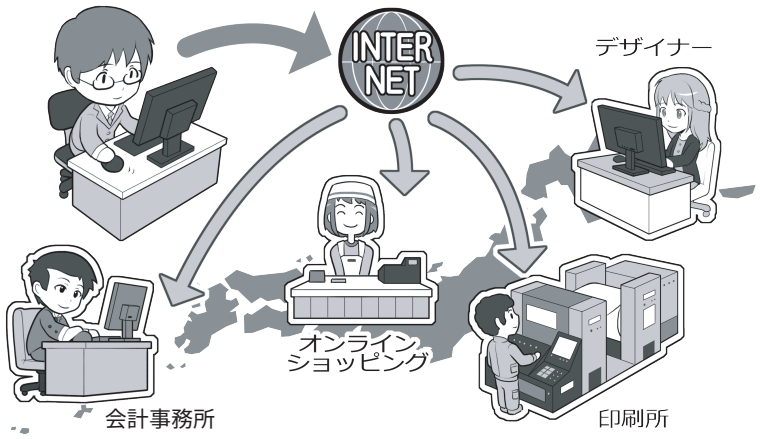
また、経理処理なども会計ソフト会社がオンライン対応になることで、取っておいたレシートをスキャナやスマホの撮影機能経由で提供されているクラウドサービスにダイレクトにアップロードすると、基本的な伝票入力が行われた状態で会計ソフトに返ってくるようになっているものもあります。

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重要です。

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。詳しくは付録06(P.172)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 ファイルの権限設定や情報の公開範囲を見直そう

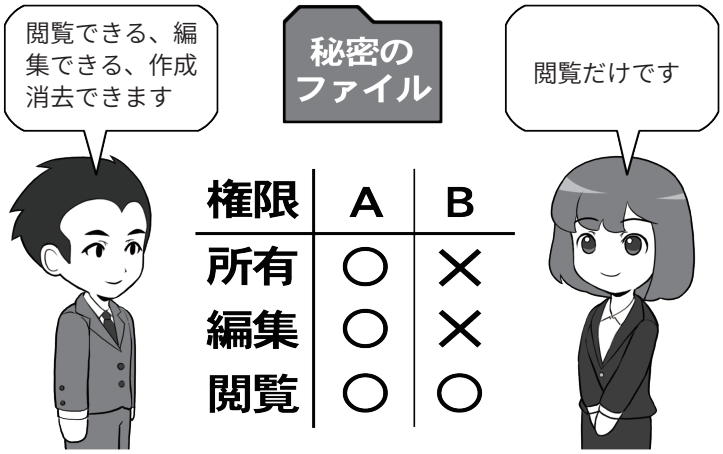
権限設定とは、私たちがIT機器上やインターネット上で使用するファイルや情報、あるいは機器そのものに関して、自分だけでなく誰かと共同で利用するときに、機密性を保つために必要な設定です。

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.181があります。

会社内でファイルをUSB▶用語集P.178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)を設けている企業であれば、ファイルを管理する「NAS」(NAS: Network Attached Storage)▶用語集P.177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。

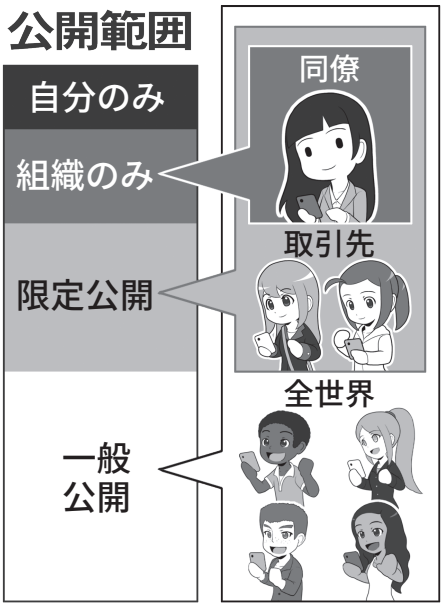
クラウドストレージサービスのようなインターネット上のサービスにも共有設定があり、「公開範囲」▶用語集P.181と呼ばれることが多いようです。インターネットのサービスの公開設定を一般公開にした場合、インターネットにアクセスする世界中のすべての人に公開することになりますので、注意が必要です。

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.180したりした企業の事例もあります。

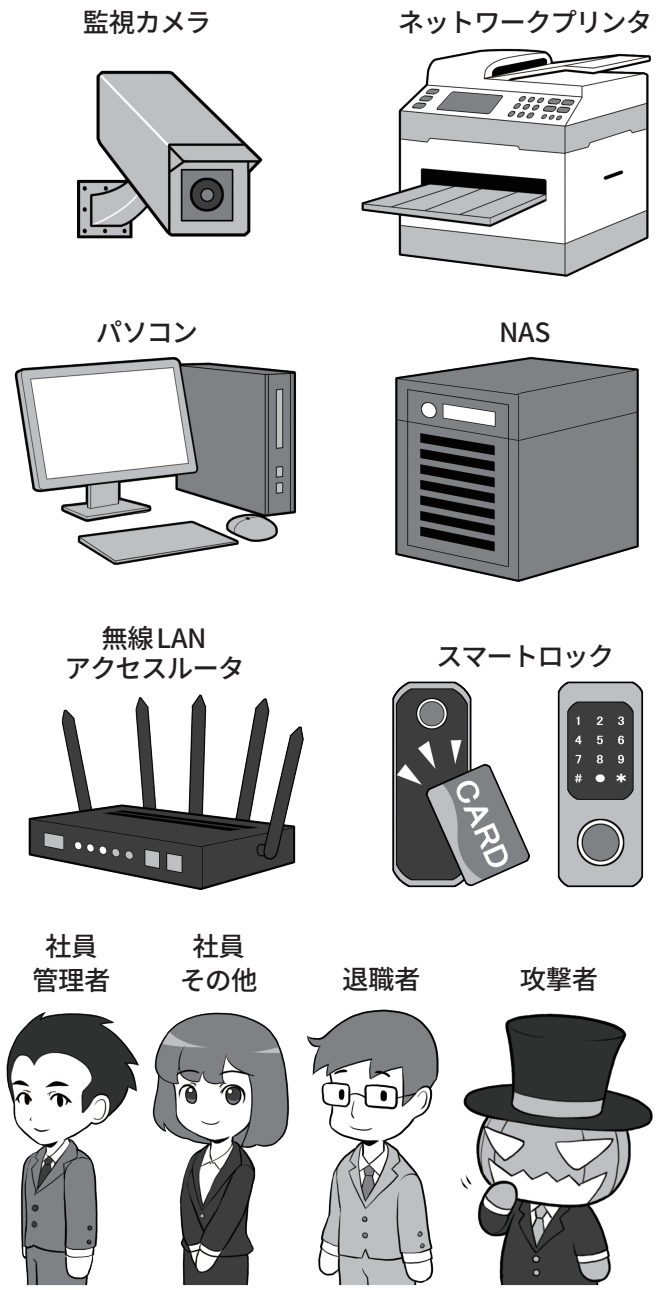
LAN上のNASでもストレージサービスでも、共有設定はファイル単位やフォルダ単位で設定できるので、その整合性に気を付けないといけないことと、例えば臨時で誰かに特定のファイルを公開したい場合、設定ではなく「見たり編集したりできる」リンク▶用語集P.189を送信することで共有することができるものもあり、この場合、そのリンクを知っている人は誰でも同じ権限を持つので、送信後の管理にとくに注意が必要です。

