インターネットの
安全・安心
ハンドブック

NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

中小組織向け 抜粋版

知る・守る・続ける
サイバーセキュリティ普及啓発

協力
警察庁 National Police Agency
総務省
経済産業省
IPA 独立行政法人 情報処理推進機構

Ver 5.00

目次

はじめに

みなさん、はじめまして。私たちは内閣サイバーセキュリティセンター(NISC) です。日本の政府機関で、国のサイバーセキュリティ政策を担当しています。突然ですが、世界中のコミュニケーションの手段と聞いたら、みなさんは何を思い浮かべるでしょうか？手紙、会話、写真、プレゼント、などいろいろなものを連想されるかもしれません。

その中でも、形は見えないけれど現代においては「インターネット」という技術が主役の1つだろう、と何となく意識されている方も多いのではないでしょうか。

インターネットによりコミュニケーションのスタイルは大きく変わりました。インターネットが普及していない昔は、どんな場所にも設置されていた公衆電話で連絡を取ることは普通でしたが、インターネットが身近になると小型化された携帯電話、いわゆるガラケーが普及しました。当時のインターネットの通信速度では、ガラケーを使って短い文章、すなわちメッセージを送る形のコミュニケーションが主流でした。

そして現代、インターネットの通信速度も安定し、大半の国民がパソコンだけでなく、スマホを所有しています。スマホは単なる電話機ではなく、「持ち歩ける小さなパソコン」と呼べるほど多機能なもので、基本的には常にインターネットに接続しています。多くの人がスマホやパソコンからチャットしたり、SNS で写真を送りあったり、映像付きのインターネット電話を使ったりして、家族や友人とのコミュニケーションを楽しんでいます。コミュニケーションの用途以外にも、調べたいことがあればブラウザでウェブサイトを検索したり、オンラインストアで買い物をしたりして、インターネットにつながったサービスに多くの人が慣れ親しんでいます。またクラウドと呼ばれるインターネット上のサーバから業務上必要なデータの保存・共有をしたり、コロナ禍で普及したテレビ会議アプリでリモート会議をしたりと、仕事で多用している人もいるでしょう。さらには社会保障や税関系など、スマホやパソコンがあればできる行政機関への申請・申告も増えています。

もはや現代において、スマホやパソコンからインターネットにつながり、民間企業・公的機関問わず、無料・有料含めて、さまざまなサービスを利用することは、家庭や職場、学校と生活のあらゆる場面で求められています。多様なサービスにつながり多くのコミュニティが形づくられ、インターネット上には1つの社会領域といえる「サイバー空間」が形成されています。

そのような便利で欠かすことのできないサイバー空間は、地域や老若

男女問わず、全国民が参画する基礎的なインフラであると呼べ、私たちが社会経済活動を営む上で重要かつ公共性の高い場として位置付けられるものです。

しかし、このサイバー空間、便利さもあれば、問題もあります。

世界中の人と距離を超えてつながるため、中には、自らの利益や自己顕示のために平気で他人の情報や財産を奪おうと悪事を働く者ともつながってしまいます。そのような悪事を働く者は、ありとあらゆる手段を用いて、スマホやパソコン、ルータなどのIT機器に対して、「マルウェア」という不正なプログラムを送りつけようとしています。インターネットにつながるということは、常にそのようなサイバー攻撃のリスクにさらされているのです。

また、SNSなどで自分の発言を広く読んでもらい自由に他の人と交流できることは、インターネットにつながることで享受できるメリットの1つですが、接する人が常に自分と友好的な意見であるとは限りません。感情的になり、誹謗中傷といえるような発言が飛び交うことも珍しくありません。しかし、SNSでの発言から、精神的に追い詰められ、自らを傷付ける行為を選んでしまう人や事例も残念ながら生じています。面と向かって言えないような他人を傷付ける発言は、インターネット上でも決して発信してはいけないのです。

サイバー空間が、人々のくらしと密接につながり基礎的なインフラとなりつつある中、国民全員が、誰一人取り残されずその恩恵を享受していくためには、国民一人ひとりが能動的にサイバー空間における攻撃や脅威の存在を知り、サイバーセキュリティに関する素養・基本的な知識を身に付けていくことが必須です。スマホやパソコンを使ってインターネットにつながるときは、みんなが常にサイバーセキュリティ対策を心掛けるべきなのです。

そのため本書では、サイバー攻撃の手口やリスク、そして被害とはどんなものがあるのかをイメージしやすくなるように、身近な具体例を取り上げながら解説しています。そして、被害を受けないようにするにはどんな対策をすればよいのか？また被害を受けてしまった場合はどんな対処をすればよいのか？についても、具体的な手順や頼れる相談窓口を紹介しています。

ほかにも、

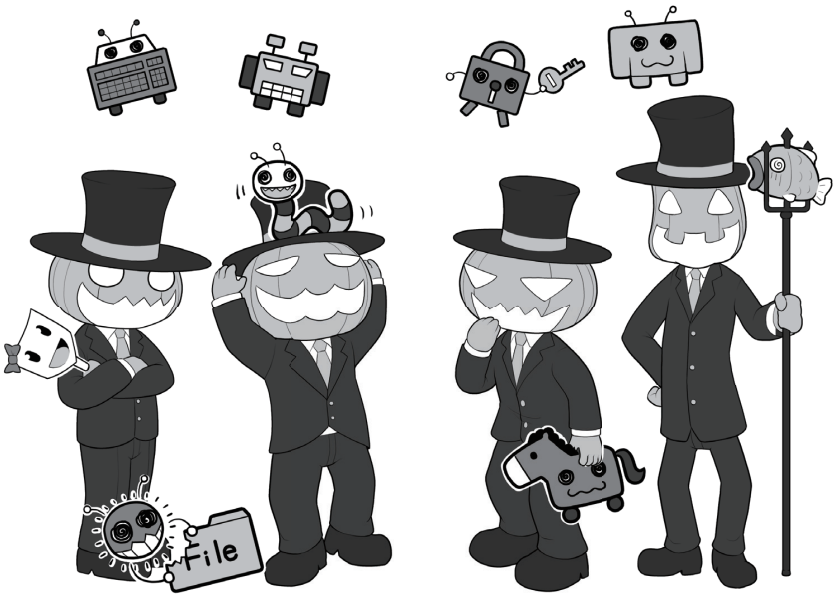
- **サイバー攻撃を防ぐための基本となるパスワードの適切な管理**
- **こどもやシニアが安全にインターネット上のサービスを利用するための方法**
- **SNSなどで多くの人と交流する際に気を付けたいマナーや法律**
- **スマホやパソコンを不安なく利用するための設定**

このイラストはインターネット上の悪意の人たちである攻撃者と、彼らが使う武器である「コンピュータウイルス（正確にはマルウェア）」をキャラクターにしたものです。

サイバー空間（インターネット）を悪意を持って利用し、自らの利益のためには他人の情報や財産を容赦なく奪い、ときにサイバー攻撃を通じて自己顕示欲を満たすといった、さまざまな悪事を働きます。

また、彼らが普通の人の仮面を被り、あるいは普通の人々が彼らの仮面を被ることもあります。

解説のイラストではそのあたりをきちんと描き分けていきますので、じっくり見てくださいね。

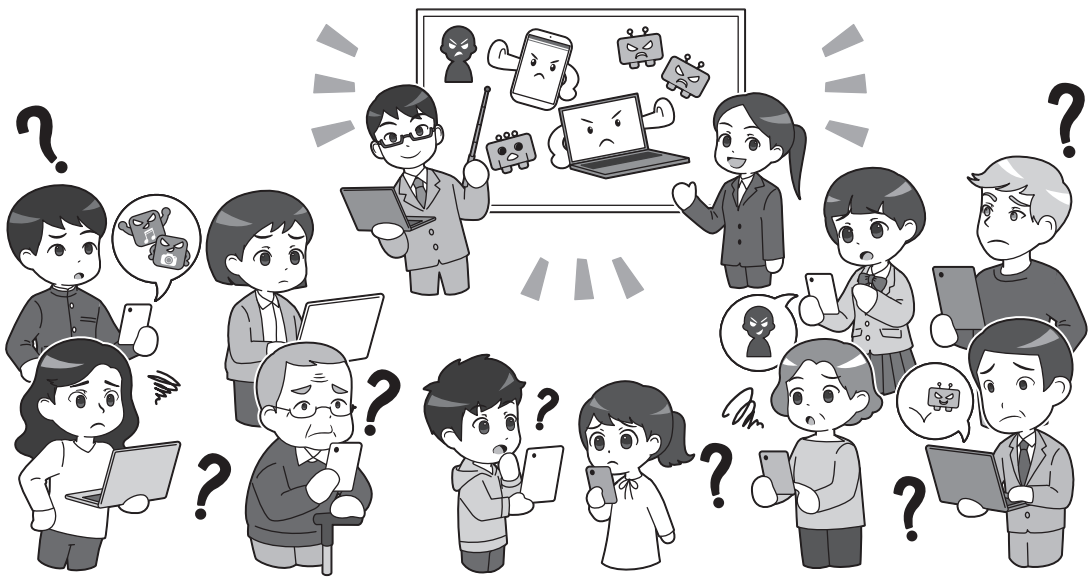


- **災害や海外など普段とは違う環境でインターネットにつながるときの事前の対策**
- **インターネットにおける通信の安全性を支える暗号化の基本**
- **中小組織のセキュリティ部門担当者に役立つ情報**

など、サイバーセキュリティ対策に必要な内容を幅広く取り上げ、いずれも読む前には専門知識を必要としない形でやさしく説明しています。本書を読んで、安全・安心なサイバー空間を一緒に作っていきましょう。

また、NISCでは、本書だけにとどまらず、「みんなで使おうサイバーセキュリティ・ポータルサイト」を運営して、サイバーセキュリティの普及啓発や人材育成に取り組んでいます。

ポータルサイトでは、こども、シニア、企業の一般社員・経営者など対象者別に適したセキュリティ施策の紹介や、セキュリティ施策におけるセミナーやイベントの実施状況などを公開しています。本書やポータルサイトをご覧いただき、国民一人ひとりのサイバーセキュリティ対策の意識を高められれば幸いです。



「みんなで使おうサイバーセキュリティ・ポータルサイト」

https://security-portal.nisc.go.jp/

※ご注意

本書では、初心者の方にサイバーセキュリティ関連の問題を理解してもらうために、実際のケースと比較してわかりやすく簡略化したり、内容を理解しやすいように関連する事項の一部を省略したりして記述している場合があります。ご了承ください。

このハンドブックを読んで、よりサイバーセキュリティに関する理解を深めていきたいと思う方は、ぜひステップアップして、さまざまな専門誌や最新の記事にチャレンジしていただけると幸いです。

なお、登場する人物、および、団体は架空のものであり、実在するいかなる人物・団体とも関係はありません。

1 最低限実施すべきサイバーセキュリティ対策を理解しよう

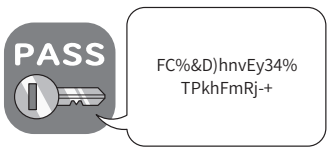
攻撃者（悪意のハッカー）による攻撃を防ぐには、まずはパソコンやスマホの基本的なセキュリティを固め、また、トラブルが発生したときの対処手段を知ることが重要です。

現在、政府系機関が掲げるサイバーセキュリティ対策の指針としては、NISC（内閣官房内閣サイバーセキュリティセンター）が「サイバーセキュリティ対策9か条」を公開しています。一般国民の誰もが最低限実施すべき対策をまとめており、本ハンドブックもこの9か条に則ってサイバーセキュリティ対策を解説していきます。

①OSやソフトウェアは常に最新の状態にしておこう

OSやソフトウェアを最新に状態にする理由は、最新の攻撃情報への対策が盛り込まれているからです。

②パスワードは長く複雑にして、他と使い回さないようにしよう



安全なパスワードの作成方法はもちろん多要素認証の重要性を説明します。

③多要素認証を利用しよう

認証用アプリや生体認証を利用したより安全性の高い多要素認証について説明します。

④偽メールや偽サイトに騙されないように用心しよう

多様化・複雑化するフィッシング詐欺メールや、公式サイト以外からアプリをインストールする危険性について解説します。

まず「**①OSやソフトウェアは常に最新の状態にしておこう**」はいわゆるアップデートのことです。 IT機器にはセキュリティホールと呼ばれる弱点が日々見つかっています。一見、大丈夫そうに見えてもそれは「ただセキュリティホールが発見されていない」だけ。OSやソフトウェアメーカーが提供している修正用アップデートを常に適用し続け、攻撃の糸口となる穴を塞ぎます。

「**②パスワードは長く複雑にして、他と使い回さないようにしよう**」は、安全性の高いパスワードを設定する際の留意点、同じパスワードの使い回しの危険性、パスワードの適切な管理方法について解説します。

「**③多要素認証を利用しよう**」は、サービスへのログインを安全に行うために、二要素以上を使って認証作業をする多要素認証について解説します。認証用アプリや生体認証を利用するとログインの安全性を高められます。

「**④偽メールや偽サイトに騙されないように用心しよう**」は、フィッシング詐欺メールが多様化しており攻撃が複雑になっていることや、公式サイト以外からアプリをインストールする危険性を解説します。

「**⑤メールの添付ファイルや本文中のリンクに注意しよう**」は、近時また猛威を振るう「Emotet」のように、マルウェア添付メールで広がる感染、標的型メールやスパムメールの実例を挙げ、具体的リスクについて解説します。

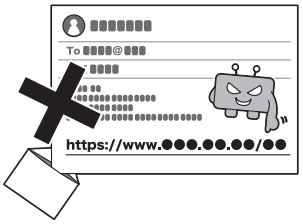
「**⑥スマホやPCの画面ロックを利用しよう**」は、スマホやパソコン(PC)の情報を守るにはまず待ち受け画面をロックすることが第一であることを解説します。また、生体認証を使用したロックの利点や、安易に他人へ端末を渡す危険性についてもふれます。

「**⑦大切な情報は失う前にバックアップ(複製)しよう**」は、普段からバックアップをとっておくことがどれほど重要か解説します。正常な状態のファイルをバックアップして保管しておくことで、仮に攻撃を許して重要なファイルを失ってしまっても、バックアップから復元することにより、被害を軽減します。とくに昨今増加しているランサムウェア攻撃に対してもバックアップを準備しておくことは有効です。

「**⑧外出先では紛失・盗難・覗き見に注意しよう**」は、勤務先や外出先でスマホやパソコンを使う際、覗き見されるショルダーハッキングなどのリスクなどについて解説します。また、飲食店などで離席時に端末を置いていく人を時折見かけますが非常に危険な行為です。公衆の場でスマホやパソコンを利用するときに注意すべきことについて把握しましょう。

「**⑨困ったときは1人で悩まず、まず相談しよう**」は、サイバー攻撃などインターネットの被害で自分だけでは対処できないときには、積極的に警察やIPAなどの窓口へ相談する重要性を解説します。あらかじめ窓口を調べておくことで、困ったときにすぐに相談できるようになります。

⑤メールの添付ファイルや本文中のリンクに注意しよう

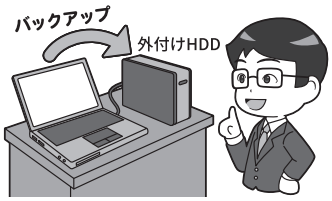


被害がなくならない「Emotet」、標的型メール、スパムメールの実例を紹介

⑥スマホやPCの画面ロックを利用しよう

スマホやパソコン（PC）の情報を守るにはまず待ち受け画面をロックすることが第一。そして生体認証が推奨

⑦大切な情報は失う前にバックアップ(複製)しよう

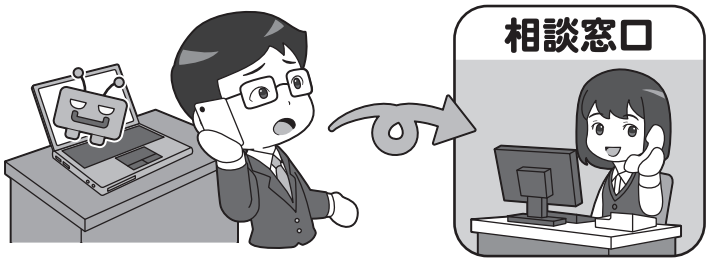


たとえ攻撃されても、適切にバックアップしておけば、すぐに復旧できます。

⑧外出先では紛失・盗難・覗き見に注意しよう

公衆の場における、ショルダーハッキングのリスク、スマホやパソコンの紛失・盗難など、利用時の注意すべきことを把握しましょう。

⑨困ったときは1人で悩まず、まず相談しよう



攻撃されたとき、どうしたらよいか分からないからとそのまま放置せず、相談窓口に相談しましょう。また、実質的な被害が出ている場合は、警察などの関係機関に報告した方がよい場合もあります。いざというとき慌てないように、あらかじめ連絡先を調べておきましょう。

*「サイバーセキュリティ対策9か条」https://www.nisc.go.jp/pdf/council/cs/jinzai/dai17/17shiryou0101.pdf

①OSやソフトウェアは常に最新の状態にしておこう

①.1 パソコン本体とセキュリティの状態を最新に保とう

悪意の攻撃からパソコンを守る第一歩は、セキュリティを最新に保ち、各種のアップデート（バージョンアップ）を行うことです。

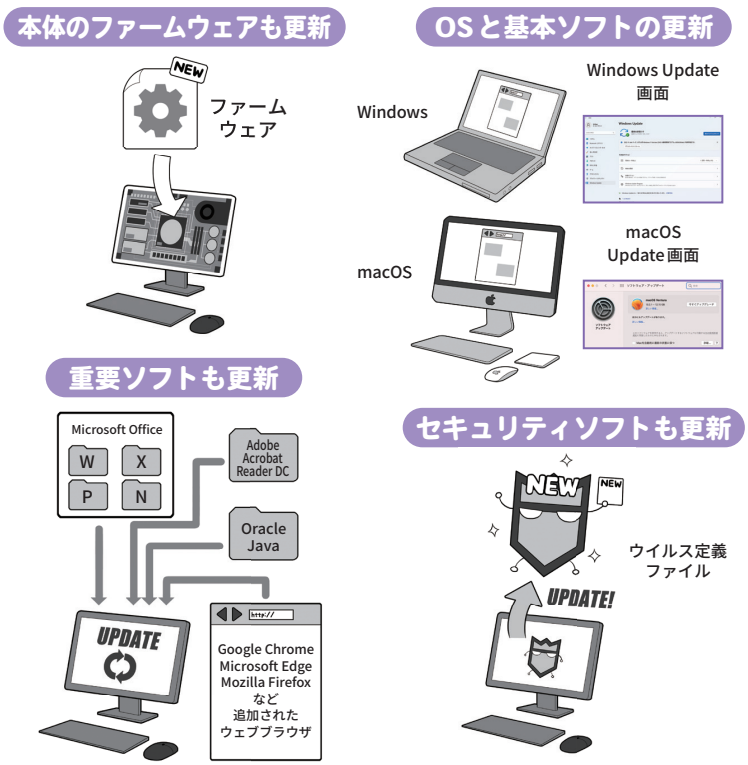
最近の機種では、OS関連のアップデート処理は自動で行われるか、アップデートを行うよう通知が出るようになっています。しかし、緊急でアップデートを行った方がよいときもあります。セキュリティ関連ニュースサイトなどでアップデートを促す情報が流れていたら、自主的に更新処理をかけるようにしましょう。Office製品などOSのメーカーが作っている重要なソフトもここで同時にアップデートします。

