はじめに

他人事ではない情報セキュリティ対策

ニュースなどで、よく「IT（Infomation Technology＝情報技術）」という言葉を見聞きします。ITとは、あらゆる情報をデジタル化してコンピュータによって処理する技術を指します。この言葉が一般に広まったのは、20世紀の終わりが近づき、21世紀という新しい時代が幕を開けようとする時期でした。当時、コンピュータの性能が飛躍的に向上し、安価で扱いやすいパソコンが爆発的に普及し始めていました。同じころ、一部の機関に限定されていたインターネットが一般に開放され、自宅に居ながらでも離れた場所からの情報収集やコミュニケーションが可能な通信環境が整いました。21世紀に入ると携帯電話とコンピュータが融合した「スマートフォン」が登場し、私たちはいつ、どこにいてもITの恩恵を受けられるようになりました。

こうした一連の変革は「IT革命」と呼ばれています。私たちの生活スタイルはIT革命により「それ以前のスタイル」が思い出せないほど激変しました。今ではショッピングや銀行の振り込みといった経済活動や、メールや会議などのビジネス活動、さらに家族や友人との気の置けない会話や写真・動画のやりとりまでもが、インターネットで行われます。そして2020年代では、オフィスへの通勤をなくし、会社の業務を自宅で行う「リモートワーク」というビジネススタイルも普及しつつあります。

しかしITは便利な生活をもたらす一方で、リスクもあります。仕事に関わる機密情報や自分の財産に関わる情報、プライベートな情報などを、すべてコンピュータで管理しなければなりません。これらの情報が盗まれたり破壊されたりするリスクは、インターネットに接続している限り消えることはありません。単なる不注意だけでなく、第三者による故意の攻撃や自然災害による偶然によっても発生します。1箇所から流出した情報が連鎖的な被害を生む可能性や、コンピュータが乗っ取られて自分が犯罪者に仕立て上げられる危険性など、IT社会ではあらゆるリスクと隣り合わせであり、アナログ情報が主体だった時代とは異なる注意が必要です。

情報セキュリティとは、パソコンやスマートフォンといったデジタル機器を安全・安心して使うための技術や取り組みです。IT社会におけるリスクを抑えるために、セキュリティ対策に意識を向ける必要があります。本書を読んでデジタル機器を扱う際に発生し得る危険性と、それに対する対策方法を具体的に理解し、実践しましょう。

※このテキストは2021年1月現在における法制度などに基づいて作成しています。

目次とスケジュール

それではテキスト学習に入ります。途中で投げ出したりしないために、計画を立ててから取り組みましょう。自分自身のペースに合わせて無理のない計画を立てましょう。１日２項目を学習するのが平均的なスケジュールです。

□は、診断で間違ったところやこれは特に重要だ、覚えておきたいという項目をチェックするために使いましょう。

目次とスケジュール

目次とスケジュール

目次とスケジュール

第1章～第10章

セキュリティ基礎知識編

なぜセキュリティ対策が必要なのか

学習のポイント

POINT 1 仕事や生活に便利なコンピュータは、犯罪者にとっても便利

POINT 2 家に鍵をかけるように、コンピュータにもセキュリティ対策を

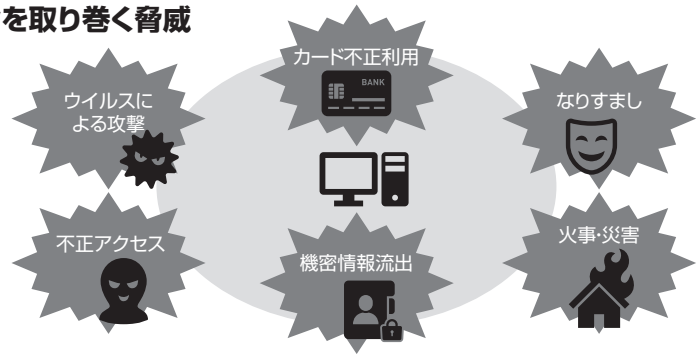
コンピュータやインターネットは、社会の至るところで利用されるインフラであるとともに、個人が日々の生活を送る上でも必要不可欠なものになっています。パソコンやスマートフォンといったコンピュータが仕事、プライベートの双方で当たり前のように使われるようになった現在、扱われるデータの重要性はますます増しています。

そしてこれらの全てのデータは、犯罪者のターゲットとなり得ます。犯罪者によってデータが破壊され、金銭が盗まれ、ときには犯罪の片棒を担がされることもあります。インターネットの普及で国境が取り払われ、誰もが世界中の犯罪者に狙われているのが現代です。そうした環境では「自分だけは大丈夫」といった安易な考えは禁物です。例えば、2019年における国内のサイバー犯罪の検挙件数は9,519件（警視庁「令和元年の犯罪情勢」）でしたが、これはあくまで検挙数にすぎず、背後にはその何十倍もの被害があるとされています。