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.189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業務関係者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、入退室に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.179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.181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.184（イントロダクション6.2（P.22）参照）で社員を騙し、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。

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いるか知り、また、攻撃者の手口を知ることが重要です。本書でも第2章でサイバー攻撃の手口について、まとめています。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▶用語集P.183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.177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。

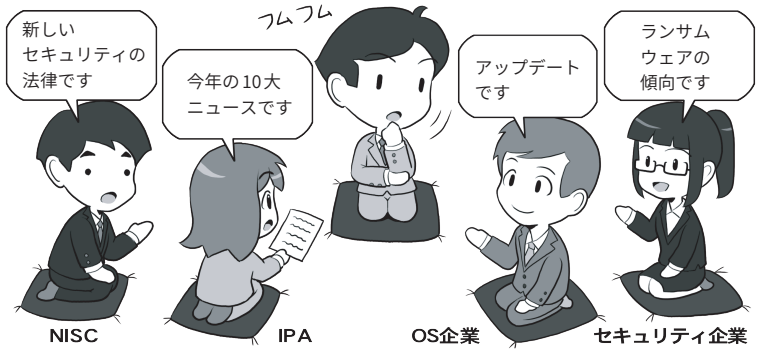
もっと横断的な情報が欲しい場合は、IPAやNISC▶用語集P.177などの政府機関のアカウントやメールマガジン、セキュリティや詐欺関連の対策機関の公式アカウント、セキュリティ系雑誌の記事を追いかけるようにしておけば、大規模なサイバー攻撃の兆候やセキュリティホール▶用語集P.184の発覚をいち早く察知することができ、その対策を立てることが容易になります。後述のように最近では、SNSによる情報発信もされているので、適宜フォローする等して、最新の状況を確認できるようにすることを推奨します。

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▶用語集 P.180メディア、セキュリティ識者のSNSやブログなどを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。そこで、RSS ▶用語集 P.177 と呼ばれる仕組みを利用することで、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るので、日常的に攻撃情報の収集が可能となります。

またX(旧twitter)により、NISC、IPA、警視庁サイバーセキュリティ対策本部などが情報発信しているのでこれをフォローすることで定期的に収集できるので有用です。

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

JP-Cert：https://www.jpcert.or.jp/rss/

トレンドマイクロ：https://www.trendmicro.com/ja_jp/download/rss.html

X(旧Twitter)

警察庁： https://x.com/mpd_cybersec

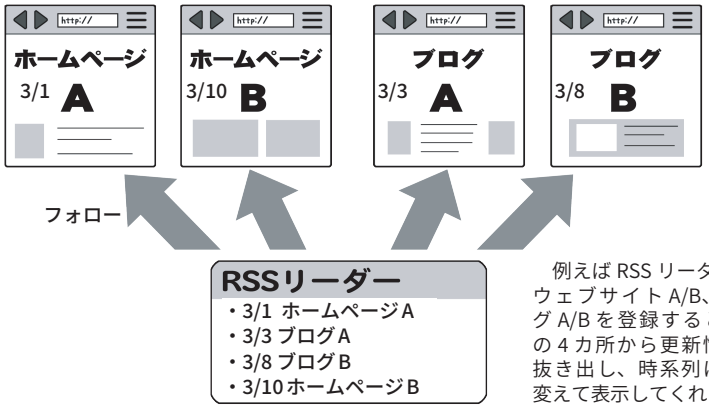
NISC(注意・警戒情報)：https://x.com/nisc_forecast

IPA(情報セキュリティ安心相談窓口)：https://x.com/ipa_anshin

RSSってなんぞや

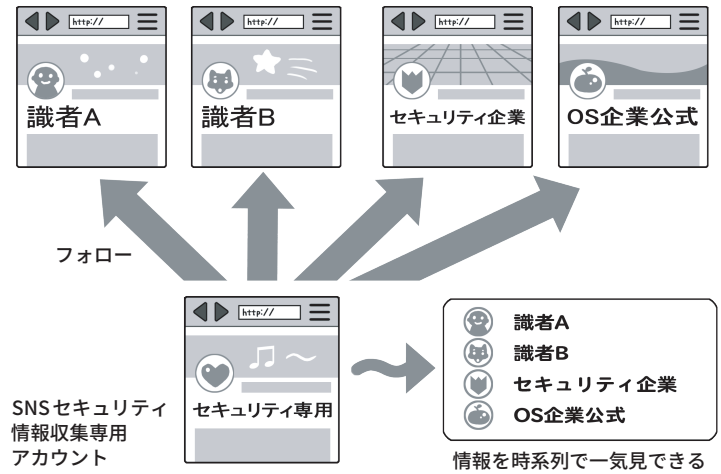
RSSとは平たくいえば、ウェブサイト上の更新情報を、見出し、もしくは概略付きで、時系列に、ウェブサイトの裏の見えない所で発信しているものです。規格（フォーマット）が決まっているので、RSSリーダーに登録すると複数の情報源を串刺しして見ることができます。