次に、サイバー攻撃で狙われやすいソフトウェアの更新を重点的に行いましょう。Adobe社Acrobat ReaderやOracle社Java、そしてGoogle Chromeをはじめとする各種のウェブブラウザは攻撃のターゲットになりやすいのです。

また、機器そのものの基本プログラムを更新するファームウェアアップデートにも気を配りましょう。こちらの更新通知は、自動で出る機器と出ない機器があるので、自分の機器用のアップデート情報は、どのようにすれば入手できるか、事前に確認して気を配ってください。

セキュリティソフトをインストールしている場合は、最新のウイルス定義ファイルに自動更新されるよう設定しておきましょう。

本体もOSもセキュリティソフトも重要ソフトもアップデート



OSやファームウェアなどは、社会でいえば鉄道や電気ガス水道のような社会インフラに相当し、そのためほとんどのパソコンで利用されています。

利用する側もアップデート（更新）が必要になれば速やかに適用して、攻撃者が攻撃できないようにしましょう。インストールしてあるが使っていない重要ソフトは削除（アンインストール）してしまってもよいでしょう。

ボットネットも、そもそも攻撃して乗っ取れる機器がなければ成立しないように、攻撃できる穴を作らない１人１人の行動が、安全なインターネットを作り社会インフラを支えるのです。

なお、OSやソフトウェア、ファームウェアは、開発者がアップデートの期限を設定しているものが多く、この期限を過ぎるとアップデートが提供されなくなります。

アップデートが提供されなくなったOSやソフトウェアは、セキュリティホールが見つかっても修正用アップデートが提供されず、攻撃に対して非常に脆弱なので、使用しないようにしてください。

①.2 スマホやネットワーク機器も最新に保とう

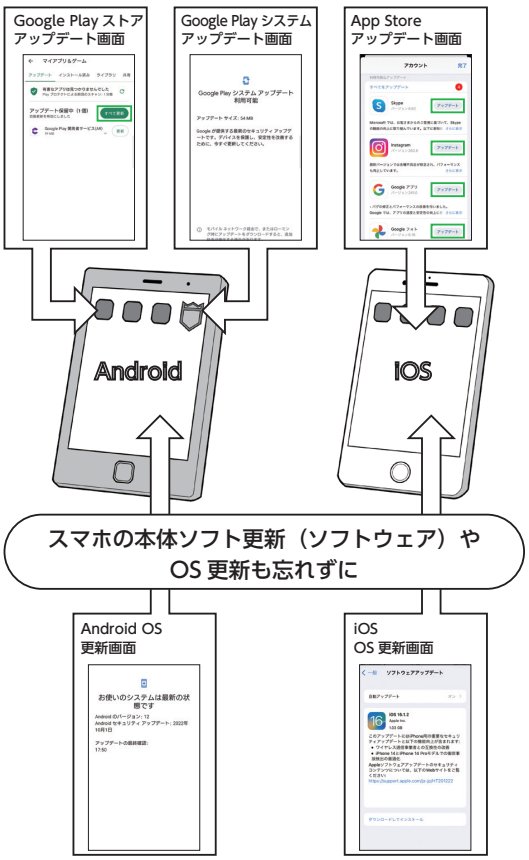
スマホも同様に各種のアップデートの適用が必須です。スマホの場合、比較的アップデートの通知がわかりやすくなっており、自動アップデート機能も充実しています。機器本体のファームウェアのアップデートでも、OSのアップデートでも、いつも使用している一般のアプリのアップデートでも、更新の通知が出たら、マメに適用するようにしましょう。そのためには、本体のファームウェア（ソフトウェア更新やシステムアップデートと書かれることも）やOSの更新が、設定メニュー上のどこにあるのかと、更新の手順を確認しておきましょう。アプリの更新が自動になっているかも確認しましょう。

スマホアプリの自動更新は、設定によっては無線LAN接続時のみ自動で行うことになっている場合もありますが、その設定でも更新時に権限変更で確認が必要な場合は自動更新されないこともあるので、気が付いたら未更新のアプリがたくさんたまったままになってしまっていることもあります。日に一度は意識してアップデート画面に行き、更新作業をするように心がけましょう。

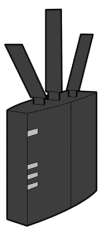
また、ネットワークにつながるルータやIoT機器、スマート家電なども脆弱性を狙った攻撃の対象となるため、ファームウェアが自動更新されるよう設定しておきましょう。2022年以降国際情勢の影響もあり、更新されていないネットワーク機器を狙う攻撃が増加しました。

ルータはここ数年で自動更新機能搭載のものが普及してきているので、可能であれば買い換えしましょう。

アプリやセキュリティソフトの更新は自動更新にしつつ、まめにチェック



ネットにつながるIT機器（ルータやIoT機器）もファームウェア更新や管理者用初期IDとパスワードの変更をしておくこと



無線LANアクセスルータ

ネットワーク対応プリンタ

ネットワークカメラ

IoT機器のファームウェアの更新は、通常はウェブブラウザで本体にアクセスして行います。このときの管理者用IDとパスワードは、必ず購入時の初期のものから変更しておきましょう。同じ機種で共通だった場合など、不正アクセスされ乗っ取られてサイバー攻撃に使われます。

②パスワードは長く複雑にして、他と使い回さないようにしよう

②.1 パスワードの安全性を高める

サイバー攻撃には、相手の機器をマルウェアに感染させて乗っ取る方法の他に、なんらかの手段でIDとパスワードを解明し、サービスや機器を乗っ取る方法もあります。

パスワードは利用しているウェブサービスなどから大量流出したものが使われる「リスト型攻撃」、文字の組み合わせをすべて試す「総当たり攻撃」、パスワードによく使われる文字列を利用する「辞書攻撃」などにより探し当てる方法や、IoT機器のパスワードを購入時のまま利用していると乗っ取られることもあります。

総当たり攻撃を防ぐには、探り当てるまでに膨大な時間がかかるようにするのが一番の防御手段で、それには1桁の文字の種類と桁数による組み合わせを増やします。例えば数字だけなら1桁10通りしかありませんが、英字を入れると36通り、英大文字小文字を入れると62通り、これに26文字の記号を入れると約88通りになります。これに桁を増やして、累乗で組み合わせを増やすわけです。総当たり攻撃は、理論上攻撃し続ければいつかは成功するのですが「時間がかかり事実上不可能な状態」にして防ぐのです。長いが覚えやすいパスワードにするか、短いが複雑なパスワードにするかは、好みの問題ともいえますが、ログイン用パスワードであれば入力ごとに遅延がかかるので、英大文字小文字＋数字＋記号混じりで10桁以上を安全圏として推奨します。しかし、より組み合わせ数を増やし安全性を高めるにこしたことはありません。

ログイン用パスワードは英大文字小文字＋数字＋記号で10桁以上

「ログインに使うパスワードは、英大文字小文字＋数字＋記号で10桁以上」の理由

「数字のみ」の10乗だと→100億通り

（英大文字小文字＋数字＋記号（88個として））の10乗だと→約2785京97兆6009億通り

数字だけで10桁と、英大文字小文字＋数字＋記号で10桁では雲泥の差がある。
そしてこれほど多量な組み合わせは、機械入力でも事実上突破不可能。

英大文字小文字＋数字＋記号混じりの組み合わせ数

アルファベット（大）＋アルファベット（小）＋数字＋記号（例）
26　＋　26　＋　10　＋26＝88

数字	英大文字	英小文字	記号	合計		5	6	7	8	9	10
10				10	数	100,000	1,000,000	10,000,000	100,000,000	1,000,000,000	10,000,000,000
10	26			36	数英	60,466,176	2,176,782,336	78,364,164,096	2,821,109,907,456	101,559,956,668,416	3,656,158,440,062,976
10	26	26		62	数英大小	916,132,832	56,800,235,584	3,521,614,606,208	218,340,105,584,896	13,537,086,546,263,552	839,299,365,868,340,224
10	26	26	26	88	数英大小記	5,277,319,168	464,404,086,784	40,867,559,636,992	3,596,345,248,055,296	316,478,381,828,866,048	27,850,097,600,940,212,224

②.2 機器やサービス間でのパスワード使い回しは「絶対に」しない

複雑なパスワードを使っても、それを複数のサービスや機器の間で使い回していれば意味がありません。1カ所から漏れればすべてログイン可能になってしまうからです。複雑なパスワードを1つ決めて、あとはおしりに数字や規則性のある文字を付けるのも、2つ以上漏れれば推測されます。それぞれに複雑なパスワードを設定し、使い回しをしないことが大切です。

同じパスワードを使い回さない。似たパスワード、法則性のあるパスワードも×

	白うさネットワーク	おさるさん銀行	三毛猫電気	たこクレジット	
×使い回し	PASSPPOI	PASSPPOI	PASSPPOI	PASSPPOI	1個漏れたら一網打尽
×おしりだけ違う	PASSPPOI1	PASSPPOI2	PASSPPOI3	PASSPPOI4	推測しやすい
×法則性あり	USAGIPPOI	OSARUPPOI	NEKOPPOI	TACOPPOI	法則性がばれたらおしまい

②.3 パスワードを適切に保管する

使い回しをせず充分な複雑さと長さを持ったパスワードは、総当たり攻撃では突破されにくくなります。しかし、適切に管理しておかず、別の方法で盗まれてしまってはひとたまりもありません。

例えばパソコンや壁に貼っていれば、誰かがそれを見て覚えてしまいますし、テキストファイルにまとめておけばマルウェアに感染したときに流出し、多くのアカウントが一気に乗っ取られるかもしれません。

パソコンでウェブブラウザにパスワードなどを覚えさせる「自動入力」機能も要注意です。あなたが席を離れた隙に、誰かがブラウザでウェブサービスを利用してしまうかもしれません。それにノートパソコンならば本体ごと盗まれることもあります。パスワードは基本的に利用する場所で保管してはいけないのです。

しかし、多くのサービスで複雑なパスワードをそれぞれ設定したら、とても覚えきることはできません。ではどうしたらよいでしょう。

1つは、パスワードを管理する紙のノートに書いてパソコンとは別に保管する方法。もう1つはスマホのパスワード管理アプリを利用する方法です。なお、後者の場合、クラウドでデータを保管する機能の利用は熟考し、過去に情報流出にまつわるトラブルのあったアプリやサービスは利用を避けるようにしましょう。それは他人の手元にIDやパスワードを保管することや、流出の危険が逆に増すことを意味するからです。

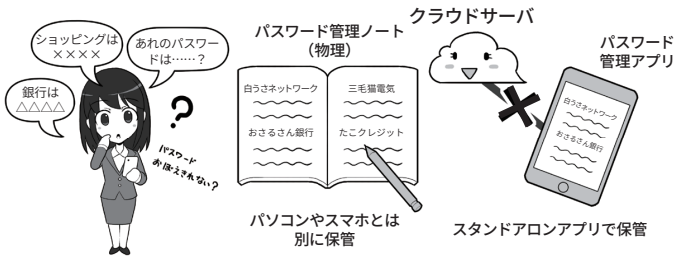
利用するところで保管するべきでないなら、スマホでパスワードを管理する場合リスクはありますが、こういったアプリは後述のPINコードや指紋認証＋暗号化で情報がガードされます。盗まれても落としても、簡単に他人が使ったりすることはできません。

ただ、管理しているパスワードは、必ずバックアップするのを忘れないようにしましょう。落としたスマホが戻るとは限りませんから。

パスワードを使用する場所に置かない。パソコンの中も×

オフィスの中ならば外の人は見ないと判断するのは×。出入りの業者が見たり、外から双眼鏡で見たりすることもできるのです。内部の人間が勝手に使うリスクもあります。

パスワードは紙のノートに書いて保管するか、パスワード管理アプリで守る



クラウド保管＝ダメというわけではなく、それは利便性との兼ね合いです。アプリのバグや過去のトラブルは、アプリ名＋「トラブル」などで検索します。

ウェブブラウザの自動入力にパスワードを覚えさせない

パスワードなどの自動入力は便利ですが、仕事場などであなたがパソコンをロックしないまま席を離れると、他人が各種サービスにログインし放題になります。

③多要素認証を利用しよう

③.1 可能な限り多要素や生体認証を使い、秘密の質問にはまじめに答えない

サービスへのログインを安全に行うために、二要素以上を使って認証作業をする多要素認証などの方法が提供されていれば必ず設定しましょう。これらの方法では通常のパスワードの他に、使い捨てにする別のパスワードを、ハードウェアトークンや生成アプリで作り、ログイン時に利用者に入力させます。メールやSMS・ショートメッセージを利用する方式もありますが、これらは安全面で非推奨です。

その他にも、USBセキュリティキーなどで利用者を確認する方法や、不正アクセスの兆候を知る手段として、サービスに不審なログインがあったときにメールで利用者に通知を送る機能も存在するので、あれば活用しましょう。

また、最近の機器では顔、虹彩、指紋で本人確認をして機器のロック状態を解く、生体認証機能もあります。

生体認証は本人のみが使えて安全性が高く、肩越しの盗み見などよる暗証番号（PINコード）の盗難には強い機能でもあります。ただ指紋認証などは寝ている間に勝手にロック解除されることがあり得るので過信は禁物です。

なお、生体認証はたいていは通常のPINコードの替わりなので、スマホでは失敗すると通常のPINコード入力に戻ります。誕生日などの個人情報をPINコードにすると予想がされやすく、本体を盗まれてロック解除される可能性が上がるため使わないようにしましょう。

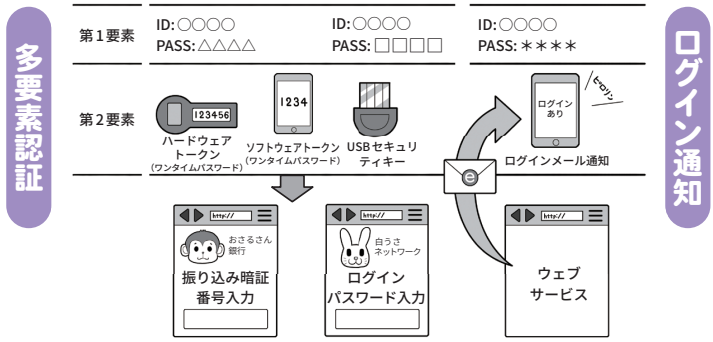
その他、認証システムによっては、スマホなどへのプッシュ通知を多要素認証に組み入れることがあります。攻撃者がパスワードなどでの認証を成功させた場合にもプッシュ通知が送られるので見知らぬプッシュ通知には回答してはいけません。

その他のウェブサービスの中には、パスワードを忘れてしまった場合や、あるいはいつもと違うログインがあった場合の本人確認のために「秘密の質問」と呼ばれる機能で対応しようとするものがあります。これはあらかじめ利用者が、自分しか知らない質問と答えを設定しておいて、合い言葉的にこれに答え、本人であることを証明するものです。

しかしこの秘密の質問は、自分で質問を作れるものもありますが、多くは「生まれた市は」「ペットの犬の名前は」と回答が類推しやすいものが大半です。

SNSが普及した今、ネット上で簡単に見つけられることもあり、安全性が高いとはいえません。秘密の質問に答えを設定する場合は推測できないものにし、忘れないようにパスワード管理アプリなどに保存しましょう。

多要素認証やログイン通知でセキュリティを向上



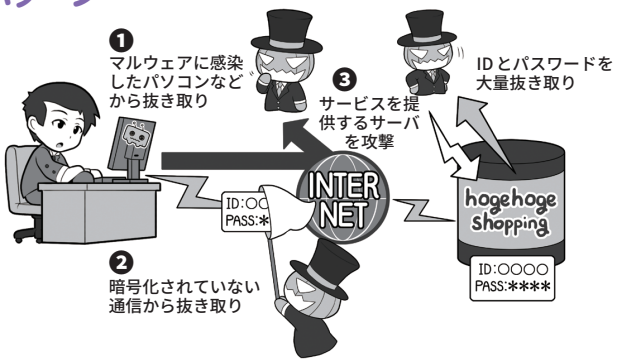
生体認証を使う

③.2 パスワードはどうやって漏れるの？どう使われるの？

さまざまなIDとパスワードの漏えいパターン

攻撃者にIDとパスワードが漏えいする事態は、機器がマルウェアに感染したり、自分が通信する過程で抜き取られたりする他に、利用しているサービス側からも流出するケースもあります。

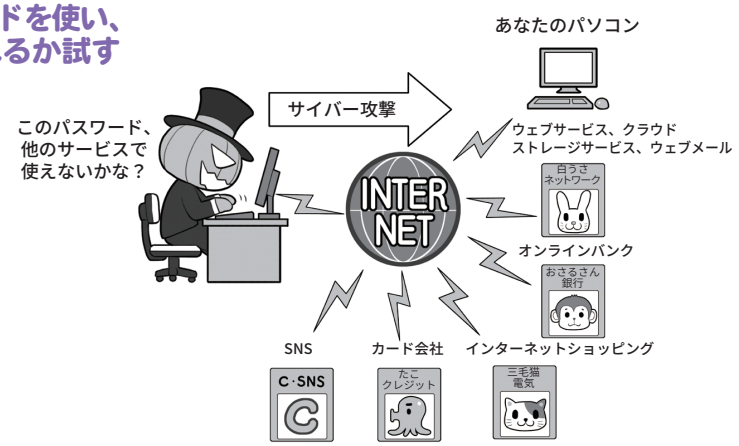
ニュースや通知でサービス側から流出が判明した場合は、速やかにパスワードを変更するなどの対応を取りましょう。



攻撃者は入手したIDとパスワードを使い、さまざまなサービスを乗っ取れるか試す

IDとパスワードをなんらかの手段で手に入れた攻撃者は、これをどこか別のサービスで使えないかさまざまな方法で試します。

こういった攻撃を成功させないために、パスワードの使い回しや、似たパスワード、パターンのあるパスワード、個人情報などから推測できるパスワードを利用するのはやめましょう。



私たちがパソコンやスマホ、あるいはSNSやウェブ上のサービスを利用するときに入力するIDやパスワード。サイバー攻撃でこれらの情報を盗まれると、かなり深刻な被害を起こしかねないものです。

では実際はどのように漏れてしまうのでしょう？

1つには、自分のパソコンなどがマルウェアに感染し、そのマルウェアがパスワードを盗み取って攻撃者に送信するケース。次に、ウェブサービスなどにログインするときに、私たちが利用する機器からウェブサービスまでの経路上のどこかで盗み取られてしまうケース。そして、ウェブサービス側でログインを認証するために控えとして持っているIDやパスワードが、攻撃者によって盗み取られ漏えいするケースなどがあります。

先ほど説明しましたが覚えておいてほしいのは、自分がマルウェアなどに感染していなくても、漏れてしまうケースがあるということです。したがってIDやパスワードを普段入力していないから安心、とも言い切れません。

そしてIDとパスワードを盗み取った攻撃者は、それを使ってどこか別のウェブサービスなどが乗っ取れないか、さまざまな場所で試します。

あなたが複数のウェブサービスの間でIDとパスワードを使い回していたり、あるいは似た形のパスワードを使ったりしていると、これらのサービスのアカウントを一気に乗っ取られます。

乗っ取られると、あとはオンラインショッピングで勝手にものを買われてしまったり、現金は送れなくてもなんらかの送金システムが利用できる場合は、それを使ってお金を奪い取られたりされてしまうわけです。