攻撃だけが問題ではありません。パソコンを盗まれたり、自分のミスで大切なデータを消してしまったり、情報を流出させてしまったりすることも考えられます。さらには、災害や事故によってデータが失われることもあります。

こうした問題から身を守り、コンピュータや情報を安全に利用するために重要なのがセキュリティ対策です。セキュリティ対策は、何らかのツールを導入するだけで完了するわけではありません。発生するアクシデントは多岐にわたるので、特性に応じた検討が必要です。とはいえ、個人で意識するべきことはそれほど複雑ではありません。ソフトのインストールや機器の設定変更の他、少し意識を変えるだけで安全が守れるものもあります。家で戸締まりをして、もしものために保険に入るのと同様、誰もが取り組むべき安全対策が情報セキュリティです。どんな危険があり、どんな対策方法があるのかを知れば、より便利で安心した生活を実現できるのです。

パソコンを取り巻く脅威



1 セキュリティの重要性を認識する

情報セキュリティにおける3つの脅威

学習のポイント

POINT 1 技術的脅威・人的脅威・物理的脅威の3つがある

POINT 2 3つの脅威に合わせたセキュリティ対策が必要

デジタル機器を使うことで発生する脅威は、一般的に「技術的脅威」「人的脅威」「物理的脅威」の3つに分類されます。

1つ目の技術的脅威は、コンピュータウイルスに代表される、ソフトウェアなどのIT技術を使った脅威を指します。ウイルスへの感染が原因でパソコンの情報が盗まれる、データが破壊されるなどの被害が発生します。この他にWebサイトやパソコンへ第三者が不正に侵入して犯罪行為を行う「不正アクセス」、データやWebサイトの内容を書き換えてしまう「改ざん」など、多くの攻撃が存在します。

2つ目の人的脅威は、人間が原因となる脅威を指します。会社のパソコンを電車に置き忘れたり、紛失したり、メールの宛先を間違えたりといった誤操作、パソコンを盗み出される盗難や、不用意な発言で問題を起こす、いわゆる「炎上」も人的脅威に含まれます。

そして3つ目は物理的脅威です。これは火災や自然災害による破損、ハードウェアの故障、物理的な破壊といった脅威を指します。

セキュリティ対策は、これらの脅威から情報を守るための対策です。技術的脅威に対しては、それぞれの攻撃に合わせた防御技術が存在しており、そうした技術を導入します。人的脅威に対しては、従業員に対するルールの徹底や教育を通じたリテラシーの向上、また、管理者による従業員の監視などを行います。物理的脅威に対してはデータのバックアップ、盗難・破壊を防ぐための戸締まりや警備の強化といった対策を講じます。

企業と個人では対策の規模は異なりますが、基本的な考え方は変わりません。人間の心理的な隙を突いて企業の情報を盗む「ソーシャルエンジニアリング」などは、個人が脅威を知っておかなければ対策できません。単にセキュリティソフトを導入するだけでなく、どのような脅威が存在するかを知ることで、セキュリティへの意識をより高めていくことが大切です。

コンピュータの3つの脅威

技術的脅威	人的脅威	物理的脅威
・ウイルス ・不正アクセス ・フィッシング詐欺 ・なりすまし ・DoS攻撃 （大量のデータでコンピュータをパンクさせる攻撃）	・紛失・盗難 ・誤操作 ・炎上 ・ソーシャルエンジニアリング （人の行動や心理状態につけこんで情報を盗む行為）	・火事 ・地震 ・台風 ・故障 ・破壊 ・ソフトウェアのバグ

情報セキュリティの3要素「CIA」

学習のポイント

POINT 1 セキュリティ対策で考慮すべき3要素は「CIA」

POINT 2 3つの要素で対策すれば安全性は高まる

情報セキュリティに必要とされるポイントは、3つあるといわれています。それは「機密性」（Confidentiality）、「完全性」（Integrity）、「可用性」（Availability）のことで、頭文字を取って「CIA」と呼ばれています。

「機密性」は、許可された人しか情報にアクセスできないように制限することです。会員登録が必要なサービスではIDとパスワードでログインするのが一般的ですが、これも他人に使わせないための対策です。機密性を保ち、外部からの侵入を防ぐためのパスワード認証や、情報漏えいを防ぐためのデータの暗号化といった対策があります。

「完全性」は、不正な破壊、改ざん、消去などから資産を守り、最新の状態で保護することです。例えば病院で職員の操作ミスにより患者のデータが別の患者のものと入れ替わってしまったら、生死に関わる重大な問題が起こりかねません。完全性を保つためには、情報にアクセスできる人や端末を制限したり、操作の履歴を残すことで内部犯による不正な操作を抑止したりするなどの対策があります。