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よるリスク

「サプライチェーン攻撃」とは、企業等間のつながり(サプライチェーン▶用語集P.182)を利用したサイバー攻撃のことです。この場合、攻撃者は、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った攻撃を仕掛けます。サプライチェーン攻撃では、例えば自社がセキュリティ対策を十分に実施していても、直接攻撃されて踏み台▶用語集P.188となった企業を経由し、さまざまな被害を受ける可能性がある点です。その意味では外部との関係性を整理するほか、関係者を含めた情報共有や緊急時の対応体制の構築が重要となります。

サプライチェーン攻撃のパターンとしては、いくつかの種類があります(本章コラム1(P.149)参照)。

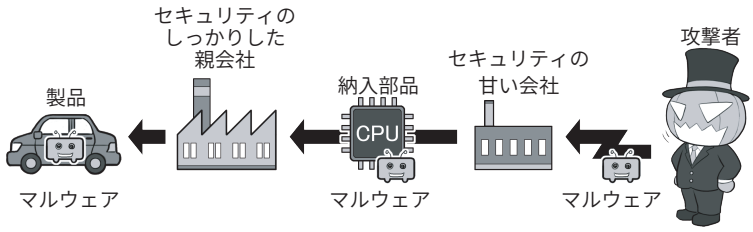
「サプライチェーン攻撃」においては、第一に機器やアカウントの乗っ取りに注意しましょう。業務上つながりがある場合は、乗っ取った企業の従業員のアカウントから、メールをダウンロードして、取引先の相手の氏名やメールアドレスを盗み出し、日常的にやりとりしている文面を模倣して、マルウェア付きのフィッシングメールを送り付けます(イントロダクション6(P.21)参照)。

また最近では、IT機器のぜい弱性▶用語集P.183を攻撃して、IT機器のアカウントを乗っ取り、そこから侵入するケースも多く見られます。

また電子機器を生産している企業に攻撃し、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.186を仕込み、これを取引先に納入させることで、取引先が生産している製品を乗っ取る環境を整えて、攻撃するなどがあります。

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。

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。

6.2 オフショア開発や海外委託によるリスク

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。

またクラウドサービスなどでは、国外企業にデータの取り扱いを再委託するケースもあります。この場合、特に個人情報保護▶用語集P.182についての法制度が異なる国への再委託では、想定しない形でデータが漏えいする可能性もあります。

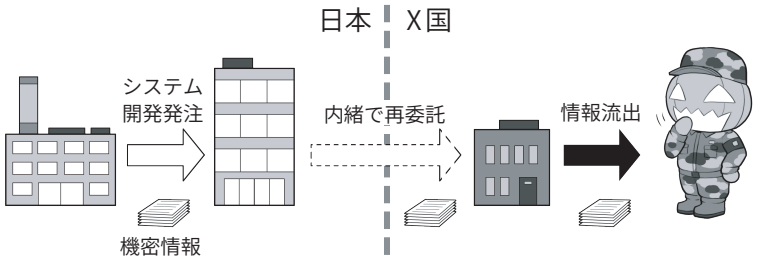
そのようなことを防ぐため、契約時には禁止行為や監査などを取り決めましょう。

またオフショア開発など以外で、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。例えば、国外事業者が提供するドローンやスマホのアプリでは、その利用に使われた利用者のデータ履歴などが、サービス品質の向上を理由に、国外に送信されるなどのケースもあります。この場合、違法ではありませんが、必ずしも利用者が意図しない形で情報が国外に流れることになります。

このように、海外への委託等を行う場合には、その契約内容等を十分に確認し、必要な管理体制を取ることが重要です。

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、受託した企業がよ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。

コラム.1 サプライチェーン攻撃のパターンと対策

一口にサプライチェーン攻撃にはいくつかの被害結果からみたパターンがあり、それに応じた平常時・緊急時の対策が挙げられます。サプライチェーン攻撃のパターンについては、例えば、

① ソフトウェア開発工程においてウイルスを混入させて、納入先に汚染されたソフトウェアを混入させる場合(保守によるソフトウェア提供含む)

② ユーザーを多く抱えるクラウドサービスなどのサービス提供事業者のサイトを攻撃した上で、そこを経由して攻撃が行われる場合

③ ビジネス上のサプライチェーン上において関連組織間でネットワークが接続されていたがために攻撃の影響が拡大するといった場合

④ 部品メーカーがサイバー攻撃を受けて操業が停止したがために、組み立てメーカーが損害を被るといた場合

などが想定されます。

例えば、①、②は自社が使うシステムやサービスの供給元において生じた攻撃への対応となります。それぞれ、平常時には供給元に対する必要なセキュリティ対応を求めるほか、攻撃などがあった場合には、適切な情報提供、特に自社へのシステムの影響や情報漏えい等の被害の可能性、対策等についての情報共有体制が重要となります。①の類型においては、より自社のシステムへの影響の可能性が高いため、システム対応上の支援等も求められます。また必要に応じてベンダーとの間での取決め(契約やSLAなど)を行い、緊急時の責任や対応の範囲を明確にすることも重要です。

③のようなケースでは、自社のシステムが外部の取引先とどのように接続されているのか、を正確に把握するとともに、接続先の企業とはセキュリティのレベルについて平常時から合意し対応するほか、緊急時の情報提供も含めた体制作りが重要となります。特に被害状況に関する情報や接続対応に関する情報が速やかに共有されることが重要となります。また接続先も、日常の取引目的だけではなく、例えばシステムのリモートメンテナンスなど取引以外の目的のためのものなどについても整理する必要があります。

④の類型の場合には、技術的なセキュリティ対策の問題というよりは、BCPとしてどのように対応するか、BCPの中に具体的なシナリオとして想定し、部品調達ルートの確保などを含めた対応を行うことが求められます。

このようにサプライチェーン攻撃については、関係者間での平常時・緊急時の情報共有が重要となりますが、個々の共有内容や対策内容などは、関係者間の類型により異なるので、それぞれのパターンをシナリオとして想定した対策が求められます。