もしパスワード流出が判明したら、まずはすぐにパスワードを変更しましょう。

④偽メールや偽サイトに騙されないように用心しよう

④.1 多様化する偽メールに注意しよう

サイバー攻撃を行う際に、攻撃者は偽メール、偽サイトを使うことが多いです。これは、攻撃者からしたら攻撃のためのコストを低く抑えられるためです。

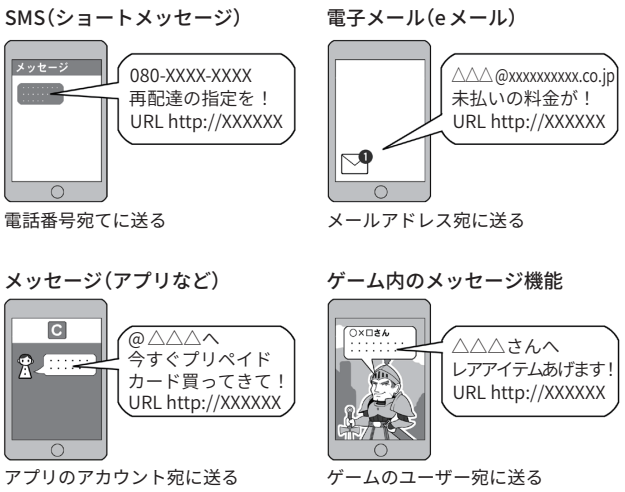
偽メールには、スマホ宛の偽SMSやSNSで使用可能なメッセージ機能なども含みます。

近年、フィッシング詐欺の攻撃で最も目を引いたのは、宅配業者の不在通知詐欺です。宅配業者を名乗って「配達に行ったが不在だった。下記のリンクから確認して欲しい」というようなSMS(ショートメッセージ)を送り付けて、利用者をリンク先の偽サイトに誘導し、そこでIDとパスワードなどを詐取するというものです。

実は、この業者は「SMSで不在通知を行なわない」のですが、それを知らない人たちはまんまとだまされてしまったわけです。関係機関で日々、「不審なメールに気を付けてください」というアナウンスをしているのですが、SMSとメールは違うものと思われてしまったのかもしれません。

偽メールについても、国税庁を装ったりETCサービスを装ったりと、騙られる送信元にバリエーションが増えてきていますが、偽メールであることには間違いありません。またこういったメッセージを使った詐欺には、SMSやメールだけでなく、SNSのメッセージ機能、あるいはゲーム内のメッセージ機能を使った攻撃も実際に発生していますので、偽メールと同様に注意してください。心当たりのないものは無視し、心当たりがあるものでも、そのメールやメッ

フィッシング詐欺はいろんな方法がある



「怪しいメール」といわれたら「メール」だけでなく似たような機能全般に気を付けましょう。

驚くと人間は警戒心を忘れる

災害時などに驚いて人間の警戒心が弱くなった瞬間を狙った攻撃もあります。注意しましょう。

フィッシング対策協議会 https://www.antiphishing.jp/
内閣サイバーセキュリティセンター Twitter @nisc_forecast

セージのURLなどにアクセスするのではなく、後述するような対処を行ってください。

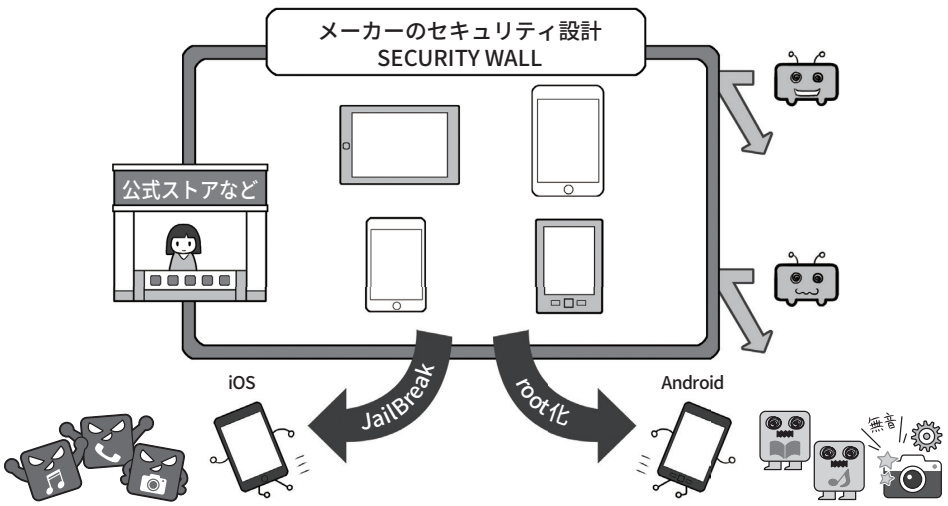
他にも、地震が発生したときに、気象庁を名乗って津波に関する迷惑メールが送られた例もありました。いずれも私たちが「だまされないぞ」と身構えているのとは違う方向や、災害時で正常な判断が行えない状況を狙っています。

こういった詐欺メールは年々手口が巧妙になっており、送信元アドレスやメッセージ中のリンクを確認しただけで、詐欺と見抜くことは極めて難しくなっています。基本は「見るだけで完結しない情報はすべて疑え」です。情報を確認する場合は、正規のウェブサイトのURLを直接入力して見るか正規のアプリから行いましょう。

また、日々巧妙になる手口を少しでも知るにはフィッシング対策協議会（https://www.antiphishing.jp/）のウェブサイトや内閣サイバーセキュリティセンターのTwitter（@nisc_forecast）をフォローするとよいでしょう。最新の事例をすぐに確認できます。

④.2 公式サイト以外からアプリをインストールすることは控えよう

サイドローディングやスマホの改造は控えましょう



スマホのセキュリティはメーカーが想定する利用方法を守っていることが前提条件です。非公式なアプリをインストールする「サイドローディング」は危険が伴う可能性がありますし、「root化」や「JailBreak」といった改造は規約違反である場合もあります。いずれもセキュリティ上、脆弱になるので非常に危険で、やってはいけません。

前項で紹介した偽メール、偽サイトの手法は多様化していて注意が必要ですが、スマホにインストールするアプリも同様に注意しなくてはいけません。

インストールしようとするアプリがどのような動作を行うものかをあらかじめ確認できればよいのですが、個人で、アプリの中身を分析し、不審な動作などがされないことを確認することは簡単なことではありません。そのような確認作業を自分ではなく信頼できる第三者がしてくれれば少し安心できます。

公式ストアで配信されるアプリに関しては、公式ストアでの配信前にストア運営者が審査しているので一定程度のリスクは軽減されます。

公式のアプリストア以外のサイトからアプリをダウンロードすることを「サイドローディング」、さらに非公式なアプリのインストール以外にもスマホを標準にはない設定に変更できる改造を「root化」「JailBreak」と呼びますが、これらはセキュリティレベルを下げるためやってはいけません。

サイドローディングは、アプリをさまざまなサイトからインストールできることで企業間の競争が促進される可能性があるかもしれません。しかし、アプリの審査を行うためには、費用や時間・労力が必要ですので、何もチェックを行わず自由に公開を許すようなサイトよりは、運営費用がかかるのは当然で、そのようなコストが価格に反映される点も考慮する必要があります。またスマホの改造は規約違反になる場合もあり、セキュリティ上、脆弱になるので非常に危険です。

スマホには、個人に関する重要な情報がたくさん存在していますから、リスクの高いアプリをインストールし、重要な情報が漏えいしてしまうと、取り返しがつきません。アプリを利用する際には、安全を確保するためには一定の費用が必要なことと、アプリの審査を行っている信頼できるストアを使うという観点が不可欠です。

例えばスマホの場合、iOS 機器は公式のストア以外からはアプリを導入できない仕組みになっていますが、Android 機器の場合は公式ストアやベンダー・メーカーのストア以外からもアプリをインストール可能です。それを利用し攻撃者がメールやSMS などであなたを誘導して、公式ストアでない場所から不明なアプリをインストールさせ、端末を乗っ取ったり、端末内の情報を盗んだりする可能性があります。

Android 機器の場合、使用しているアプリで別のアプリをインストールする設定が最初からオフになっております。不明なアプリをインストールしないためにもこの設定はオフのままにしておくようにしましょう。

また、Android 機器でも iOS でも、アプリのインストール時や初回起動時に、同意を求められる「権限」には充分注意してください。

権限とはインストールするアプリに対して、スマホのどの機能の利用を許可するか、という確認です。

単なるカメラアプリなのに住所録にアクセスするものや、撮影する必要がないのにカメラにアクセスするもの、著しく多くの項目にアクセスしようとするものなどは要注意の例です。項目別に許可を却下するか、そうできない場合、そのアプリは導入しないようにしましょう。また、最初は無害に見えて、導入後のアップデートで権限の増加の許可を求めるものも、その変更項目に注意してください。

その他、有用なアプリの開発者から、攻撃者が当該アプリを買い上げて、後からアプリをマルウェア化してしまう攻撃もあります。

このような場合は、ニュースサイトでそのような事案が紹介されることも多いので、情報収集時に気にかけておくとよいでしょう。

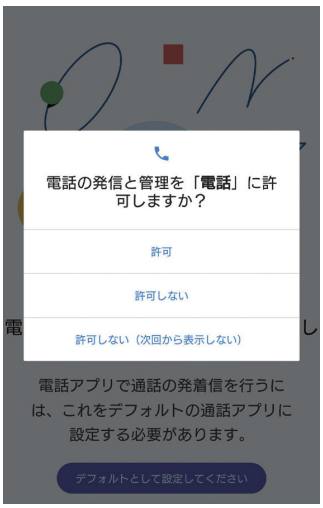
その他、アプリ間での機能連携やウェブサービス間で連携して、間接的に権限を奪取するものもあるので「連携」という言葉にも充分注意してください。

「不明のアプリ」という言葉に注意

・Android

項目や文言は、使用する Android のバージョンやスマホメーカーによって異なりますが、アプリのインストール時に「不明なアプリ」と表示されたり、最初からオフに設定されている「不明なアプリ」に関する項目を変更させようとするものは、すべてセキュリティ上危険なものと判断するようにし、最初からオフの設定のままにしておくようにしましょう。アプリは、基本的に公式ストアからのみインストールするようにして、その他の場所からは避けましょう。

導入時や起動時の権限付与に注意



・Android、iOS（画面は Android）

アプリのインストール時や、起動時にさりげなく表示されるため、多くの人が無意識に「承認」や「同意」してしまっていますが、これは、「アプリがスマホのこれらの情報に自由にアクセスできる許可」を求めている画面です。

個別に却下することができない場合もあるので、その際は導入しないようにしましょう。そして、そもそも不必要な権限を求めるアプリは怪しいと警戒しましょう。

⑤メールの添付ファイルや本文中のリンクに注意しよう

標的型メールとスパムメールの例

標的型メールの例

スパムメールの例 SMS(ショートメッセージ)を使った例

前節で述べた「偽メール」と類似しますが、添付ファイルやリンクは、標的型攻撃でもよく使われますし、今でもときどき復活しては、猛威を振るう「Emotet」も、マルウェアを添付したメールを受信者が開き、添付ファイルを実行することで感染が成立します。

心当たりのない送信元からのメールに添付されているファイルやリンクは、基本信用ならないものとして、むやみやたらに開かないようにするとともに、機器の設定などを堅牢に保ち、感染の隙を作らないようにしましょう。

スパムメールでの攻撃は、引っかかる率が少なくとも、その攻撃の母数を大きく取ることで攻撃者にとっての利益回収のパフォーマンスを上げています。

例えば、「フィッシングメールの例」の画面は、実際にSMSに送り付けられた、銀行を名乗るフィッシングメールを模したものです。

送信元とされる金融機関の口座を持っていない人であれば、フィッシング(＝詐欺)メールだと気付くことができるかもしれませんが、現在もこういった攻撃に引っかかる人が一定の割合でいます。その先が詐欺サイトではなく、ゼロデイ攻撃のマルウェアが埋め込まれたウェブサイトならば、開いただけで感染してしまうでしょう。

また、もっとやっかいなのが、攻撃者ではなく、善意でマルウェアを拡散させてしまう人々です。友人から「このアプリ面白いよ！」と薦められたら、多くの人はあまり不審に思わないでしょう。

しかし、友人は知らなくても、実はこのアプリがマルウェア入りだったり、あるいは拡散する間は無害でも、後に権限を拡大して個人情報を抜き取るかもしれません。

これが、他人の発信ならば警戒できますが、親しい友達や家族だった場合、警戒するでしょうか？

対抗策としては、こういったお薦め系のものは1つの線引きを持って接するようにしましょう。メールの文面など、目の前に見ている情報で完結しないものは一律に警戒するのです。動画が面白いとかお金が儲かる方法があるとかだけでなく、リンクでジャンプするとか、添付ファイルを開かせるものは一律に避ける。

それは、現実世界で「ちょっと向こうまで付き合ってよ」とか「ちょっとこの車に乗ってよ」といって連れて行かれるのに等しいと思いましょう。

さらに、「リンクでジャンプしないけど検索エンジンで調べて見る分にはいいよね」、と思っても、攻撃者はそうやって検索エンジンからやってくる人向けに、二段構えでマルウェアを仕込んだウェブサイトを用意していることもある、と覚えておいてください。

⑥スマホやPCの画面ロックを利用しよう

⑥.1 スマホやパソコンには必ず画面ロックをかけよう

スマホやパソコン(PC)の情報を守る第一歩は、待ち受け画面にロックをかけることです。

ロックには「PINコード*」によるロック、パターンロック、指紋や顔など生体情報を用いた認証によるロックなどがあります。ロック機能は「誰かにスマホを持ち去られるなど、手元からスマホが離れたとき」に情報を確実に守るためのしくみの1つです。

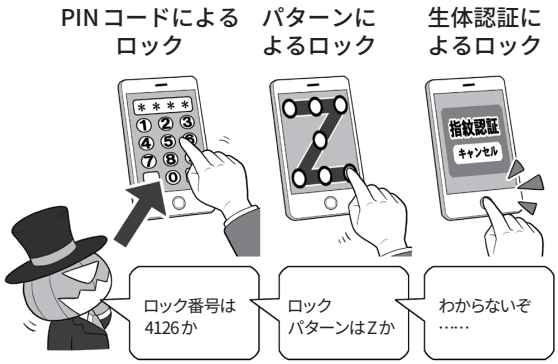
とくに生体認証は周りから覗かれPINコードを盗まれる危険性の排除をしつつ、入力の面倒くささを省くので便利な機能です。

指紋認証や顔認証が代表的ですが、その他にも、スマートウォッチなど特定のウェアラブル機器を着けたり、GPSに連動して自宅など特定の場所にいたりすることで自動的にロックを解除できるものもあります。

ただし、気を付けておきたいのは、セキュリティ向上のためのロック機能を設定しても、そのパソコンやスマホをロック解除したまま置いてその場所を離れたり、ロックを解除して他人に見せたり貸したりすれば、一瞬で情報を盗み、乗っ取ることが可能です。画面ロックは、情報を保護するための強力なツールですが、ロック解除するための認証方法が脆弱だと意味がなくなります。ロックがかかっているから安心とそれだけに頼り切りにならず、ロックを解除するための機能や、スマホやパソコンの管理にも留意しましょう。

スマホやパソコンは自分のすべての情報が詰まった持ち歩く金庫だと思って、必ず肌身離さず自分のそばに置き、使わないときはこまめにロックをかけた状態にすることが重要です。

スマホやパソコンにはロックをかけよう



席において離れたり、人に貸したりしないようにしよう

スマホを席に置いたままでは、本体も情報も盗まれるおそれがあります（とくにロックを設定しなかったり、ロック解除したままの状態で放置）。

スマホを貸すと、プライバシーを覗かれたり、一瞬でスパイアプリのようなものをインストールされたりすることがあります。むやみに渡してはいけません。

⑥.2 よくある情報の漏れ方と対策

SNS用のアプリなどでは、本体のPINコードなどとは別に、アプリ専用のPINコードが設定できるものもあります。盗難などの際、SNSの内容を見られたくなければ、このアプリPINコードも設定しましょう。情報の守りが二重になります。一部の機種では生体認証をアプリのロック解除に利用できるものもあるので、セキュリティを向上させても快適な利用の妨げにはなりません。

一方、攻撃する側から見ると、スマホのロックをなんらかの方法でパスできたとしても、また、別の関門が待ち構えているわけで、手間をかけさせ侵入を諦めさせるというセオリーに沿っているわけです。

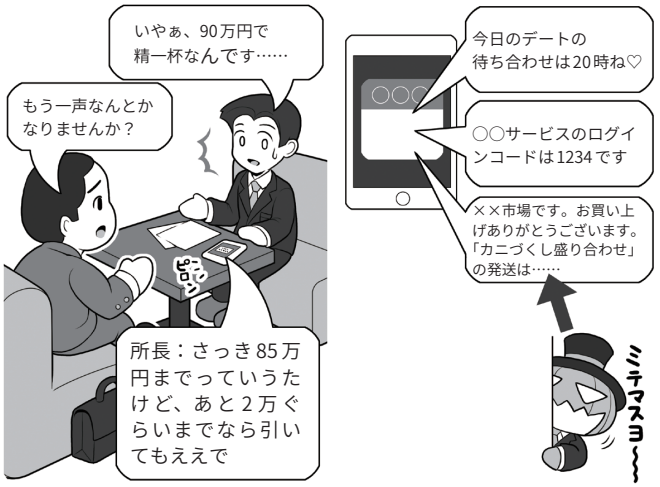
なお、アプリのPINコードを使う場合は、スマホロック解除のPINコードと異なるものを設定しましょう。PINコードの使い回しはセキュリティがないのと一緒になってしまいます。PINコードもそれぞれ異なってこそ意味があるのです。

スマホをロックしていても情報漏れが発生することもあります。

例えば自分だけで使っているときは便利なメールの通知機能。ロック画面にメールの内容を表示していると、誰かと会話中や商談中に、うっかり内部情報を見られてしまったり、あるいは差出人が分かるだけで、状況によっては知られると問題のある情報を提供してしまうことになりかねません。

また、同様にロック画面にメールの内容を表示していると、せっかくセキュリティ向上のために設定した多要素認証のパスワードメールも見られてしまうことがあり得ます。そうするとスマホやメールアドレスの正当な持ち主であることを確認する役割を果たせず、画面を除き見ただけの第三者によって認証が突破できてしまいます。

待ち受け画面に表示する通知はよく検討する



ロック画面だけでなく、普段使用している画面に通知ウインドウとして表示される場合でも、同じく情報を見られてしまう原因になります。スマホを使って説明しているときに、不適切なメールの内容が表示されることも……。情報漏えいには気を付けましょう。

アプリごとにPINコードをかけられる場合はかける

本体のロックを解除されても、SNSのアプリに別のPINコードがあれば、流出の危険性は低くなります。それでも、自分が席を離れるときにスマホを残してはいけません。なお、勝手に他人のスマホのロック解除をすることは、れっきとしたサイバー攻撃です。

⑦大切な情報は失う前にバックアップ(複製)しよう

⑦.1 何をするにもバックアップを取ろう

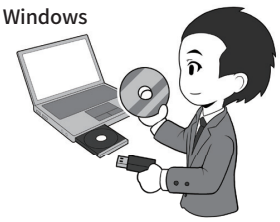
各種のサイバー攻撃や、パソコン・スマホの故障などからいち早く復旧して事業を継続するには、システムやデータのバックアップが不可欠です。とくに近年は感染するとファイルを暗号化して身代金を要求するランサムウェアの流行により、バックアップの重要性が格段に上がっています。バックアップの方法は主にパソコンやスマホのOSの種類により異なっています。パソコンの場合には、macOS搭載の機器のように、外付けの補助記憶装置(ハードディスクやSSD。以降記憶装置)を接続するだけでバックアップが行え、復旧もシステムとデータすべてをほぼ全自動で行えるものもあります。これに対してWindows搭載機器では、基本的にはデータをバックアップする考え方で、システムの復旧とデータの復元は、別に行うようになっています。

スマホの場合も機種ベンダーによる差もありますがほぼ同様です。

iOS搭載機器はパソコン上に専用の同期ソフトを導入して全体をバックアップします。この機能は機器を紛失した場合にも、新しい機器を接続すると全自動で復元が行えます。

Androidに関しては標準ではパソコンに全体をバックアップする機能はないので、Windowsに似た、データのみをバックアップする形で行います。なお、バックアップを取得するだけではなく、できれば取得したバックアップを用いてちゃんとシステムの復元を行えるか確認してください。

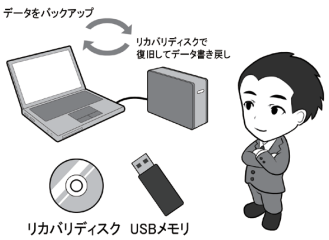
macOS機器、Windows機器のバックアップと復元



mac OS機器はまるごとバックアップ、まるごと復元の性格が強く、Windowsは基本的にはOSを復元後、別途データを書き戻すイメージと考えるとよいでしょう。

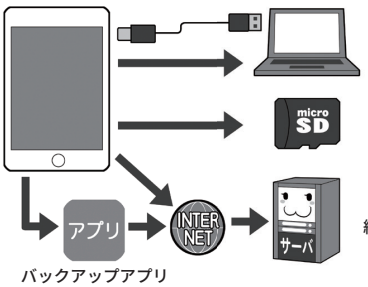
実際は他にも専用のソフトウェアを導入したり、細かい設定を変えることで、バックアップの方法を変える手段はあります。

ですから基本的なそれぞれのOSの立ち位置や性格と考えて下さい。善し悪しや優劣はありません。



スマホもバックアップは定期的に取ろう

バックアップの方法はいろいろ



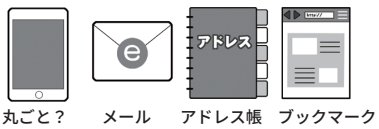
パソコンにつないで丸ごとバックアップ

内蔵できるmicroSD

メモリカードにバックアップ

直接あるいはアプリ経由でクラウドサーバにバックアップ

なにがバックアップできるか確かめる



なにがバックアップできるのか確かめて、機種やバックアップ方法を選択します。また、取得したバックアップを用いてシステムがちゃんと復元できるか確認してください。

⑦.2 ランサムウェアや天災にも対応できるバックアップ体制

ランサムウェアなどの、データを破壊することが多いマルウェアの対策にはバックアップが有効ですが、では実際にどう運用するのでしょう。

ランサムウェアはパソコンなどが感染すると、そのパソコンに繋がっている記憶装置すべてを暗号化してしまいます。仮にバックアップしていても、常時接続したままにしていると、その外付け記憶装置まで巻き添えで暗号化されることもあります。

そのため、バックアップ自体はマメにしておくべきですが、常時接続はしておかないという、かなり難しい運用が求められます。

また、最近は大雨による水害で、事務所にあったパソコンと外付け記憶装置が両方とも水没して復旧が困難になるという話もありました。これに対応する手段としては、バックアップの「3-2-1ルール」というものがあります。バックアップは本体を含め3個以上、2種類以上の媒体、そして1個は遠隔地に置くというものです。

遠隔地とは、現実的には「クラウドサーバ」などの利用を意味します。会社に同時に災害に遭わなそうな支社などがある場合は、そこにバックアップをおいてもよいでしょう。クラウドサーバは最近では手頃になりましたが、それでも本体の全データをバックアップできる容量は高価です。したがって、事業継続に必要な重要なデータを選別してバックアップすることになるでしょう。

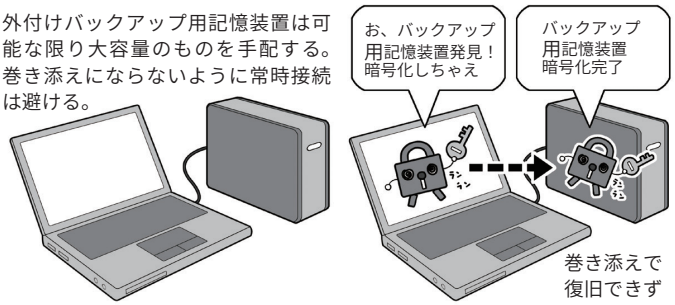
なお、最近のクラウドでのバックアップはランサムウェアの巻き添えになりにくい規格のものもあるので、利用にあたっては調べてみましょう。

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内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。バックアップはまめにしておきましょう。

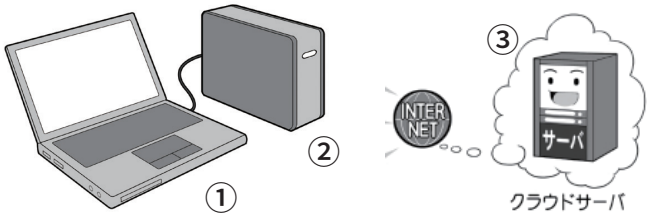
バックアップの体制を整える

外付けバックアップ用記憶装置は可能な限り大容量のものを手配する。巻き添えにならないように常時接続は避ける。



環境を整えたらバックアップを開始します。なにかソフトの導入や、環境を変更したらバックアップします。システムのアップデート後もバックアップします。ただし、バックアップ用記憶装置を常に接続しておくとランサムウェア感染で巻き添えになって、復旧に使うためのデータも失われてしまいます。

バックアップは3個以上、2種媒体以上、1個は遠い場所



本体＋バックアップ用記憶装置＋クラウドサーバで条件を満たします。クラウドサーバは多要素認証などで、攻撃者に乗っ取られないようにしましょう。

⑧外出先では紛失・盗難・覗き見に注意しよう

勤務先や外出先でスマホやパソコンを使う際に、誰かにスマホやパソコンを覗き見られている、そう感じたことはありませんか？

友人知人と冗談の範囲で「何やってるの～？」と1回2回茶化すくらいならまだしもあまりに覗き見の頻度が高かったり、あるいは見知らぬ人に何も言わずにずっと横や後ろから覗き見られてたりしているようならば要注意です。

見られている内容が機密情報であったり、秘匿したい個人情報であったりする場合には、あなたの情報が漏れる心配があります。

「見られても大したことない情報しか自分のスマホやパソコンには保存してないよ」と心配しない人も多いかもしれませんが、覗き見している人はあなたの情報もさることながら、あなたがやりとりしている相手がターゲットかもしれません。

「ロックをかけてあるから大丈夫」と思っても、ロックを解除する方法がすでに相手の手に渡っている懸念もあります。例えば、相手に直接接触せず情報を入手する方法として、電車で座席に座っている人のスマホ操作を見てPINコードやパターンロック形状を盗む「ショルダーハッキング」、カフェなどのテーブルに放置されているスマホの画面に残る指の脂跡からパターンロックを見破る方法などがあります。飲食店などで席の確保にスマホなどを置き去りにする行為を時折見かけますが、紛失・盗難・覗き見、いずれの被害に遭ってもおかしくない非常に危険な行為です。ついやってしまう、という人はすぐにやめてください。

外出時は自分のスマホやパソコンが他人から見られる可能性は高い

外出時は、使用しているスマホやパソコンを他人から覗き見されないよう注意が必要です。また、うっかり紛失して盗難されれば、大事な情報が盗まれるリスクは大きく高まるので、よく注意しましょう。

スマホ使用時によく狙われるソーシャルエンジニアリング

ショルダーハッキング

公共の場でロック解除をするときは、背後などから見られていないか気を付けましょう。

画面についた脂の跡を見る

スマホを席に残しておいたり、席取りのためにテーブルに置いて離れたりしてはいけません。

⑨困ったときは1人で悩まず、まず相談しよう

自らサイバー攻撃に気付いたり、あるいは第三者からの連絡で気付いた場合は、直ちに処置を取り、その後必要な各種窓口に相談しましょう。

あらかじめ対応者を決めてあるならば、その人を中心に対応するか、決めていない場合には、ITに詳しい社員などがいたらその人を中心に対処しましょう。

一番最初にするべきは電源を落とさないままインターネットから切断することです。これはマルウェアなどの拡散を防ぎつつ、後々警察に連絡をする場合の証拠保全になります。

次に、連絡するには状況を把握しなければならないので、なるべく分かる範囲で5W1Hのように分けて事象を記録しましょう。いつから始まったのか、どのようなことがあったのか、誰が作業していたのかなどです。当然のことながらその間、攻撃が行われたと思われるパソコンなどの機器は使わず、その他の機器や紙のメモで記録します。

サイバー攻撃を受けたときに相談するサービスを契約している場合はそちらに相談し、無い場合は、IPAの「情報セキュリティ安心相談窓口」のウェブサイトを検索して、類似の例がないか調べてから、電話やメールで相談しましょう。

ランサムウェアによりデータを暗号化されて脅迫されたり、情報を消されたり、何か機器を故障させられたり、あるいは情報を盗難されたりなど、明確に被害がある、もしくは被害に遭ったおそれがある場合は、各都道府県警のサイバー犯罪相談の窓口などに相談しましょう。

そして自社や団体で扱っている個人情報を盗まれたり消されたりしてしまった場合、「望ましい対応」として、原因究明や再発防止策の策定、そして「努力義務」として個人情報保護委員会などへの速やかな報告が求められます。

従来はファックスや郵送での報告ですが、令和元年3月からは、ウェブサイトからフォーム入力による方法で報告できるようになりました*。

* 詳しい報告先や対応方法は個人情報保護委員会ウェブサイトをご覧下さい。

各種連絡窓口のウェブサイトなど

IPA「情報セキュリティ安心相談窓口」

https://www.ipa.go.jp/security/anshin/
電話番号：03-5978-7509（平日 10:00-12:00, 13:30-17:00）
メールアドレス：anshin@ipa.go.jp

IPA「J-CRAT/標的型サイバー攻撃特別相談窓口」

https://www.ipa.go.jp/security/tokubetsu/index.html
メールアドレス：tokusou@ipa.go.jp

東京中小企業サイバーセキュリティ支援ネットワーク（Tcyss）「中小企業サイバーセキュリティ相談窓口」

https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/tcyss.html
電話番号：03-5320-4773（平日 9:00-12:00, 13:00-17:00）

都道府県警察「サイバー犯罪等に関する相談窓口」

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

消費者庁「「消費者ホットライン」188」

https://www.caa.go.jp/policies/policy/local_cooperation/local_consumer_administration/damage/
電話番号：188

個人情報保護委員会「漏えい等の対応とお役立ち資料」

https://www.ppc.go.jp/personalinfo/legal/leakAction/

2 パスワードを守ろう、パスワードで守ろう

2.1 パスワードってなに？

私たちが、スマホやパソコンなどのIT機器や、各種のウェブサービスを使う上で、欠かせないのが「パスワード」です。

機器やウェブサービスを利用するときに、正当な利用者や持ち主である自分だけが利用でき、他人が利用できないようにするための鍵の役割を果たすものです。

パスワードは、いわば「家の鍵」や「金庫の鍵」。これを適切に守らなければ、家や車、金庫を勝手に開けられてしまうように、パソコンやスマホ、ウェブサービス上にある私たちの個人情報やメール、銀行口座が攻撃者に不正にアクセスされ、情報が流出したり、お金を盗まれたりしてしまいます。

なお、こういった役割を担うものには、他に「暗証番号」などや、通信している情報やパソコン・スマホの中のデータを暗号化して、他人や攻撃者が読めないようにする、「暗号化と復号の鍵＝暗号キー」というものもあります。

この3つは、性格や役割が異なるのですが、よくまとめて「パスワード」と記述されることがあるのと、暗証番号、パスワードと暗号キーは、等しく攻撃の対象になるために、ここでは一括して扱います。

2.2 3種類の「パスワード」を理解する

私たちは、機器やウェブサービスを利用するとき、あるいはファイルを開くときに入力するものを、まとめて「パスワード」と呼び、同じような役割をするものと思いがちです。しかし、セキュリティ上の性質から、「パスワード」とまとめて呼ばれるものは、大きく3つに分けて理解する必要があります。

1. 銀行のキャッシュカードやクレジットカードの利用時や、スマホのロック解除時に使用し、通常4桁から6桁以上の数字だけで構成されることが多いもの（暗証番号やPIN、PINコード、パスコード。通信事業者のネットワーク暗証番号などを含む）
2. パソコンやデジタル機器、ウェブサービスなどの利用時にIDとセットで入力し、英大文字小文字、数字、記号を用い複雑さと一定以上の長さが推奨されるもの（狭い意味でのパスワード、ログインパスワード）
3. パスワードと呼ばれていることもあるけれど、本当はファイルや通信内容を暗号化しまた復号するための暗号鍵として単独で用いられるもの（ZIPファイルのパスワード、WordやExcel、PowerPointの保護パスワード、Wi-Fi機器の暗号化キー、暗号キー、パスフレーズ、セキュリティキー、ネットワークキー）

一口にパスワードといっても、上記のとおり、実にさまざまなものがあります。

この本では、以降、この3つを混同しないように、

1を「PINコード」
2を「ログインパスワード」
3を「暗号キー」

と呼びます。

2.3 「PINコード」と「ログインパスワード」に求められる複雑さの違い

機器やウェブサービスを利用するとき、「ログインパスワード」として、英大文字小文字＋数字＋記号混じりで少なくとも10桁以上を推奨しました。

一方、同様に使う「PINコード」は、メーカーが数字のみの4桁から6桁以上でよいとしています。

この2つは、両方とも機器やウェブサービスを利用するときに使用するのに、求められる長さや複雑さに差があるのはなぜでしょうか。

そもそもパスワードに「複雑さ」が求められる理由は、攻撃者が制限のない状態でパスワードの文字列を総当たりで試すと、時間はかかるが「いつか必ず探り当てることが可能」だからです。これは、どんな複雑な「ログインパスワード」でも変わりません。

こうやって力業（ちからわざ）でパスワードを探り当てる攻撃を「総当たり攻撃（ブルートフォース攻撃）」と呼び、「ログインパスワード」を守る第一歩は、いかにこれを成功させないかにあります。

スマホの「PIN コード」の場合は、数回間違うと「入力遅延」といって一定時間「PIN コード」を入力できないようになり、さらに「10 回間違えば以降 PIN コード入力不可にする（ロック）」「場合によっては機器を初期化する（ワイプ）」ことで「総当たり攻撃」を不可能にし、攻撃者による不正利用を防ぎます。

さらに、厳しいキャッシュカードなどでは、3回間違うと以降カードが利用できなくなりますが、これも同じ考え方です。

「PIN コード」では、こういった厳しい制限を設けることで「総当たり攻撃」を不可能にし、4桁から6桁以上の数字でも攻撃者から機器やサービスを守れるのです。

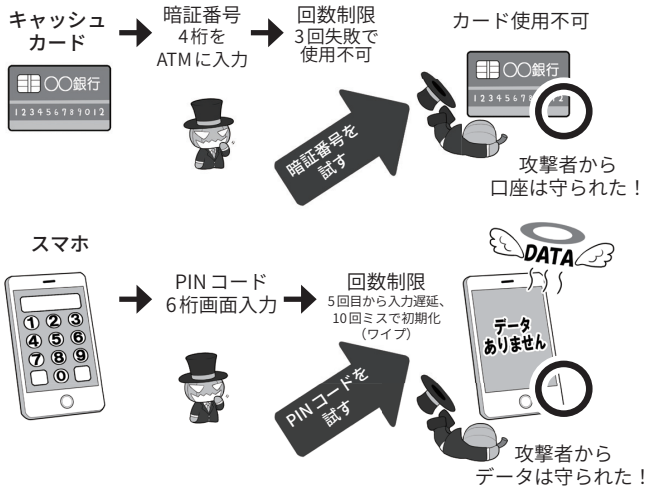
一方、「ログインパスワード」は、通常「PIN コード」のようにワイプまでする機能がついていることは、ほぼありません。数回失敗すると入力間隔が開く、一定時間入力をロックするなどのペナルティを受ける場合もありますが、ペナルティがないものも多いのです。

この「ログインパスワード」は、ウェブサービスのログインページや、パソコンや IoT 機器のログイン画面に入力するもので、こういった入力画面では、ネット経由でログインを試みた場合、どう頑張っても1秒に数回～数十回程度しか入力することができず、これだけで実質的に高速な攻撃を防ぎます。

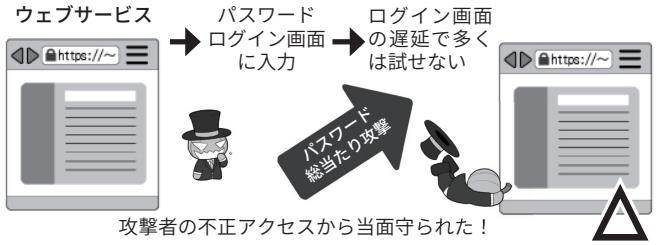
本書の推奨どおり、英大文字小文字＋数字＋記号 26 種＝88 種類の文字を使い、10 桁のパスワードを作ったとすると、その組み合わせは約 2785 京個（京は兆の上の単位）、1秒5回の制限で「総当たり攻撃」をした場合、全部を試すまでに約 1760 億年かかるわけです。

3種のパスワードを理解する

①「PIN コード」の基準で安全性を保てる例

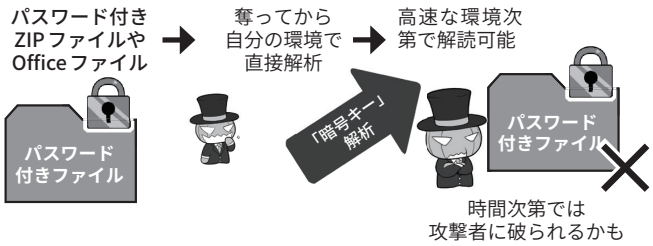


②「ログインパスワード」の基準で安全性を保てる例



攻撃者の不正アクセスから当面守られた！
ただし、辞書攻撃やリスト型攻撃には弱い

③「暗号キー」の基準で安全性を保てる例



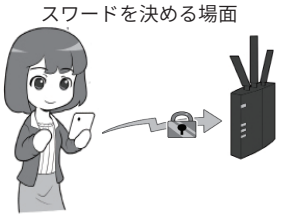
時間次第では攻撃者に破られるかも

一見、安全性を保つための基準がわかりにくい例

内蔵記憶装置暗号化の救済が必要になる場面

「ログインパスワード」基準の複雑さで安全性を保てそうに思えるが、実際には入力遅延による防御が働かないので「暗号キー」の基準を採用すべき。

無線 LAN アクセス時に入力するパスワードを決める場面



ルータにログインする際のパスワードは「ログインパスワード」でよさそうだが、「暗号キー」の基準で設定した方がよい。

※この図は一例であり、実際の機器の条件とは異なります。

これならば、100年以内に探り当てられる確率は非常に小さく、事実上不可能といえるわけです。

このような攻撃の想定を、セキュリティ用語的には「オンラインアタック(攻撃)」といいますが、ここでは「『ログインパスワード』への攻撃」と呼ぶことにします。

2.4 「暗号キー」に求められる複雑さ

上記の「ログイン画面」に入力する「ログインパスワード」とは異なり、「暗号キー」の場合は、攻撃者が暗号化されたデータを盗んで持ち帰り、ログイン画面の遅延などなく、自分のペースで高速な暗号化解除(解読)の攻撃ができます。