コラム.2 サプライチェーンに対する攻撃事例について

近時は、企業間でもDXが進展する中で、サプライチェーン型のシステムやサービス利用が増えています。サイバー攻撃においても第６章６(P.148)で示すように、サプライチェーンでつながっている組織の一部、または連鎖的に攻撃し、サプライチェーンで主要な地位を占める事業者への攻撃や、サプライチェーン自体が機能しなくなることを狙った攻撃も見られます。

ここでは、サプライチェーンを狙った攻撃、特にランサムウェアを用いた攻撃の例を紹介します。

【医療機関の納入業者におけるサプライチェーンを狙った攻撃の例】

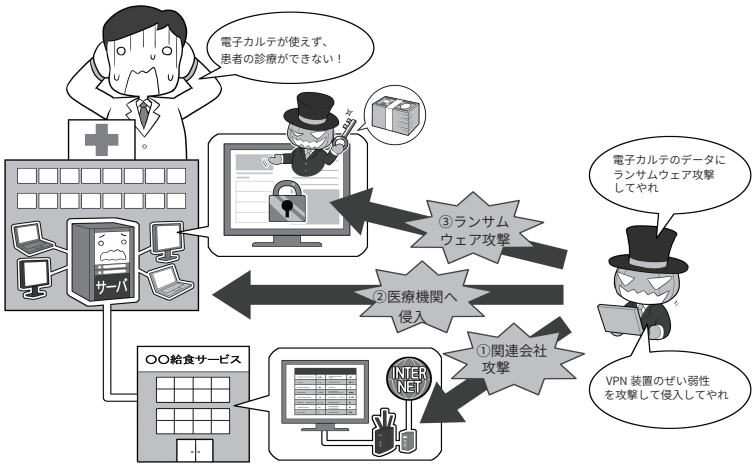
医療機関Ａは、県立病院であり、地域の中核的な医療機関としての役割を果たしていました。医療機関Ａの病院内のシステムでは、医療情報を取扱う関係でインターネットの接続を制限していましたが、入院患者向けの給食を納入する外部の給食事業者Ｂとの間では、個別にネットワーク接続していました。給食事業者Ｂは社内システムのメンテナンスをシステムベンダによるリモート保守で行っていましたが、そのために設置したVPN装置が攻撃され、そこから給食事業者経由で医療機関Ａのシステムに侵入され、ランサムウェアによる攻撃を受けることとなりました。

その結果、新規の外来や入院を制限せざるを得ない状況となり、地域医療に大きな影響を与えることとなりました。なお、復旧には、最終的には70日余りを要することとなり、この間、地域医療に影響が生じました。

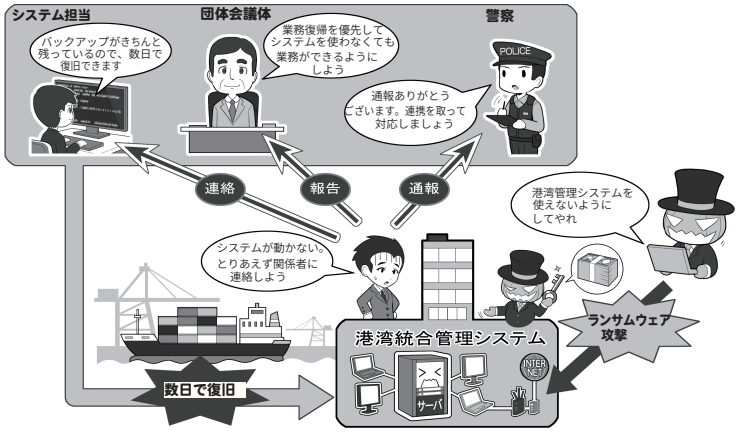
【ランサムウェア攻撃を受けたものの、速やかに復旧した事例】

港湾運送の事業者団体であるＡ団体では、複数のコンテナターミナルを一元的に管理するターミナルシステムを運用していました。このシステムがランサムウェア攻撃を受け、コンテナの搬入・搬出の作業が停止することとなりましたが、約２日半後にシステムを復旧、作業を再開させました。早期復旧の要因として、Ａ団体では日頃から情報セキュリティ研修等の場を通じて警察との関係を構築していたことが挙げられます。この関係を通じ、事案発生時の相談、対応がスムーズになされました。また、事案発生後早い段階で招集されたＡ団体内の関係者による会議体が事実上の意思決定機関として機能したことも要因として挙げられています。

医療機関の納入業者におけるサプライチェーンを狙った攻撃の例



港湾施設におけるサプライチェーンを狙った攻撃の例



6.3 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。

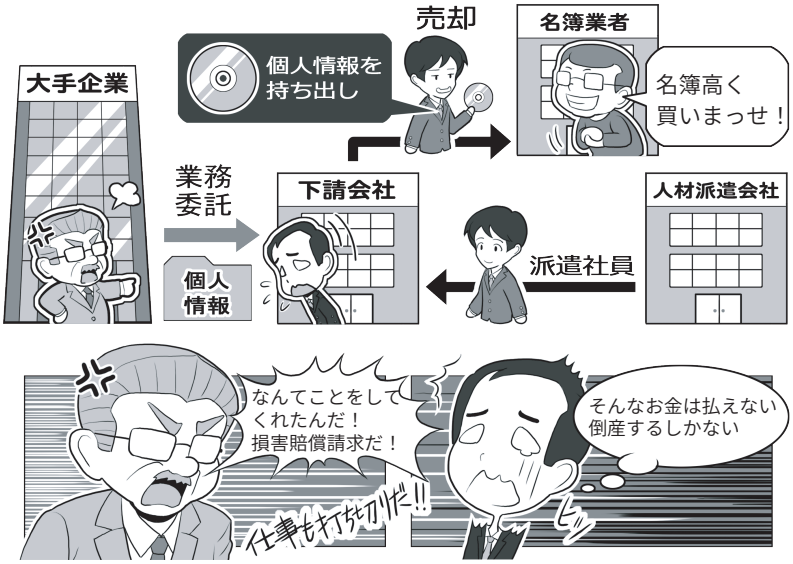
本件は、クラッキングなどを行ったサイバー攻撃によるものではありませんが、内部犯行者によるれっきとしたサイバー攻撃でした。

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企業だったら、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 サイバー攻撃の脅威を知ろう

サイバー攻撃は日々、多様化、巧妙化しています。このようなサイバー攻撃を含む、情報セキュリティに対する脅威について、IPAでは前年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から選定したものを「情報セキュリティ10大脅威」を毎年公表しています。

これによると、近年組織向けの脅威として上位のものとして、

・ランサムウェアによる被害
・サプライチェーンの弱点を悪用した攻撃
・内部不正による情報漏えい等の被害
・標的型攻撃による機密情報の窃取

などが挙げられています。これらの脅威については、本書でも紹介していますが、このような攻撃などにさらされていることを知りましょう。そのうえで、攻撃されたことにすぐに気づくようにし、速やかに対応できるよう心がけましょう。

なお、上記「10大脅威」では、それぞれの脅威について、概要、被害事例、対策方法等を解説が示されていますので、参考にするようにしてください。

「情報セキュリティ10大脅威」組織向け脅威の順位

組織向け脅威	2025	2024	2023
ランサム攻撃による被害	1	1	1
サプライチェーンや委託先を狙った攻撃	2	2	2
システムのぜい弱性を突いた攻撃	3	7	8
内部不正による情報漏えい等	4	3	4
機密情報等を狙った標的型攻撃	5	4	3
リモートワーク等の環境や仕組みを狙った攻撃	6	9	5
地政学的リスクに起因するサイバー攻撃	7	-	-
分散型サービス妨害攻撃（DDoS攻撃）	8	-	-
ビジネスメール詐欺	9	8	7
不注意による情報漏えい等	10	6	9

出所：https://www.ipa.go.jp/security/10threats/index.html

7.2 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。それを受けて調べてみると、社員で共用で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。

不正アクセス用語集P.187の要因として、上記の例にあるようにIDやパスワードを何らかの方法で不正に入手されて、そこから内部で管理しているデータにアクセスされるケースと、システムで用いている機器のぜい弱性を攻撃して、そこから内部システムに侵入されるケースがあります。

前者のID/パスワードを窃用される場合ですが、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。

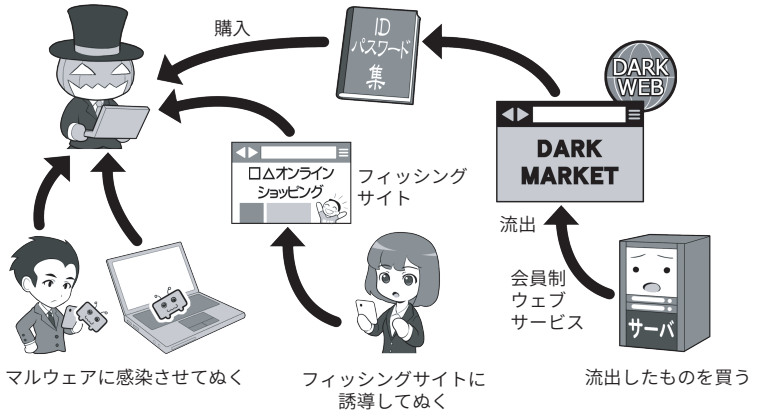
①のIDとパスワードの流出はマルウェアの感染やウェブサービスからの流出などが想定されます。マルウェアの感染などによるものを防ぐには、セキュリティ対策をきちんと講じるほか、適切なパスワード管理を行うことが求められます（第5章1(P.99)参照）。一方、ウェブサービスからの流出は、多要素認証▶用語集P.184を導入していないセキュリティ意識が低いサービスを避けるなど、消極的手段はありますが、最終的にはサービスが提供するセキュリティに依存せざるを得ず、自分でどうにかすることはできません。

②のなぜクラウドにアクセスできたかについては、この場合は個人と業務用で共用されていたパスワードの使い回し▶用語集P.186をしていたことが原因として考えられます。これを防ぐため、1つはパスワードの使い回しを絶対にしないこと（第1章3（P.32）、第6章7.7（P.158）参照）。もう1つは、自社で用いるシステムに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（第1章4（P.34）、第5章1（P.99）参照）。

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

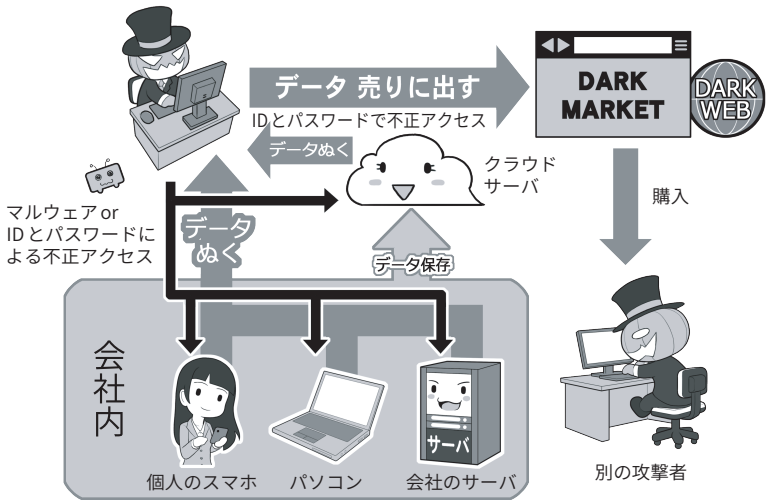
不正アクセスを行うために攻撃者は…

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。

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(本章４(P.144)参照)、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(第５章５(P.129)参照)。

システムで用いている機器等のぜい弱性を攻撃して、そこから内部システムに侵入されるケースでは、管理者が機器等のぜい弱性を放置している、あるいは対応がわからないことに乗じて、機器等を攻撃し、内部システムへ侵入します。最近は特に外部との接続に用いられる通信機器が標的にされることが多くなっています。この対策としては、機器のぜい弱性に関する情報を定期的に確認し、対応することが求められます(第１章2(P.29)、第４章3(P.94)参照)。