この攻撃の対象となるのは、「1つ、または複数のファイルを圧縮したパスワード付きZIPファイル」、「パスワードを設定したMicrosoft Officeのファイル」、「暗号化されたUSBメモリ」や「パソコンから取り出された内蔵補助記憶装置(ハードディスクやSSD。以下記憶装置)」、あるいは「暗号化された無線LAN通信の内容」などです。

こういったものでは、「パスワード」と思って設定しているものが、実はパスワードではなく、中身を読まれないようにするための暗号化に使われる鍵=「暗号キー」となっている場合が多いのです。

ZIPやMicrosoft Officeのファイルは、パスワードが設定されていると、開くときにパスワード入力画面が出るので、入力遅延の防御があるように見えますが、実はその画面はZIPやOfficeのプログラムが提供しているもので、ファイルそのものは単なる暗号化されたデータにすぎないのです。

そのため、パスワード入力画面を使わなくても直接ファイルに対して暗号化解除の攻撃が可能であり、遅延による防御はありません。

このような暗号化解除は、「暗号キー」が短いと、スーパーコンピュータを使うまでもなく、市販されているゲーム用パソコンの性能で十分可能なレベルの難易度なのです。少し古いデータになりますが、2019年ごろの一般流通するゲーム用パソコンでもグラフィックボードに搭載されているGPUというプロセッサーを駆使すれば、ZIPファイルに対して40億回/秒の暗号化解除の攻撃が可能というデータすらあります。さきほどの約2785京個の組み合わせがある場合でも、解読までにかかる期間は78.5万年に短縮、8桁のものになると103年、8桁で記号抜きの62種の文字だと6年、英大文字小文字だけだと2年となります。短く単純なパスワードなら短時間で解読可能できてしまう、GPUの性能が向上すればそのような日がいずれ訪れても不思議ではありません。そのため本書では、「暗号キー」には、完全にランダムで英大文字小文字+数字+記号混じりで15桁以上のものを推奨し、これを基準とします。

ZIPのパスワードに、15桁ものランダムな文字列を使うのは、覚えられなくて無理だと思われるでしょうが、8桁程度のパスワードでは破られてしまうので、暗号化したつもりでも攻撃者の前では意味がないのです。なお、このような想定の攻撃をセキュリティ用語的には「オフラインアタック(攻撃)」と呼びますが、ここでは「『暗号キー』への攻撃」と呼ぶことにします。

2.5 総当たり攻撃以外のパスワードを破る攻撃や生体認証を使った防御

パスワードなどを破る攻撃には、「総当たり攻撃」の他にもさまざまな手法があります。

パスワードでよく使われる言葉などを集めた、専用の辞書を利用する「辞書攻撃(ディクショナリアタック)」、ウェブサービスなどから流出した名簿やIDとパスワードのリストを入力して試す「リスト型攻撃(アカウントリスト攻撃・パスワードリスト攻撃)」など。

これらに対する防御のためにも、「ログインパスワード」には意味のある単語や、自分に関連の深い語句やよく使われるパスワードは避け、推奨する基準に従い、充分に複雑で、かつ他の機器やウェブサービスで使い回していないものを設定しましょう。

「PINコード」は、入力を間違え続けると「入力遅延」や「ロック」機能があるため、「総当たり攻撃」などの手法が有効ではありません。

しかし、「PINコード」の強さは「盗み見や、推測されないこと」が前提ですので、入力するときは周りに気を配り、また、自分の個人情報など推測しやすいものは使わないようにしましょう。

2.6 パスワード流出時の便乗攻撃に注意

サービス側から、パスワード再設定の通知がメールなどで送られて来た場合、まずそれが本当にサービス側から送られてきたものかどうか、該当のサービスのウェブサイトやニュースサイトでチェックし、事実の確認をしましょう。

サービス側を装ったパスワードリセットの通知は、流出事故に便乗したフィッシング詐欺などのよくある攻撃パターンです。パスワードを奪う攻撃者の罠かもしれません。通知のメールにパスワードリセットのリンクなどが貼られていても、うかつにクリックしたりせず、リセットする場合も直接公式サイトやアプリからしましょう。

なお、ウェブサービスを利用するときは、パスワードが流出した場合に簡単にアカウントを乗っ取られないように、必ず二要素以上の多要素認証を設定しておきましょう。これが提供されないサービスは、セキュリティ意識が低い可能性があるのでそのサービスの利用は再考しましょう。

2.7 適切なパスワードの保管

さて、日常的にインターネットを利用していると、IDとパスワードは無限に増えていきます。どう管理すればよいのでしょう。

本書では、「スマホ用のパスワード管理アプリ」か「物理的な紙のノート」の利用を推奨します。

スマホのパスワード管理アプリを導入する場合は、ネットにデータを置く「クラウド連携(バックアップ)機能」を安易に利用せず、まずはスマホ内だけで管理する「スタンドアロン」状態で利用できるものを優先しましょう。

紙と比較した場合、スマホはネットに接続されているので、攻撃者にクラッキングされる可能性は捨てきれませんが、利用規約を守り、システムを最新に保っている限りは、スマホのセキュリティは十分に高い設計となっています。

また、紛失や盗難に遭っても、最新のスマホはデータを暗号化した状態で保存していますし、パスワード管理アプリも独自に暗号化するので二重に暗号化された金庫での保管に等しくなります。加えてスマホは、事前にきちんと設定しておけば、紛失や盗難に遭っても遠隔操作でロックして操作できなくしたり、場合によってはワイプ(消去)して情報流出を避けたりできるという、紛失に対する三重四重のセキュリティが設けられています。

一方、紙のノートを推奨する理由は、あたりまえではありますが、紙のノートはネットに接続できないからです。接続できなければネット経由のサイバー攻撃も不可能です。奪うには現実世界で「盗む」という行動を起こさなければならず、攻撃者が姿を現すリスクがあることが抑止力になるからです。

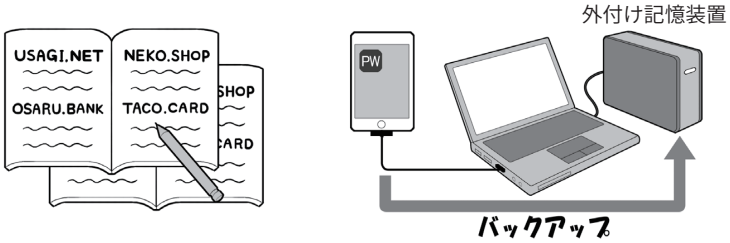
ウェブブラウザにはパスワードを保存しない

ウェブブラウザにパスワードを保存すると、席を離れた隙に勝手に利用されたり、パソコンをクラッキングされた際に根こそぎ盗まれる可能性があります。

パスワード管理方法の例

一見分かりにくい
紙のノートに二重で

管理アプリのデータは、暗号化した記憶装置にバックアップ



紙のノート二冊に記入したり、スマホのパスワード管理アプリを使って、パソコン経由で暗号化した記憶装置にバックアップする方法があります。紙のノートは一見内容が分からないようにできる専用のパスワードノートも売られています。

2.8 パスワード情報をクラウドで保管する善し悪し

パスワード管理アプリや、同様の機能を持つソフトには「クラウド連携機能」やクラウドを用いた「バックアップ機能」があり、これを利用すると複数端末でパスワード情報を共有できたり、明示的にバックアップ処理をしなくても自動でクラウド上にバックアップデータが作られたりします。

この機能を無条件で推奨しない理由は、「重要な情報が複数箇所に存在すれば、流出する可能性がその分増える」からです。

加えて、クラウドサービスを利用する場合、他人の手元でデータが保管されますが、利用者には、そのサービスが運用しているシステムのセキュリティレベルの実態を知ることも管理することもできません。

また、パスワード管理アプリのデータがスマホ上にある限りは「PIN コード」方式で守られますが、クラウドのバックアップデータが流出すれば、マシンパワーにものをいわせた高速なオフラインアタック、暗号化解除の攻撃が可能になるからです。

銀行の口座からお金が盗まれれば、自分にミスがない限り銀行が補填してくれますが、クラウドから流出した情報は実質的に回収不可能です。これは、「お金は補填が可能だが、重要情報の秘密性は戻らない」からなのです。

2.9 ノートやスマホを失くした場合のリカバリ考察

さて、パスワードを記録したスマホも紙のノートも、紛失してしまうと困るのは同じです。ただ、スマホの場合、パソコンでスマホのデータを丸ごと暗号化してバックアップをしておけば、紛失しても代替機をパソコンに接続し「復元」を指示するだけで、環境やパスワード管理アプリの内容を含めて、すべて元の状態にできるものもあります。

また、スマホを丸ごとバックアップしなくても、パスワード管理アプリのデータを、パソコン経由で暗号化された外部記憶装置などにバックアップし、普段は接続せず適切に保管しておけば、復旧は容易です。アプリによっては紙に印刷して保管する機能もあります。

なお、クラウドサービスのメリットとデメリットを理解した上で、クラウドを使った複数機種での連携機能、自動バックアップやそれに付随するリカバリ機能を利用するのは1つの選択肢といえます。

紙のノートの場合は、原則自宅など安全な場所で保管し、持ち運ぶのは避けましょう。万一の盗難などに備え予備を用意しておくとさらに安心です。

パスワード管理方法のメリットデメリット

	盗難・紛失対策	ネット経由のセキュリティ	データの管理者
 紙のノート	○ 持ち歩かず自宅などの安全な場所に保管する	○ 攻撃不可	本人
 スマホアプリ	△ 盗難・紛失のリスクが高め。バックアップが必要	△ セキュリティレベルによる	本人
 外付けＨＤＤへバックアップ		○ ただし普段は接続しない	本人
外付け記憶装置へバックアップ  クラウドサーバにバックアップ		△ サービス側のセキュリティレベルによる	事業者

パスワードの管理方法とバックアップ方法を、１つの表で同列にまとめていますが、一番右列のデータの管理者の項目をよく見て下さい。クラウドサービスを使ったバックアップは便利ではありますが、データの管理者は自分ではなくなります。また、クラウドサービスのセキュリティがどのレベルなのかは、自分では容易に判断できません。

パスワードに関してのみは多少の不便さはあっても、自らの責任において管理するのか、それとも他人の手を借りるのか、クラウドはそれに伴うメリットとデメリットをよく勘案して利用しましょう。

コラム　パスワードを記録する演習

前項でも解説しましたが、パスワード管理アプリは利便性に優れていますが、端末がネットに接続している限りサイバー攻撃のリスクからは逃れられません。一方、紙のノートによる管理は、ネットから遮断されているためサイバー攻撃でパスワードを盗み見ることは不可能です。

加えて、大切な家族のためにパスワードなどを記録しておくことは重要です。

次頁のメモ欄を利用しながら、安全にパスワードを記録・保管する方法を実践してみましょう。

注意事項として紙のノートは紛失した場合、中を見られなくする制限はかけられません。また、外出時は覗き見のリスクがあるため、ノートはむやみに持ち歩かずに自宅など安全な場所で保管・管理しましょう。

万が一、ノートを紛失したり、誰かに覗き見されたりした可能性がある場合は、予備を作成・保管しておき、その予備を参考にしながら早急にパスワードを変更することが必要です。

また、パスワードを記録する際には、盗み見した者が記録されたパスワードを使用して、すぐに悪用できてしまう可能性を少しでも下げる工夫を施しておくと、より安全にパスワードを保管できます。

具体的には「実際には含まれない余分な文字を混ぜてノートに記録する」「実際のパスワードは前後どちらかに2,3桁程度、暗記できる数の文字が追加されたものに設定して、すべての文字はノートに書き残さない」などがあります。工夫次第でさまざまな方法が考えられますし、煩わしさを感じない、無理のない範囲で工夫してみしょう。

パスワードを紙のノートに記録しておくことは重要

パスワードを確認できて便利で、万一の備えとしても家族のために役立つ

サイト名：通販〇〇
ID／ユーザー名：nisctaro
パスワード：3%2/aGNA%G!Listw

メールアドレス：nin******@gmail.com
メモ：毎月5の付く日がお得！

サイト名：動画サイト〇〇
ID／ユーザー名：nischanako
パスワード：Dc(fq--)a)td4un%

メールアドレス：hn*****@gmail.com
メモ：サブスクプラン利用（月額980円）

課金しているサービスはプラン名や金額を記載しておくとよい

盗み見されてもすぐに悪用されないような工夫があるとより安全

サイト名：
ID／ユーザー名：
パスワード：X!#KejNiD9$+Z7JT,gRl/hs!

メールアドレス：
メモ：

実際のパスワードは偶数番目だけの文字にする

サイト名：
ID／ユーザー名：
パスワード：TnW$TMAFyWXPqAhzRKE!Y72s9

メールアドレス：
メモ：

パスワードのみなど、最低限の情報の記録に留める

実際は前後どちらかに2,3桁程度、暗記できる数の文字が追加されたパスワードに設定して、すべての文字はノートに書き残さない

サイト名：
ID／ユーザー名：
パスワード：

メールアドレス：
メモ：

サイト名：
ID／ユーザー名：
パスワード：

メールアドレス：
メモ：

サイト名：
ID／ユーザー名：
パスワード：

メールアドレス：
メモ：

サイト名：
ID／ユーザー名：
パスワード：

メールアドレス：
メモ：

サイト名：
ID／ユーザー名：
パスワード：

メールアドレス：
メモ：

サイト名：
ID／ユーザー名：
パスワード：

メールアドレス：
メモ：

サイト名：
ID／ユーザー名：
パスワード：

メールアドレス：
メモ：

サイト名：
ID／ユーザー名：
パスワード：

メールアドレス：
メモ：

MEMO

3 社内・社外のセキュリティを向上しよう

3.1 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。

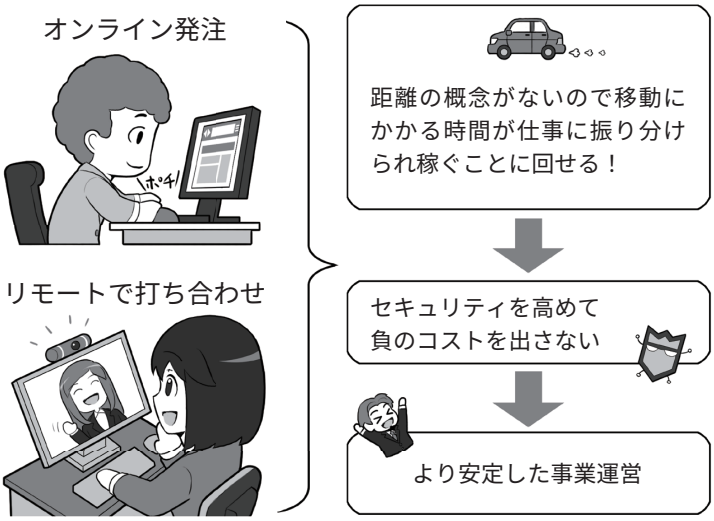
近年では「セキュリティ・バイ・デザイン」という考え方が一般的になりつつあります。企業のITシステムや業務プロセスなどを設計する段階でセキュリティ対策を組み込んでおき、サイバー攻撃による不測の事態に備えるのです。

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。

3.2 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、クラウドストレージ、ウェブサーバなどが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。

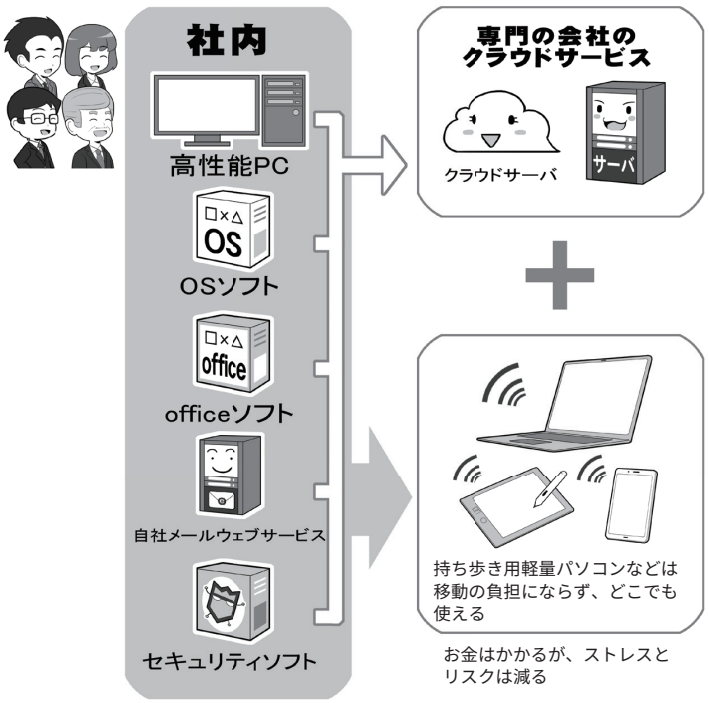
こういった新しいシステムや環境は、セキュリティ対策も込みで提供される場合や、これまでバラバラだったコストが集約・整理されて軽くなる場合があり、総コストが従来より安く済むこともあります。ただし、逆にコストがかかる場合があるので、導入前にしっかり確認しましょう。また、クラウドサービスは設定次第で誰でもアクセスできる場合がありますので、設定に注意して利用する必要があります。

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

4 災害時の会社のために事業継続計画(BCP)を作ろう

4.1 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)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。

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。

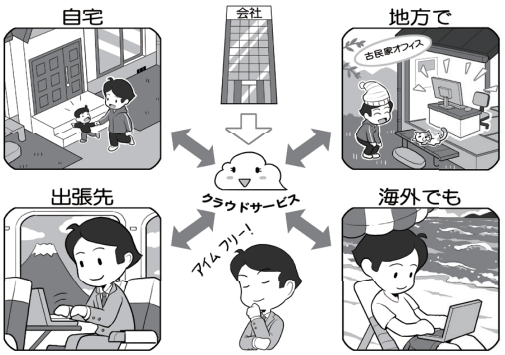
2点目。災害時には被災者が通信を円滑に行えるよう暗号化されていない無線LANが各所で提供されます。これも攻撃されやすいポイントなので、使用する場合はVPNを使うこと。

3点目として、専門用語ではBYOD(Bring Your Own Device)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。

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

4.2 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。

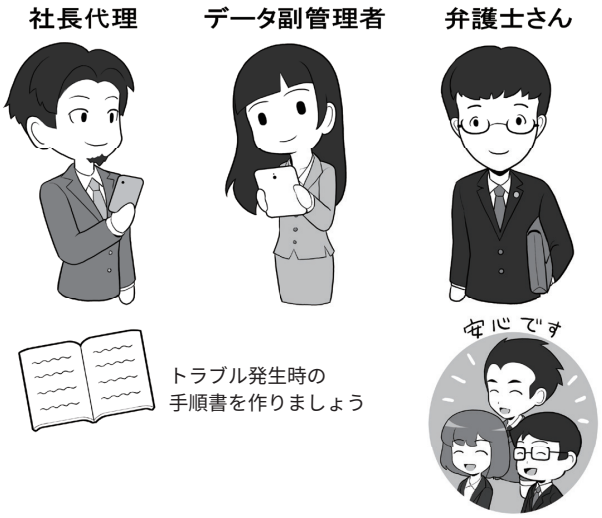
このように災害に遭った場合、どのように事業継続するか、そのバックアップ体制を考えましょう。