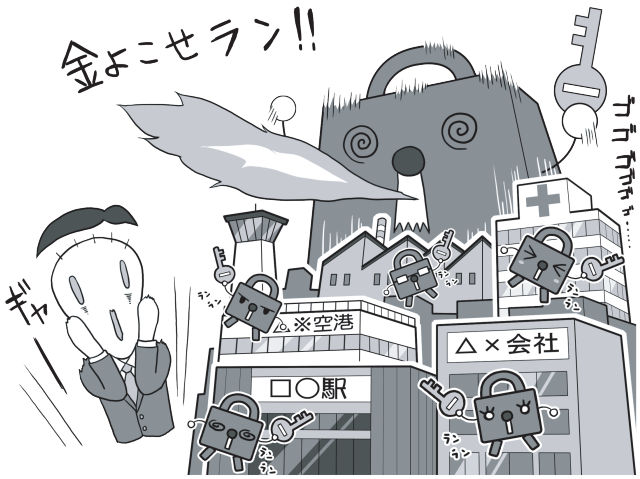
7.3 ランサムウェアの傾向

「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)と呼ばれるマルウェアの典型的な手口です(イントロダクション４ (P.18)、第２章２ (P.59) 参照)。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.182しバックアップ用語集P.186から復旧できる体制を整えることです(第１章８ (P.44) 参照)。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.187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。

7.4 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。」

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すがアウトです。この話には3つのポイントがあります。

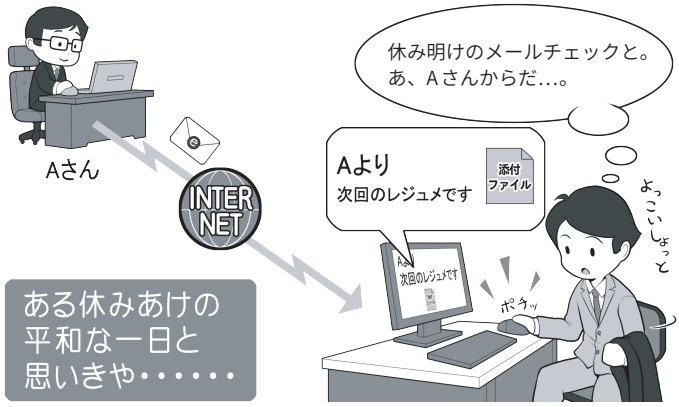
1つは、長い連休中にはセキュリティアップデートや、総合セキュリティソフトの更新が行われている可能性があります。日常的な業務を始める前に、まずアップデートして連休中に見つかったシステムのセキュリティホールや新しいマルウェアに対応できる状態にしましょう。

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.180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。

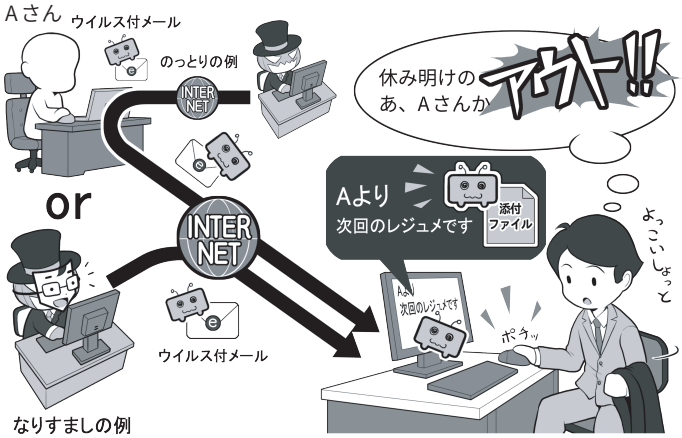
それに原則的なルールは、「メールを見ただけで完結しないものはすべて疑え」であり、「挙動が怪しい場合には、組織内にセキュリティ担当の窓口が設置されていれば、そちらに連絡する」です。それは添付ファイルでもメールの文中の外部ウェブサイトへのリンクでも同じです。

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。

7.5 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、それを騙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。

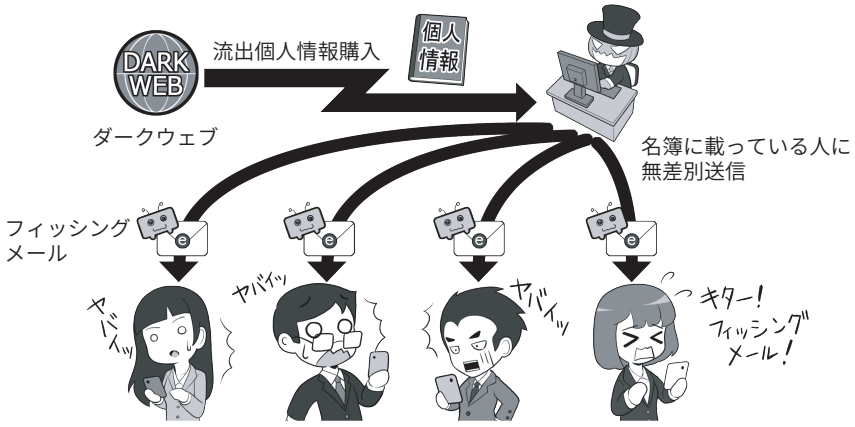
一方で、そのウェブサイトがショッピングサイト相当の暗号化(https://)▶用語集 P.177 に対応していて、一見そのショッピングサイトと同じ名前を掲示していても、実は「アルファベットに似た別の言語の文字」を使用している場合もあります。

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.178 に見えて別のウェブサイトを作ることができるのです。

すぐに対処しようと思ったら…

SMS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。

7.6 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.176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.184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。

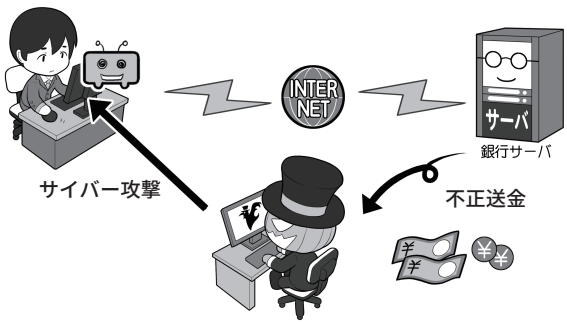
幸いにして情報の流出などと異なり、銀行の場合は過失が無いことが認められれば、銀行側が補填してくれることもあります。クレジットカードの不正利用なども同様です。

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5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。不審だ」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。

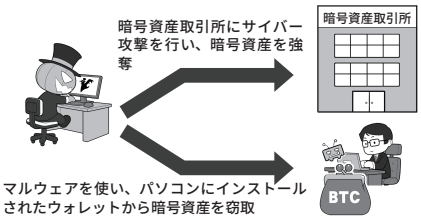
オンライン決済は常に狙われている



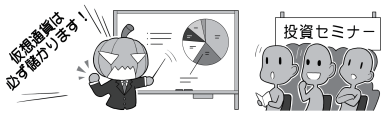
オンラインの銀行決済は常に狙われています。取引先になりすましてBECだけで誤った口座に送金させる手口や、偽サイトでIDやパスワードを奪う方法、そしてなんらかの手段で決済の中間に割り込んで振込先を自分の口座にすり替えてしまう中間者攻撃。

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



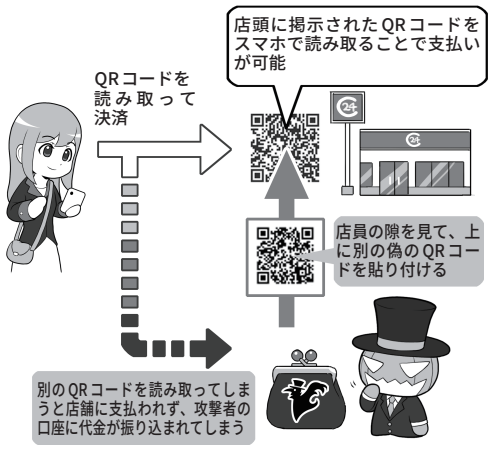
暗号資産を巡るサイバー攻撃も続発しています。実際、国内海外含め多くの暗号資産取引所がサイバー攻撃を受け、大きな金銭的被害が生じた事例がある他、暗号資産の窃取を目的としたマルウェアも登場しています。



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



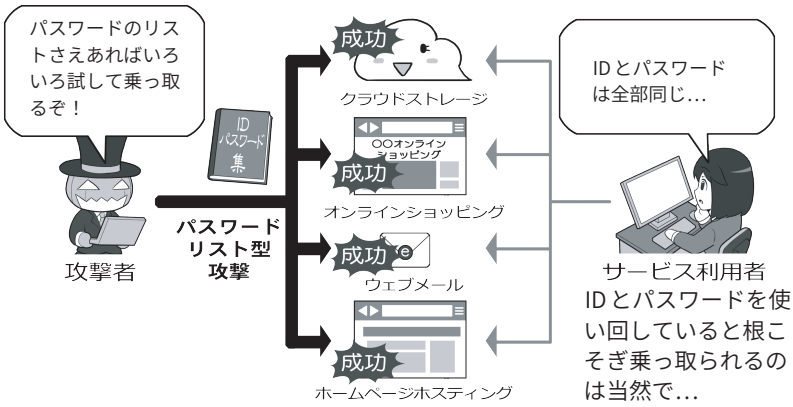
まず犯罪者が店舗に掲示されたQRコードの上に、別のQRコードを貼り付けます。利用者がそのQRコードを使って決済を行うと、代金は店主ではなく犯罪者の口座に振り込まれてしまうという流れです。

7.7 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.178などを用いて、攻撃者が不正ログイン▶用語集P.187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

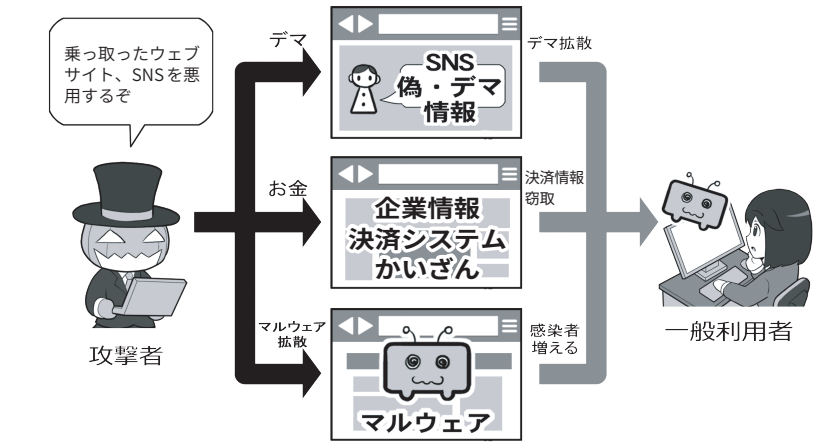


つい面倒くさがってIDとパスワードを使い回ししていると、どこか1つでも流出が起これば、同じIDとパスワードを使用しているサービスが根こそぎ乗っ取られる場合があります。また、別々のパスワードを使っていても、そのパスワードがよく使われるような簡単なものだった場合、そういったパスワードをまとめたリストが流通していて、それを使ってアカウントを乗っ取る攻撃が行われます。一部を変えただけなど、似たようなパスワードも非常に危険です。

7.8 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.188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ぜい弱性▶用語集P.183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ぜい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。

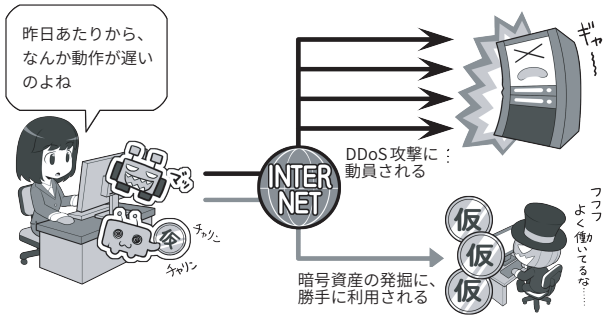
7.9 DDoS攻撃

DDoS攻撃▶用語集P.176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。最近では金融機関や交通機関などへの大規模なDDos攻撃がなされ、インフラ機能にも影響を及ぼしています。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.176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。