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。

5 テレワークとアウトソーシングをうまく利用しよう

5.1 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。

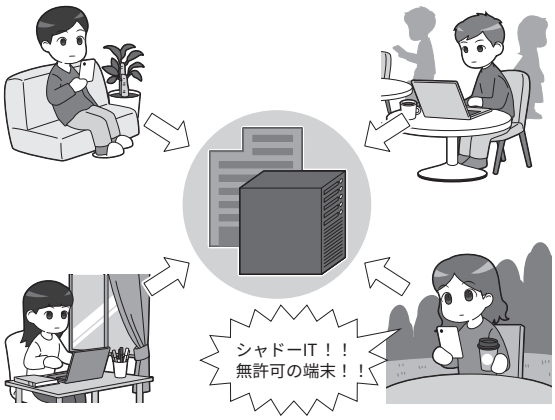
BYODの実施にあたっては、従業員が端末を盗難された場合など、想定されるセキュリティ上のリスクを企業側が事前に把握しておく必要があります。

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

5.2 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。

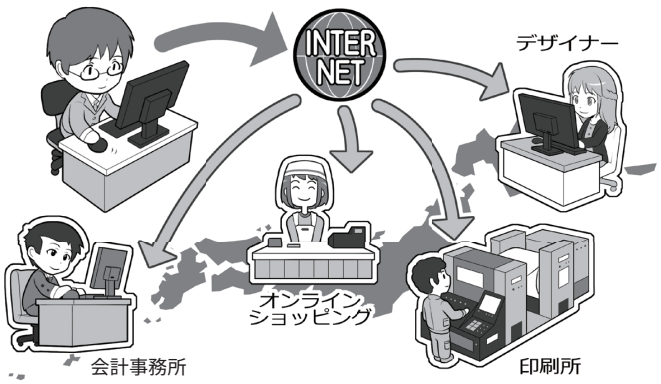
また、経理処理なども会計ソフト会社がオンライン対応になることで、取っておいたレシートをスキャナやスマホの撮影機能経由で提供されているクラウドサービスにダイレクトにアップロードすると、基本的な伝票入力が行われた状態で会計ソフトに返ってくるようになっているものもあります。

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

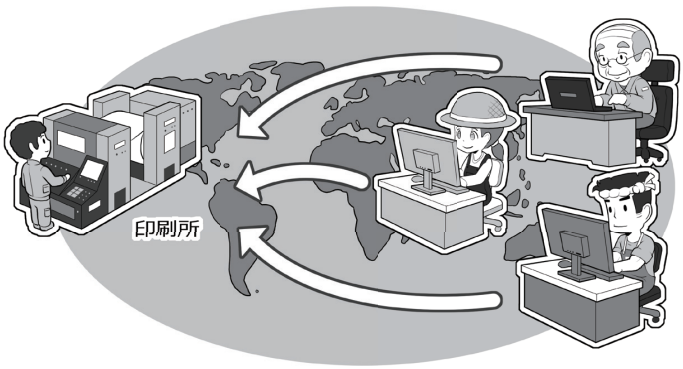


社員がどこにいても仕事ができるのと同様に、地方に住んでいる専門分野の人たちと仕事をする制約も少なくなります。場所ではなく求める技術を基準にフリーランスの人を探して仕事を依頼することもできますし、自社で原稿だけを作り、制作や印刷といった後工程の業務を、遠方のプロにオンラインで発注することもできます。場合によっては特定の業務を行う自分の手間と発注のコストを計算して比較して、それをアウトソーシングすることで、自社や自団体が自らが得意とする分野に注力して能力を向上し、逆に選んでもらえるプロになりましょう。

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。

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。

6 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。

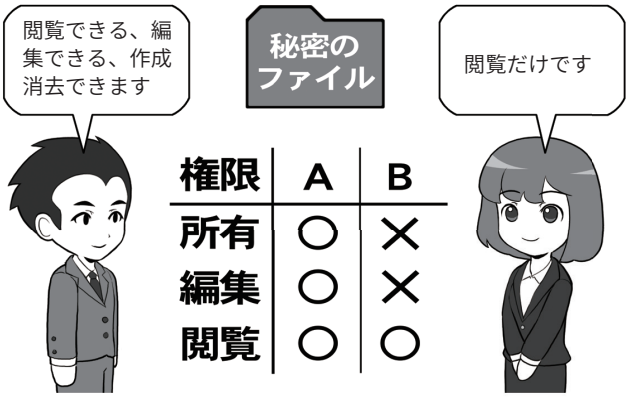
共有設定には、ファイルの管理を例にあげれば、単純に見られるか見られないかを意味する「閲覧」、そのファイルを編集して内容を書き換えることができる「編集」、そしてファイルそのものを作ったり削除したりできる「所有」などの、大まかに3つの権限があります。

会社内でファイルをUSB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」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。

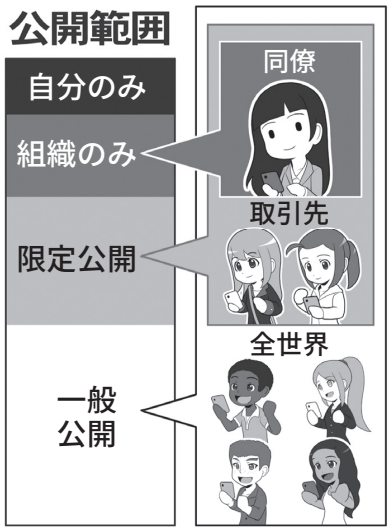
この公開設定の初期設定が一般公開になっていたり、誤って公開範囲を変更してしまったりした場合、情報が外部から閲覧できる状態になります。何者かに情報を持ち去られたり、公開された情報が原因で報道やSNSで話題になり炎上したりした企

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。

業の事例もあります。

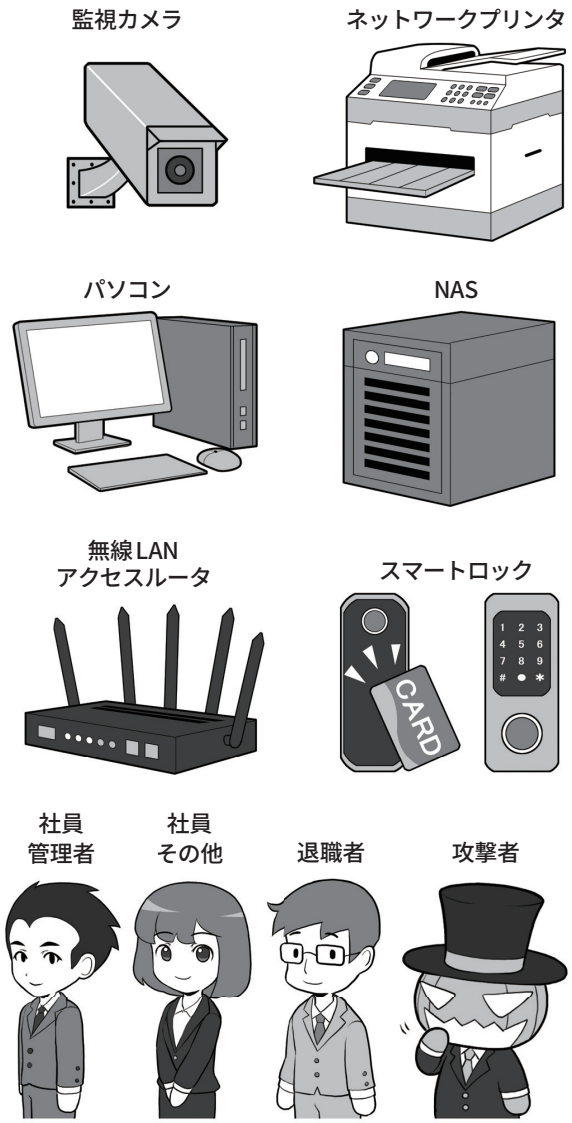
LAN上のNASでもストレージサービスでも、共有設定はファイル単位やフォルダ単位で設定できるので、その整合性に気を付けないといけないことと、例えば臨時で誰かに特定のファイルを公開したい場合、設定ではなく「見たり編集したりできる」リンクを送信することで共有することができるものもあり、この場合、そのリンクを知っている人は誰でも同じ権限を持つので、送信後の管理にとくに注意が必要です。

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。

7 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

7.1 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。

7.2 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。

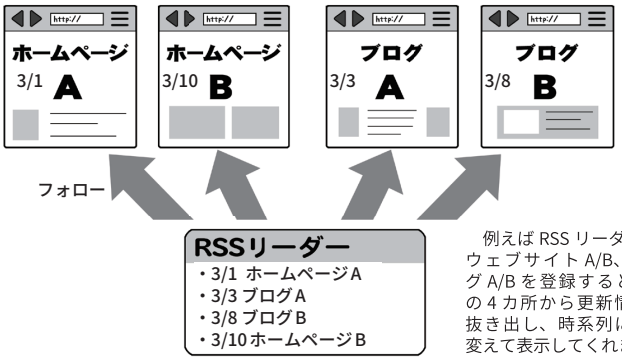
そうしたRSSを簡単に閲覧できるのが、RSSを管理できるウェブサービスとスマホ用のRSSリーダーと呼ばれるアプリの組み合わせです。それらを利用すると、まるでSNSを閲覧する感覚で、毎日世界中のどこかで起きているサイバー攻撃情報やトレンドが読むことができ、否が応でもセキュリティに関しての知識が蓄積されるでしょう。

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

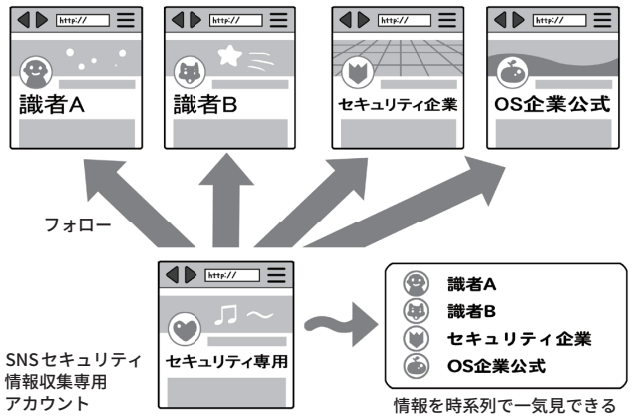
RSSとは平たくいえば、ウェブサイト上の更新情報を、見出し、もしくは概略付きで、時系列に、ウェブサイトの裏の見えない所で発信しているものです。規格（フォーマット）が決まっているので、RSSリーダーに登録すると複数の情報源を串刺しして見ることができます。

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。

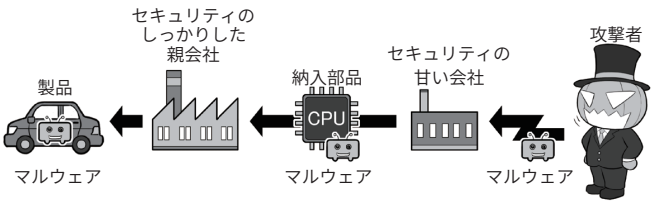
8 企業が気を付けたい乗っ取りのリスクを理解しよう

8.1 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。

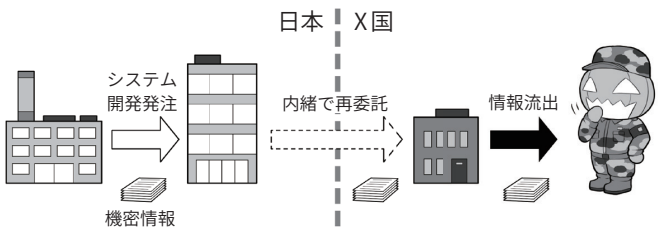
また電子機器を生産している企業などでは、生産しているIT部品にマルウェアやバックドアを仕込み、これを大企業に納入させることで、大企業が生産している製品を乗っ取る環境を整えるなどします。例えば大企業へ納入するのがネットワーク部品で、大企業が生産する最終製品がパソコンなら、最悪の場合、マルウェアやバックドアが仕込まれたパソコンが一般流通する事態になります。こういった攻撃に遭うと、サプライチェーンに関係する中小企業や団体にも責任が生じます。

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。

8.2 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。

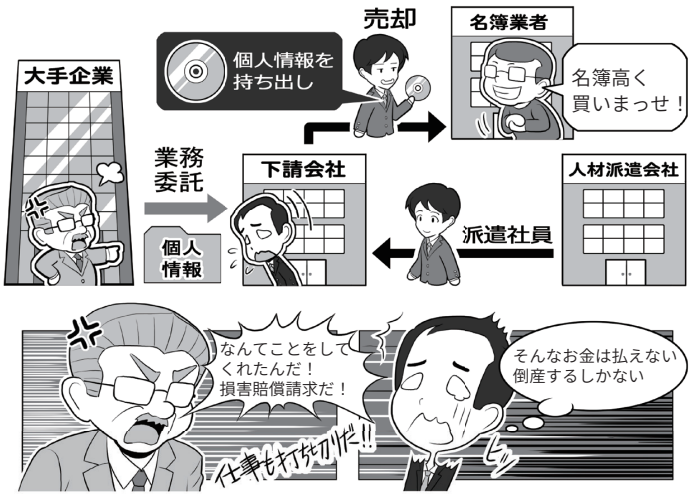
本件は、クラッキングなどを行ったサイバー攻撃によるものではありませんが、内部犯行者によるれっきとしたサイバー攻撃でした。

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。

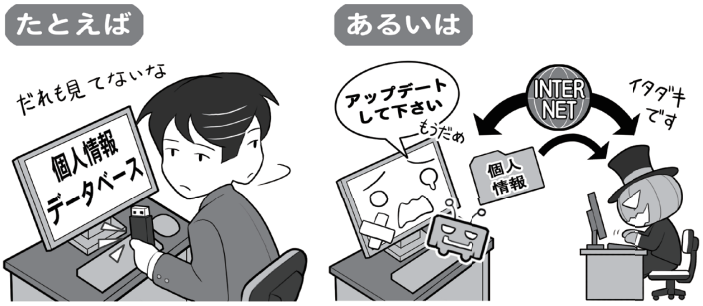
ましてやこれが、社員数名しかいない中小組織だったら、金銭的賠償は不可能でしょうし、NPO だった場合は、高い意識を持って始めた事業であっても、情報流出を起こしたことで信頼を失い、その目的の達成を断念せざるを得ない事態に陥ったでしょう。

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？



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。

9 企業が気を付けたいサイバー攻撃の具体例を知ろう

9.1 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。

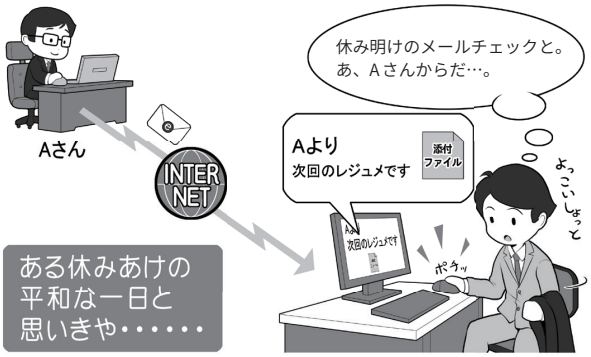
1つは、長い連休中にはセキュリティアップデートや、総合セキュリティソフトの更新が行われている可能性があります。日常的な業務を始める前に、まずアップデートして連休中に見つかったシステムのセキュリティホールや新しいマルウェアに対応できる状態にしましょう。

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。

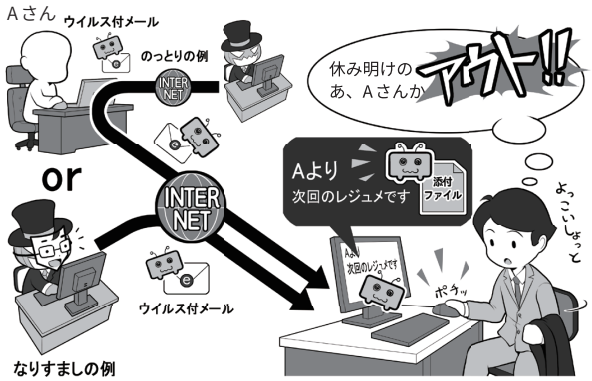
それに原則的なルールは、「メールを見ただけで完結しないものはすべて疑え」であり、「挙動が怪しい場合には、組織内にセキュリティ担当の窓口が設置されていれば、そちらに連絡する」です。それは添付ファイルでもメールの文中の外部ウェブサイトへのリンクでも同じです。

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。

9.2 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。

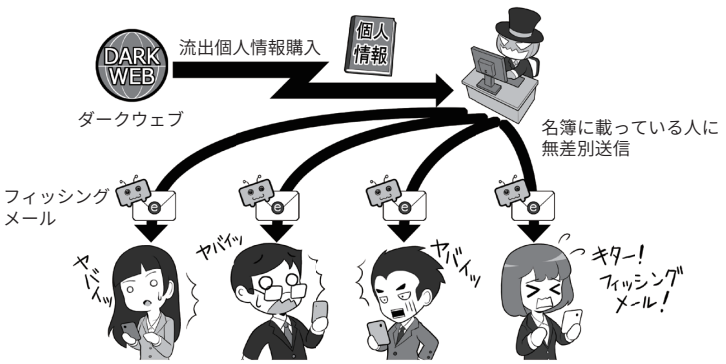
一方で、そのウェブサイトがショッピングサイト相当の暗号化(https://)に対応していて、一見そのショッピングサイトと同じ名前を掲示していても、実は「アルファベットに似た別の言語の文字」を使用している場合もあります。

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。

9.3 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。

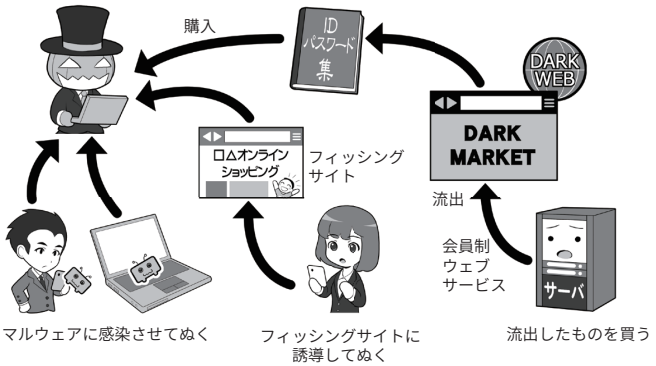
①のIDとパスワードの流出はマルウェアの感染やウェブサービスからの流出などがあり、自分で防げるものと防げないものがあります。自分で防ぐには、セキュリティをきちんと固めるだけです。一方、ウェブサービスからの流出は、多要素認証を導入していないセキュリティ意識が低いサービスを避けるなど、消極的手段はありますが、最終的には自分でどうにかすることはできません。

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。

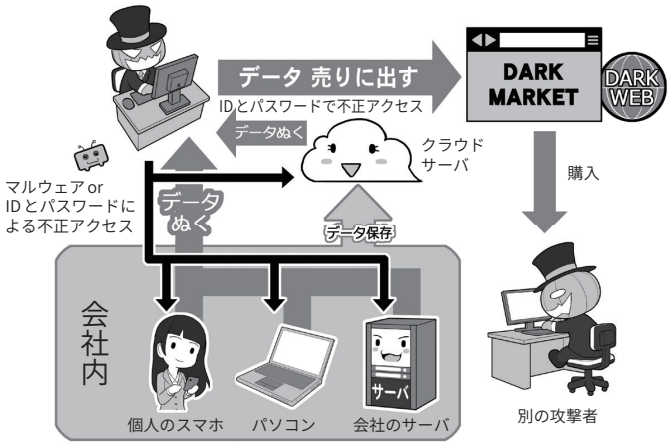
不正アクセスを行うために攻撃者は…

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。

9.4 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」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。