7.10 従業員・職員等の利用者に対する情報教育等を怠らない

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.181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いとまがありません。

「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▶用語集P.184などで販売されれば、サイバー攻撃につながります。利用者も情報資産を取扱う要素の一つである以上、そのリスク対応は重要なセキュリティ対策となります。

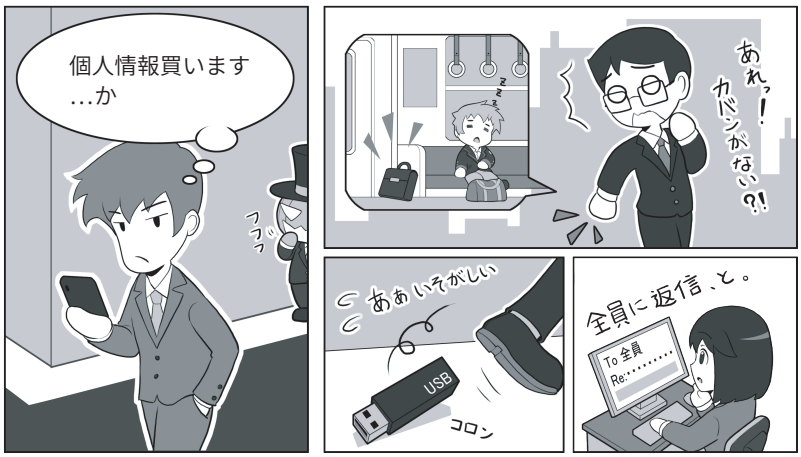
こういった内部犯行や情報流出を防ぐには、防御手段をとった上で従業員や職員等の利用者に対して情報教育をきっちり行うことです。

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、問題が起こったらどう対処するか、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、それら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ぐ、重要なセキュリティ対策として位置づけられます。

情報流出の可能性はたくさんある



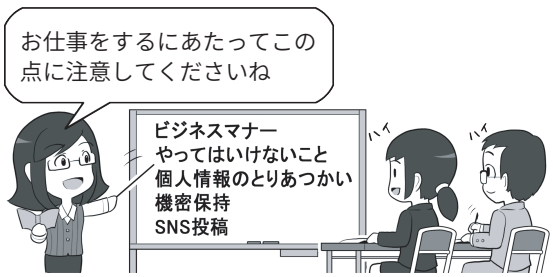
流出の可能性は情報を扱う人を狙ってそそのかすことだけではありません。機密情報を入れたパソコンをカバンごと電車やタクシーの中に置き忘れる、生徒の成績などが入ったUSBメモリを落とす、多数の人に一斉メールを送ろうとしたら、互いのメールアドレスが分からないBCC欄ではなく、見えてしまうTOやCC欄に入れて送信してしまった、などなど。パソコンやスマホ、IT機器は便利な反面、ミスを犯すときも一瞬で多量に失います。要注意です。

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。

8 個人情報は法律に則り適切に取り扱おう

個人情報の取扱いに関することは、「負のコスト」を回避するための重要な要素です。

個人情報保護法は、中小企業等含め、個人情報データベース等を業務で利用する等（「事業の用に供する」）の場合には、個人情報取扱事業者として適用され、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。

同法では、個人情報取扱事業者に対して、「その取り扱う個人データの漏えい、滅失又は毀損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない」（第23条）とし、セキュリティ対策を含む安全管理措置の実施を求めています。具体的には、「個人情報の保護に関する法律についてのガイドライン（通則編）」（個人情報保護委員会▶用語集P.182）の「10（別添）講ずべき安全管理措置の内容」に示されており、中小企業等（「中小規模事業者」）における手法の例示なども含まれているので参考にしましょう。

そのほか、個人情報取扱事業者が遵守すべき規律について、上記ガイドラインなどを参照して、確認する必要があります。なお、同法に違反した場合、当局から指導等を受ける可能性等があるほか、社会的信用を損なう可能性もあります。

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.189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 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やISMSを取得しているなど、きちんと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

などが求められます。そのうえで、契約内容が確実に履行されていることを確認するため、

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

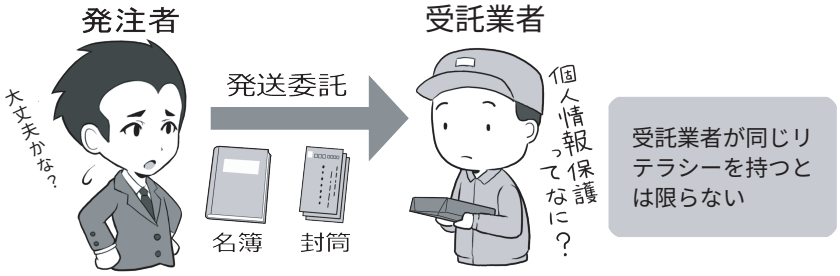
を実施することが有効です。

詳しくは個人情報保護委員会のウェブサイトなどが参考になりますが、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。

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…



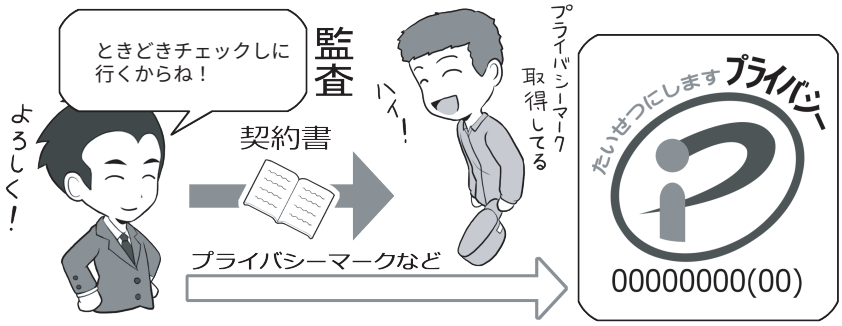
個人情報やプライバシーに関して、きちんと管理しなければならないことであるという意識は広がりつつありますが、それは自社や自団体の中だけにはなっていませんか？

その意識は取引先や委託用務先まで徹底されているでしょうか？

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) 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/EU/