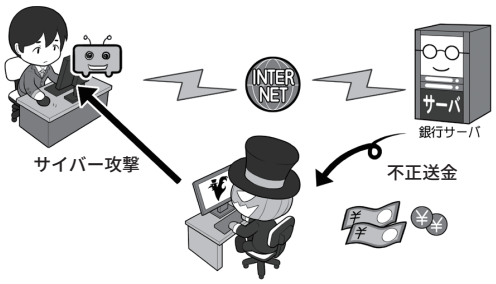
幸いにして情報の流出などと異なり、銀行の場合は過失が無いことが認められれば、銀行側が補填してくれることもあります。クレジットカードの不正利用なども同様です。

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。

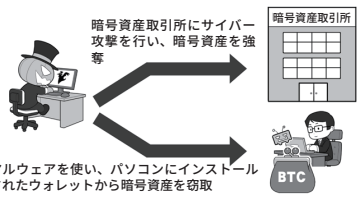
オンライン決済は常に狙われている



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

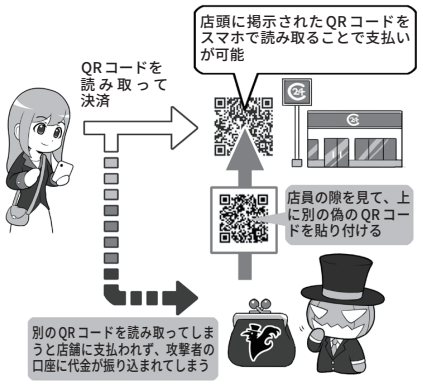


暗号資産を巡るサイバー攻撃も続発しています。実際、国内海外含め多くの暗号資産取引所がサイバー攻撃を受け、大きな金銭的被害が生じた事例がある他、暗号資産の窃取を目的としたマルウェアも登場しています。

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。

9.5 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)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

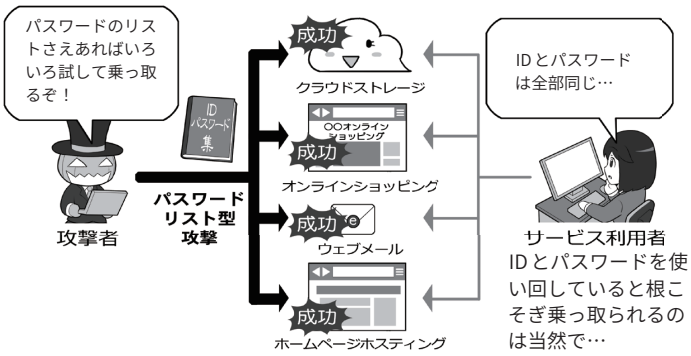
ランサムウェアはパソコンなどの中のファイルを勝手に暗号化するため、感染すれば仕事上の極めて重要なファイルも人質に取られてしまいます。大事なデータが入ったパソコンが使えなくなれば、業務停止、納期遅延など顧客に迷惑をかけ、その結果、会社としての信用を失う恐れもあります。バックアップは常にしておきましょう。

9.6 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セキュリティキーなどを用いて、攻撃者が不正ログイン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

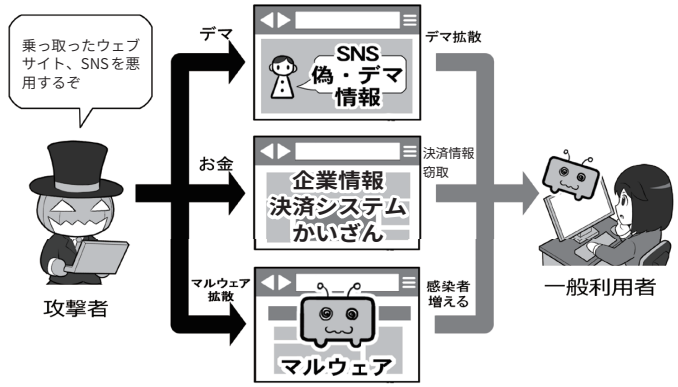


つい面倒くさがってIDとパスワードを使い回ししていると、どこか1つでも流出が起これば、同じIDとパスワードを使用しているサービスが根こそぎ乗っ取られる場合があります。また、別々のパスワードを使っていても、そのパスワードがよく使われるような簡単なものだった場合、そういったパスワードをまとめたリストが流通していて、それを使ってアカウントを乗っ取る攻撃が行われます。一部を変えただけなど、似たようなパスワードも非常に危険です。

9.7 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。

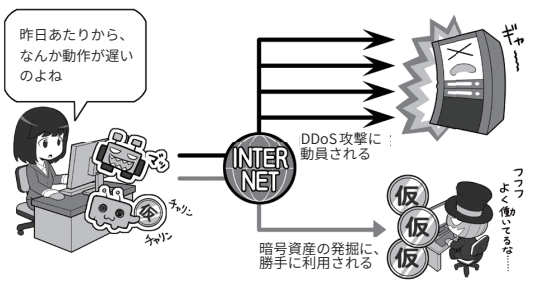
9.8 DDoS攻撃

DDoS攻撃とは、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)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。

9.9 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(まいきょ)に遑(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。

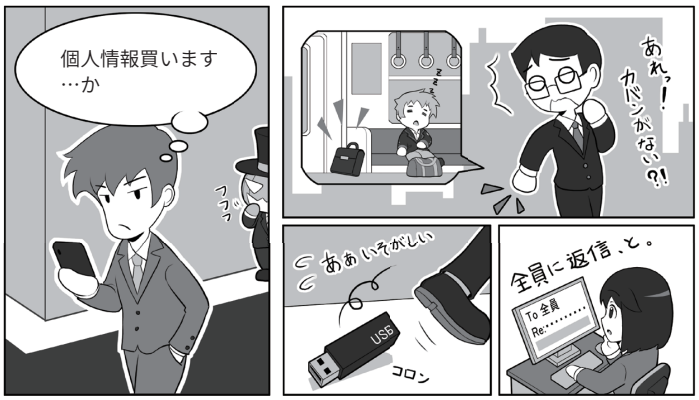
例えば内部犯行防止に、必要がないときに顧客情報を扱う部屋に人を入れないよう、部屋や建物に施錠をしているでしょうか。アルバイトや社員に、きちんと情報モラル教育をしているでしょうか。

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。

情報流出の可能性はたくさんある



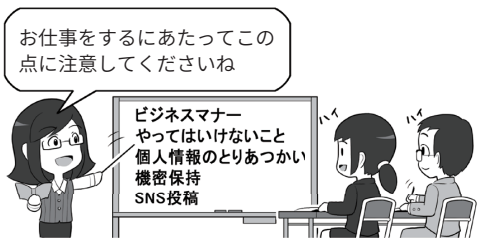
流出の可能性は情報を扱う人を狙ってそそのかすことだけではありません。機密情報を入れたパソコンをカバンごと電車やタクシーの中に置き忘れる、生徒の成績などが入ったUSBメモリを落とす、多数の人に一斉メールを送ろうとしたら、互いのメールアドレスが分からないBCC欄ではなく、見えてしまうTOやCC欄に入れて送信してしまった、などなど。パソコンやスマホ、IT機器は便利な反面、ミスを犯すときも一瞬で多量に失います。要注意です。

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。

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

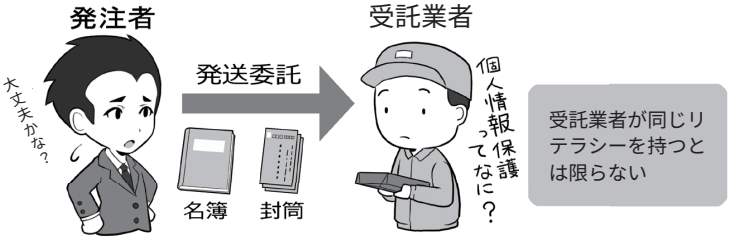
が義務づけられます。

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。

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…



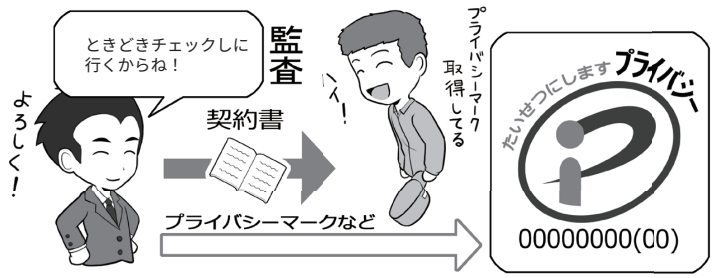
個人情報やプライバシーに関して、きちんと管理しなければならないことであるという意識は広がりつつありますが、それは自社や自団体の中だけにはなっていませんか？

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) 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/

付録01 サイバー攻撃を受けた場合①〜情報関係機関への相談や届け出

一般国民向け　中小組織向け

会社や団体として、相談したり必要に応じて届け出を行うものとしてはどのようなことを知っておくとよいのでしょうか。

まず、とりあえずサイバー攻撃を受けたらどこに相談したらいいのか。

代表的なものとしてIPAによる「情報セキュリティ安心相談窓口」があります。同名のウェブサイトを検索すると、「良くある質問」や、過去のサイバーセキュリティに関するレポートなどが掲示されているので、一通り目を通し、それでも解決しない場合は、電話やメールで問合せしてみるとよいでしょう。

「標的型メール攻撃」に関しては「標的型サイバー攻撃特別相談窓口」が個別に設けられています。詳しい情報を提供すると、より速やかに的確な対応ができるようになっています。それとは別に、義務ではありませんが、「ウイルスの届け出」「不正アクセスの届け出」を受け付けているので、可能であれば届け出ましょう。そうすることで他の人が攻撃に遭うのを避けることが可能になります。

地域の商工会議所がサイバー攻撃対応支援サービスの一環として、有料の相談窓口を設けている場合もあります。なお業種によって、例えば医療機関でのサイバー攻撃に関しては、厚生労働省が、医政局 研究開発振興課医療技術情報推進室で連絡を受け付けています。また、IPAでは、その年のサイバーセキュリティ上の懸念される脅威を「情報セキュリティ10大脅威」として公開しています。個人編と組織編に分けて順位付けされており、脅威の内容に加えて、参考事例や注意するポイントがまとまった内容となっています。

さらに、組織を狙った脅威として急激に増えているランサムウェアに関しては、「ランサムウェア対策特設ページ」が用意されています。万が一、企業や組織でランサムウェアの被害に合った場合、まずここのページをご覧いただき、迅速かつ正確な対応を進めていきましょう。

情報セキュリティ10大脅威	
https://www.ipa.go.jp/security/vuln/10threats.html ※脆弱性対策（IPA公開資料一覧ページ）https://www.ipa.go.jp/security/vuln/index.html	
ランサムウェア対策特設ページ	
https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html	
IPA情報セキュリティ安心相談窓口	
URL	https://www.ipa.go.jp/security/anshin/index.html
電話での相談	03-5978-7509 （受付時間 10:00〜12:00、13:30〜17:00、土日祝日・年末年始は除く）
メールでの相談	anshin@ipa.go.jp
FAXでの相談	03-5978-7518
郵送での相談	〒113-6591 東京都文京区本駒込2-28-8 文京グリーンコート センターオフィス16階 IPAセキュリティセンター 安心相談窓口

IPA安心相談窓口で対応出来ない例

なお、IPA安心相談窓口では、下記のような相談は受け付けていません。

- 直接来訪しての相談や面談
- 契約・支払いに関する相談
- 法的解釈に関する相談
- 個別の端末調査や犯罪調査に関する相談
- 特定の製品やサービスの紹介
- 特定企業への改善や指導に関する相
- パソコンの具体的な操作方法や手順などの案内
- 他組織への連絡や通報などの仲介

一方、IPAではなく他の機関が開設している窓口で対応出来る場合もあります。それぞれの窓口の受け付ける事柄を、ウェブサイトなどでよく確認してご相談ください。

●サービス提供または購入などの契約に関するトラブルで困っている場合

消費者ホットライン（消費者庁）
http://www.caa.go.jp/region/shohisha_hotline.html

国民生活センター
http://www.kokusen.go.jp/

●犯罪行為に関する被害届や捜査について相談をしたい場合

都道府県警察本部のサイバー犯罪相談窓口等一覧
https://www.npa.go.jp/cyber/soudan.html

●法的トラブルの相談をしたい場合

法テラス
https://www.houterasu.or.jp/

●インターネット上での違法・有害情報に関し相談したい場合

違法・有害情報相談センター
https://www.ihaho.jp/

社団法人 コンピュータソフトウェア著作権協会
不正コピー情報受付
https://www2.accsjp.or.jp/piracy/

●インターネット上の違法情報を通報したい場合

インターネット・ホットラインセンター
https://www.internethotline.jp/

●迷惑メールの受信に関して困っている場合

財団法人 日本データ通信協会迷惑メール相談センター
https://www.dekyo.or.jp/soudan/ihan/

●フィッシングサイトの発見または被害に関して困っている場合

フィッシング対策協議会
https://www.antiphishing.jp/registration.html

警察庁 フィッシング110番
https://www.npa.go.jp/cyber/policy/phishing/phishing110.htm

●インターネットに繋がらないなどのトラブルで困っている場合

利用プロバイダまたはパソコンのメーカー・購入店の各サポート窓口

IPA「他の機関が開設している相談窓口等」より
https://www.ipa.go.jp/security/anshin/external.html

付録02 サイバー攻撃を受けた場合②
～警察機関への相談や届け出、ガイドライン 中小組織向け

サイバー攻撃では前項のように、自分が攻撃を受けたことに関する相談の他に、実際に情報を盗難されたり、なんらかの被害を被ったり、あるいは法律で禁止されている不正アクセスなどに該当する場合は、警察への相談や通報が必要となります。

まずは都道府県警察本部のサイバー犯罪相談窓口に相談することを最初に考えるとよいでしょう。

その場合でも5W1Hのように「なにがどうなってどういったことが起こっているのか」を、紙に書くなどして整理して明確にし、漠然とした相談にならないようにしましょう。警察がなんらかの捜査をする場合は、そのための情報や証拠が必要となります。

データ損失や不正送金など実害が発生した場合は、やたらにその機器を操作せず、まず相談窓口に相談して対処方針を決めるとよいでしょう。

さてそういった相談窓口を知っておいた上で、大切なのはサイバー攻撃を受けたときにパニックになってどうしてよいか分からなくならないようにすることです。

IPAが公開している「中小企業の情報セキュリティ対策ガイドライン」では、問題が発生したことを想定してシナリオを作っておくことを薦めています。このガイドラインを読むことで、サイバーセキュリティに関するトラブルがの発生に「どう備えるか」ということに対するアイデアが得られるので、ぜひ一度目を通して、自分の会社や団体なりの対応マニュアルを作ってみて下さい。

警察庁サイバー犯罪対策プロジェクト	https://www.npa.go.jp/cyber/
各都道府県のサイバー犯罪相談窓口等	https://www.npa.go.jp/cyber/soudan.html

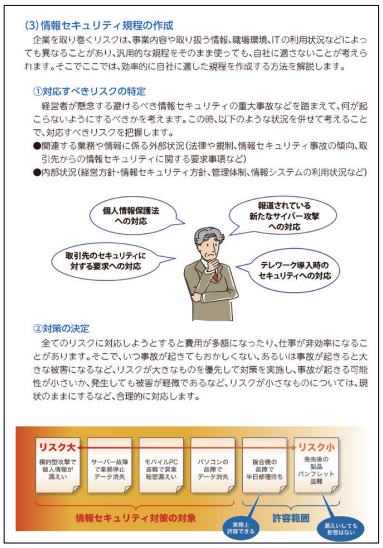
各都道府県警の、サイバー犯罪相談窓口の一覧。

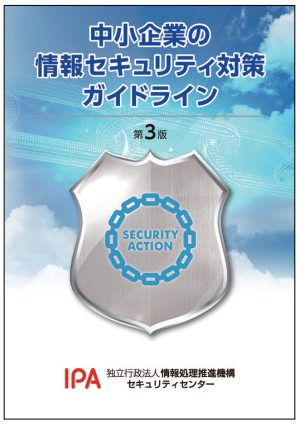
代表の電話番号の場合やサイバー犯罪相談等専用電話番号の場合もあるので、どの電話番号にかけているのかをよく確認しましょう。

ウェブサイト上のサイバー犯罪に関する情報は、表記されているアドレスだけでなく、他のページにも記載されている場合があります。

「中小企業の情報セキュリティ対策ガイドライン」

IPAによる「中小企業の情報セキュリティ対策ガイドライン」は小さな会社やNPOでも役立つ内容が記載されています。ぜひ手に取って役立つ部分を探してみましょう。





https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html

情報セキュリティ自社診断シートなどもあるので参考になります。

付録03 IPAが取り組むさまざまな中小企業向けセキュリティ対策支援

中小組織向け

1 中小企業の情報セキュリティ対策ガイドラインとは

IPA（独立行政法人情報処理推進機構）は誰もがITの恩恵を享受できるIT社会の実現を目指して、サイバーセキュリティ対策など各種の取組みを行っている経済産業省所管の政策実施機関です。

そのIPAが発行している「中小企業の情報セキュリティ対策ガイドライン」（以下「対策ガイドライン」）は、ITを何らかの形で経営に活用している中小企業であれば、必ず参照しておくべき指針です。

この対策ガイドラインは、中小企業の経営者に対し、対策の必要性に気づいてもらい、サイバーセキュリティ対策に全く取り組んでいない状態から、徐々にステップアップし、しっかりとした社内ルールと体制を作って組織的なサイバーセキュリティのマネジメント体制を構築する道筋を提供することを目的に編集されています。

ウェブサイトにおいてPDFの電子ファイル版で無償配布されている他、印刷版も有償で提供されています。

この対策ガイドラインの構成は、大きく本編と付録に分かれ、さらに本編は、第1部の「経営者編」と第2部の「実践編」で構成されています。

「経営者編」では、経営者がサイバーセキュリティの必要性を認識し、自らの責任で考え、実行しなければならない事項について説明されています。

対策を怠ることで企業が被る不利益や、経営者などが問われる法的な責任、社会的な責任などが、事例や主な関係法令の条項と処罰とともに説明されています。そして経営者が認識しておかなければならない「3原則」と、経営者自ら、または、従業員に指示して実行しなければならない「重要7項目の取組」が記述されています。

「実践編」では、具体的にどのように対策を進めていくかについて記述されています。

規模の小さな会社や、これまで十分なサイバーセキュリティ対策を実

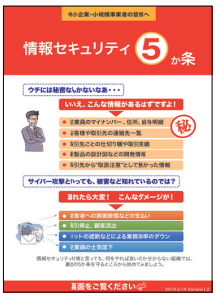
「中小企業の情報セキュリティ対策ガイドライン」とその付録

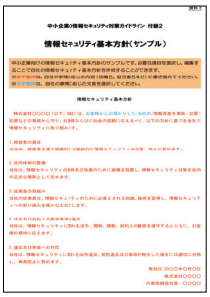
「中小企業のセキュリティ対策ガイドライン」には本編と、各企業が取り組まなければいけないチェック項目や、自社のセキュリティ資料を作るためのひな型、そしてクラウドの安全利用のための手引きが含まれます。

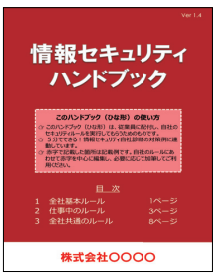
中段左から「情報セキュリティ対策5か条チラシ」、中段中「情報セキュリティ基本方針」のサンプル、中段右「5分でできる自社診断」、下段左「情報セキュリティハンドブック」のひな型、下段中「情報セキュリティ関連規程」のサンプル、そして下段左が「中小企業のためのクラウドサービス安全利用の手引き」となっています。

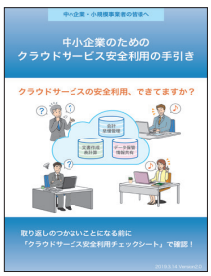
ひな形やサンプルは、文章中の項目を自社の組織や社員名に書き換えればすぐに使えるよう、作られています。

この他にやや専門的になりますが、EXCEL形式の「リスク分析シート」があります。









中小企業の情報セキュリティ対策ガイドライン	https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html

施してこなかった企業などでも、すぐにできることから開始して、ステップバイステップで、企業それぞれの事情に適した対策が実施できるように、進め方を説明しています。

中でも「情報セキュリティ5か条」は、対策ガイドライン実践編の冒頭で紹介しています。

この5か条は、まず取り組んでいただきたい基本的な対策を最小限にまとめられたものです。ぜひここから対策をスタートしてください。

こののち、実践編では、現状を知り改善するステップ、本格的に取り組むステップについて解説しています。

それぞれのステップは、中小企業の実態やサイバーセキュリティ対策のありかたを熟知している有識者により検討された内容となっています。

「付録」は実践編に取り組む際に使用するひな型やシート類です。構成は以下のとおりです。

- **情報セキュリティ対策5か条チラシ**
- **情報セキュリティ基本方針（サンプル）**
- **5分でできる自社診断**
- **情報セキュリティハンドブック（ひな形）**
- **情報セキュリティ関連規程（サンプル）**
- **中小企業のためのクラウドサービス安全利用の手引き**
- **リスク分析シート**

5分でできる自社診断の25項目

診断編

診断項目	No	診断内容	チェック：実施している	一部実施している	実施していない	わからない
Part 1 基本的対策	1	パソコンやスマホなど情報機器のOSやソフトウェアは常に最新の状態にしていますか？	4	2	0	−1
	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1 は最新の状態にしていますか？	4	2	0	−1
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	4	2	0	−1
	4	重要情報に対する適切なアクセス制限を行っていますか？	4	2	0	−1
	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	4	2	0	−1
Part 2 従業員としての対策	6	電子メールの添付ファイルや本文中のURLリンクを介したウイルス感染に気をつけていますか？	4	2	0	−1
	7	電子メールやFAXの宛先の送信ミスを防ぐ取り組みを実施していますか？	4	2	0	−1
	8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？	4	2	0	−1
	9	無線LANを安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？	4	2	0	−1
	10	インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をしていますか？	4	2	0	−1
	11	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？	4	2	0	−1
	12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？	4	2	0	−1
	13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？	4	2	0	−1
	14	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？	4	2	0	−1
	15	関係者以外の事務所への立ち入りを制限していますか？	4	2	0	−1
	16	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？	4	2	0	−1
	17	事務所が無人になる時の施錠忘れ対策を実施していますか？	4	2	0	−1
	18	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？	4	2	0	−1
Part 3 組織としての対策	19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？	4	2	0	−1
	20	従業員にセキュリティに関する教育や注意喚起を行なっていますか？	4	2	0	−1
	21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？	4	2	0	−1
	22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？	4	2	0	−1
	23	クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定していますか？	4	2	0	−1
	24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？	4	2	0	−1
	25	情報セキュリティ対策（上記1～24など）をルール化し、従業員に明示していますか？	4	2	0	−1

※1 コンピュータウイルスを検出するためのデータベースファイル「パターンファイル」とも呼ばれる
※2 重要情報とは営業秘密など事業に必要で組織にとって価値のある情報や顧客や従業員の個人情報など管理責任を伴う情報のことです

A 実施している の合計点	B 一部実施している の合計点	C わからない の合計点
点	点	マイナス(−) 点

診断の後は次ページ以降を読んで対策を検討してください。

3

A+B+C 合計	点

付録「5分でできる自社診断」の中にある、診断のための25項目。それぞれの項目に答えることで自社のセキュリティレベルが診断できます。

先々どういったセキュリティ項目を満たしていかないといけないか、というビジョンを持つためには目を通しておくとよいでしょう。

情報セキュリティ対策支援サイトでもオンラインで診断ができます。
https://security-shien.ipa.go.jp/learning/

これらのうち、「5分でできる自社診断」は、25問のチェック項目に回答することで自社の対策状況を把握することが出来るというものです。「基本的対策」、「従業員としての対策」及び「組織としての対策」という構成になっており、「基本的対策」は前述の「情報セキュリティ5か条」と同じになっています。

これに加え、「従業員としての対策」では、電子メール利用時や情報を格納した機器などの持ち出し、管理、バックアップなどの13項目、「組織としての対策」では、従業員教育や、取引先との契約時の秘密保持、

緊急時の体制整備、ルール化など7項目が設けられています。これら25項目により、サイバーセキュリティ対策の実施状況を点数化し100点満点でどの程度の達成状況か、また、どのような項目が弱点かを測ることができ、対策に取り組むうえでのポイントを見える化することが出来ます。

同じく、付録に収められている「情報セキュリティ基本方針」や「情報セキュリティ関連規程」のサンプルは、それぞれ、自社の状況や方針に沿って記述を選択、あるいは書き換えることで自社固有のものに仕上げることが可能です。また、「情報セキュリティハンドブック」(ひな型)は、社内ルールに合わせて書き換えができますので、従業員ひとりひとりへのルール徹底に役立ちます。

2 サイバーセキュリティ対策自己宣言「SECURITY ACTION」

「SECURITY ACTION(セキュリティアクション)」制度は、中小企業がサイバーセキュリティ対策に自発的に取り組むことを社の内外に宣言する制度です。

IPAの他、商工団体、中小企業に関係する士業団体などが連携して創設し、IPAが運用を行っています。

サイバーセキュリティ対策を始めたくても「なにをすればよいかわからない」、「経営者が重要性を認識してくれない」という中小企業の実態(IPAが実施した実態調査より)を踏まえ、まず何をすべきか、よりよくするために何をすべきか、ということを示し、実際に取り組んでいることを中小企業に自己宣言してもらおう、というのがこの制度の趣旨です。

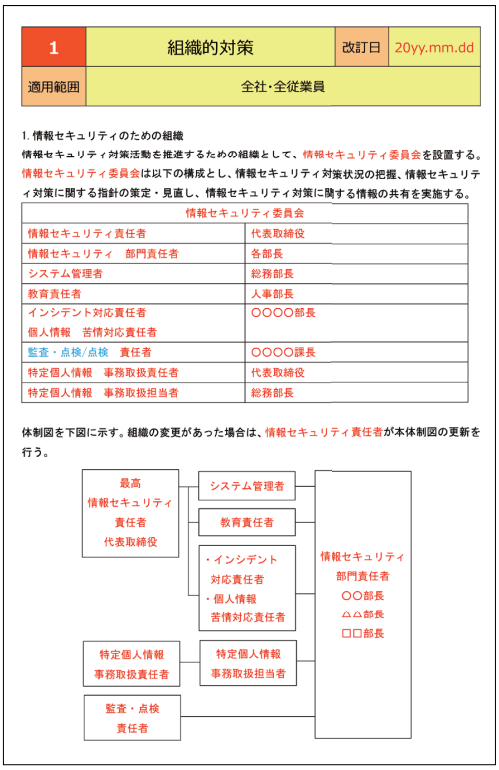
SECURITY ACTIONは、現在「一つ星」と「二つ星」の2段階があります。一つ星は「情報セキュリティ対策5か条」に取組むことを宣言するもの、二つ星は、「5分でできる自社診断」で自社の状況を把握するとともにサイバーセキュリティ基本方針を定めてウェブサイト上などで外部に示したことを宣言するものです。これらは、「中小企業向け情報セキュリティ対策ガイドライン」と同調しています。

この宣言をすることにより、社内意識の醸成、また、社外からは取組みを評価され、信頼の獲得と向上につながるなどの効果が期待できます。

まずはじめる、その一歩としてSECURITY ACTIONを宣言してはいかがでしょうか?

(執筆:IPA)

情報セキュリティ関連規程のサンプル



1	組織的対策	改訂日	20yy.mm.dd
適用範囲	全社・全従業員		

1. 情報セキュリティのための組織

情報セキュリティ対策活動を推進するための組織として、情報セキュリティ委員会を設置する。情報セキュリティ委員会は以下の構成とし、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。

情報セキュリティ委員会	
情報セキュリティ責任者	代表取締役
情報セキュリティ　部門責任者	各部長
システム管理者	総務部長
教育責任者	人事部長
インシデント対応責任者 個人情報　苦情対応責任者	○○○○部長
監査・点検/点検　責任者	○○○○課長
特定個人情報　事務取扱責任者	代表取締役
特定個人情報　事務取扱担当者	総務部長

体制図を下図に示す。組織の変更があった場合は、情報セキュリティ責任者が本体制図の更新を行う。

付録「情報セキュリティ関連規程」のサンプルの中の「組織内対策」のページ。

用意されたサンプルの中の赤字の部分を自社の情報に書き換えていくことで、自社の「情報セキュリティ関連規程」が完成するようになっています。

関連規程といってもなにを盛り込んでよいかわからないといったことが、このサンプルをなぞることで解決されます。

ウェブサイトに掲載するSECURITY ACTIONのマーク

セキュリティ対策自己宣言

セキュリティ対策自己宣言

SECURITY ACTIONの条件を満たした上で、これらのマークをウェブサイトに掲載することで、外部の企業などに対して自社のサイバーセキュリティに対する取り組みの「本気度」を示すことができます。

3 サイバーセキュリティお助け隊サービス

前述したガイドライン、「SECURITY ACTION」の内容を読めばセキュリティ対策の知識を深めることはできますが、実際にサイバー攻撃を防ぐための対策を講じると、費用面でも時間面でもコストがかかります。

人材・体制・資金などのリソースが限られている多くの中小企業にとって、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。

そんな中小企業の負担を軽減するためにも、IPAでは「サイバーセキュリティお助け隊サービス」を2021年度から運用しています。

IPAは2019年度、2020年度の時点から、中小企業への攻撃実態把握や中小企業向けのサイバーセキュリティ対策支援のしくみを構築するため、「サイバーセキュリティお助け隊実証事業」を実施し、この事業で得られた知見をもとに中小企業にとって不可欠なセキュリティサービスを示す「サイバーセキュリティお助け隊サービス基準」を制定しました。そしてこのサービス基準を充足する民間サービスには「サイバーセキュリティお助け隊マーク」を付与し普及を促進することで、多くの中小企業へ無理なくサイバーセキュリティ対策を導入・運用することを支援しています。

2023年1月時点で、「サイバーセキュリティお助け隊サービス」ではサービス基準を満たす20以上のセキュリティサービスが提供されています。

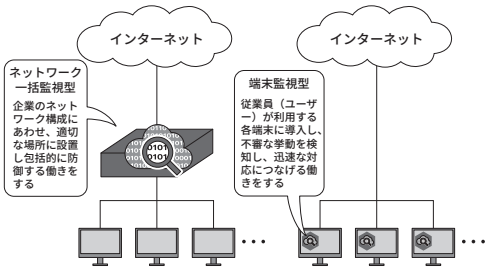
サービスの具体的内容は、

- 中小企業のサイバーセキュリティ対策を支援するための相談窓口
- UTM（Unified Threat Management・統合脅威管理）などのネットワークセキュリティ監視装置を用いたユーザーのネットワーク通信の異常を一括監視、またはEDR（Endpoint Detection and Response）などエンドポイントセキュリティソフトウェアを用いたユーザーの端末の異常を監視（両方が提供されるサービスもあり）
- サイバー攻撃発生時の初動対応（駆付け支援など）
- 被害に遭った際に備える簡易サイバー保険

などがあり、中小企業がサイバー攻撃への対処として不可欠なサービスを効果的、網羅的にカバーし、かつ安価に提供しています。

企業経営において省くことはできないセキュリティ対策に悩んでいる中小企業にとって、効果的なセキュリティサービスをワンパッケージで利用できるようになっています。

「サイバーセキュリティお助け隊サービス」における異常監視のしくみ

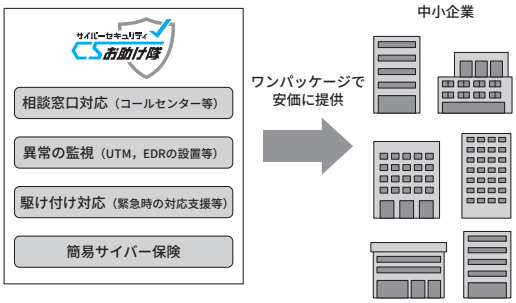


セキュリティ対策では、目に見えないサイバー攻撃を可視化し、侵入などの異常に早く気付くことがもっとも大切です。サイバーセキュリティお助け隊サービスでは、ネットワーク一括監視型、端末監視型、またはその両方（併用型）による異常の監視を提供しています。

「サイバーセキュリティお助け隊サービス」案内ページ

ユーザー向けサイト	https://www.ipa.go.jp/security/otasuketai-pr/
IPA案内ページ	https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html
概要説明資料（PDF）	https://www.ipa.go.jp/files/000100463.pdf

「サイバーセキュリティお助け隊サービス」で提供するサービス内容



中小企業がサイバー攻撃への対処として不可欠なサービスを効果的、網羅的にカバーし、かつ安価に提供しています。

付録04 中小企業がもっとクラウドサービスを利用しやすく！～認定情報処理支援機関（スマートSMEサポーター）

中小組織向け

認定情報処理支援機関（スマートSMEサポーター）とは、経済産業省の外局である中小企業庁が運営する、中小企業のIT活用を支援するITベンダーなどを中小企業等経営強化法に基づいて「情報処理支援機関」として認定する制度です。

近年、IT技術の進展や通信回線の高速化によって、サーバーなどの設備を持たなくてもソフトウェアの利用が可能なクラウドサービスの提供が増えてきました。

クラウドサービスは、設備やソフトウェアを購入する必要が無いため、初期導入コストが低く、しかも経営指導の専門家などとも情報共有がしやすく、クラウドサービス同士を組み合わせて活用することができるなど、中小企業にとっても数々のメリットがあります。

一方で、セキュリティ実装状況や保存したデータの取扱い条件などに関する情報提供が、クラウドサービスを提供するITベンダーによって異なり、中小企業にとっては分かりにくい部分がありました。

中小企業庁では、専門家との検討により、①クラウドサービスの安全・信頼性に関する情報、②セキュリティ対策状況、③利用者のサポート体制、④利用終了時のデータの取扱い、などの確認すべき項目を定めて、スマートSMEサポーターの認定申請時にITベンダーから申告させ、認定後には中小企業庁が特設サイトにて公開しています。

上記の項目の詳しい確認方法については、IPAが「中小企業のためのクラウドサービス安全利用の手引き（https://www.ipa.go.jp/files/000072150.pdf）」で解説していますので、参照下さい。

その他、同じくIPAが提供する「中小企業の情報セキュリティ対策ガイドライン（https://www.ipa.go.jp/security/keihatsu/sme/guideline/）」、「SECURITY ACTION セキュリティ対策自己宣言」（https://www.ipa.go.jp/security/security-action/）や経済産業省が提供する「中小企業のサイバーセキュリティ対策（https://www.meti.go.jp/policy/netsecurity/sme-guide.html）」も参考になります。

便利なITツールでも、利用者がデータを取り出せなかったり、セキュリティ対策がおろそかでは、安心して使い続けることができません。

スマートSMEサポーターとして公開されている情報を参考にして、クラウドサービスなどの中小企業にとって生産性向上に役立ち安全・安心に使えるITツールを上手に選んで活用しましょう。

●Smart SME Supporter 情報処理支援機関検索

https://smartsme.secure.force.com/smartsmesearch/

情報処理支援機関検索

情報処理支援機関として認定された、みなさんの生産性を高めるITツールを提供するITベンダーが検索出来ます。

本書ではコンテンツを作る業種を例に挙げましたが、この検索を用いることで、業種別、サービス別、そして地域別に、必要としているベンダーの情報を得ることが出来ます。

例えば、「東京都」で「飲食・サービス」業で、「予約」システムを提供してくれる会社を知りたい、というように検索します。

NISC関連ウェブサイト、SNS一覧

■ 内閣官房内閣サイバーセキュリティセンター(NISC)公式ウェブサイト

https://www.nisc.go.jp/
日本政府のサイバー政策の策定や政府機関へのサイバー攻撃の検知と調査を行っている機関。国民へのサイバーセキュリティ意識の啓発も行う。通称「NISC」。

■ みんなで使おうサイバーセキュリティ・ポータルサイト

https://security-portal.nisc.go.jp/
NISCが運営する、サイバーセキュリティ関連の情報を発信する普及啓発用サイト。本ハンドブックの配布も行っている。

NISCのSNSによる情報発信

■ Twitter
内閣サイバー(注意・警戒情報)

@nisc_forecast
フィッシング詐欺・マルウェアなどの注意喚起情報やソフトウェアの更新情報を発信している。

■ Twitter
公式アカウント

@cas_nisc
NISCの取組やサイバーセキュリティに関連する情報を発信している。

■ Facebook

https://www.facebook.com/nisc.jp/
NISCの活動の紹介や、サイバーセキュリティに関するお役立ち情報を原則1日1回、コラムの形で発信している。

■ LINE
セキュリティ関連情報

LINEID: @nisc-forecast
原則1日1回、サイバーセキュリティに関するお役立ち情報をコラム形式で発信している。

内閣官房内閣サイバーセキュリティセンター (NISC)ウェブサイト：https://www.nisc.go.jp/
NISC「みんなで使おうサイバーセキュリティ・ポータルサイト」：https://security-portal.nisc.go.jp/
内閣サイバーセキュリティセンター 公式Twitter: @cas_nisc
内閣サイバー（注意・警戒情報）Twitter:@nisc_forecast
内閣サイバーセキュリティセンター NISC LINE公式アカウント：@nisc-forecast
NISC Facebookページ: https://www.facebook.com/nisc.jp

インターネットの安全（あんぜん）・安心（あんしん）ハンドブック 中小組織向け 抜粋版

2023年3月1日　発行

内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

制作・著作　内閣官房　内閣サイバーセキュリティセンター (NISC)
協力　警察庁　総務省　経済産業省　独立行政法人情報処理推進機構(IPA)
改訂検討会メンバー：猪俣 敦夫（主査：大阪大学 教授）
宮本 久仁男（株式会社NTT データシステム技術本部 サイバーセキュリティ技術部 情報セキュリティ推進室 NTTDATA-CERT セキュリティマスター）
松下 孝太郎（東京情報大学 総合情報学部 総合情報学科 教授）
上沼 紫野（虎ノ門南法律事務所 弁護士　一般社団法人安心ネットづくり促進協議会 理事）
横山 尚人（独立行政法人情報処理推進機構（IPA）　セキュリティセンター　企画部　エキスパート）
酒井 啓悟（株式会社技術評論社 デジタル事業部）