「可用性」は、端末やデータなどの資産がいつでも安全に利用できることです。パソコンがウイルスに感染して必要なデータにアクセスできずに業務がストップすることがないように、対策が必要なのです。可用性を保つためには、ウイルス感染を防ぐためにソフトウェアを最新の状態に更新したり、災害に備えて東京と大阪の2拠点でデータを二重にバックアップしたりといった対策があります。

個人レベルでもこの3つの観点を考慮したセキュリティ対策が効果的です。離席するときにはパソコンをロック（⊞+Lを押す）して第三者が操作できないようにする、自宅のWi-Fi（無線LAN）は暗号化の設定をする、重要なデータをクラウドストレージ（インターネット上にデータを保存するサービス）にバックアップするといったように、自宅でも「CIA」を意識して対策しましょう。

情報セキュリティの3要素「CIA」

機密性（Confidentiality）
・許可された人しかアクセスできないこと

完全性（Integrity）
・破壊・改ざん・消去されずに完全な状態であること

可用性（Availability）
・必要なときに必要な情報にアクセスできること

ノーガードでは済まされないセキュリティ

学習のポイント

POINT 1 セキュリティ対策を怠るとあらゆる脅威にさらされる

POINT 2 一つひとつの脅威ごとに対策を講じる必要がある

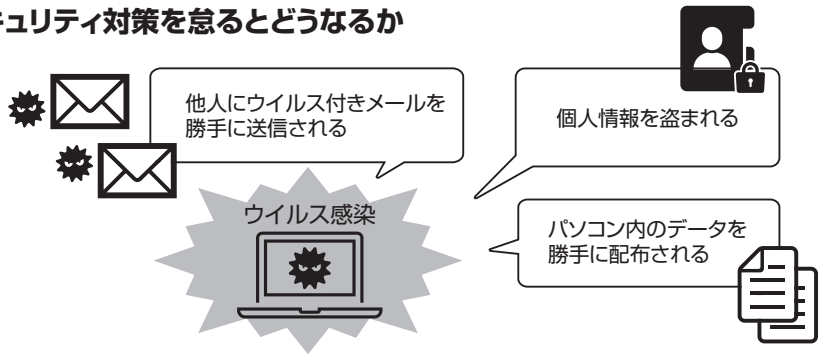
パソコンを使う上で欠かせないのがセキュリティ対策です。適切に対策することでパソコンの安全性が高まり、犯罪から守ることができます。逆に言えば、対策をしないと攻撃者に狙われやすくなるということです。実際にセキュリティ対策を怠ると、どのような被害に遭うのでしょうか。

セキュリティ対策をしていないパソコンとは、セキュリティソフトをインストールしなかったり、パソコンを最新の状態に更新していなかったりするものを指します。ほとんどのパソコンは、インターネットに繋ぐと知らないうちに「ポートスキャン」を受けます。これは攻撃の前段階といえる、攻撃者が弱点を持ったパソコン（ターゲット）をインターネット上で探す行為で、手当たり次第に行われます。ポートスキャンで被害が発生することはありませんが、もし弱点が見つかると、セキュリティ対策が行われていないパソコンではウイルスが送り込まれ感染したり、不正アクセスされたりしてしまいます。これによりパソコン内のデータを盗み出して外部に送信されたり、パソコン自体が乗っ取られてインターネットの掲示板に犯罪予告を書かれたり、勝手にウイルスメールを他人に送られたりする危険性があります。

また、パソコンはユーザーごとにパスワードを設定するのが基本ですが、これを怠ると誰でもパソコン内のデータにアクセスが可能になります。パソコンを共有して社内のユーザーのみ、家族のみしか使っていなくても、内部犯行で情報が流出したり、意図せずにデータを漏えいさせてしまう恐れがあります。さらにパソコンの紛失や盗難に遭えば、全てのデータが漏えいしかねないばかりか、大切なデータを永遠に失う可能性もあります。

何も対策しないと、パソコンは犯罪者の格好の標的となり、多大な損害を被ることになります。さまざまな攻撃があるため、一つひとつの脅威に合わせた対策が必要です。

セキュリティ対策を怠るとどうなるか



4
セキュリティの重要性を認識する

安全性とコストのバランス

学習のポイント

POINT 1 脅威に見合ったコストでセキュリティ対策を

POINT 2 面倒に感じないセキュリティ対策を

全ての脅威に完璧な対策をしようとすると、高額な投資が必要になり現実的ではありません。そのため、脅威を知った上で自分の環境に適した対策を行う必要があります。脅威には、技術的脅威、人的脅威、物理的脅威という3つの分類がありますが、それはそのまま対策にも通じます。

技術的対策は、セキュリティソフトを導入するなどの方法があります。Windowsパソコンであれば標準搭載されています。

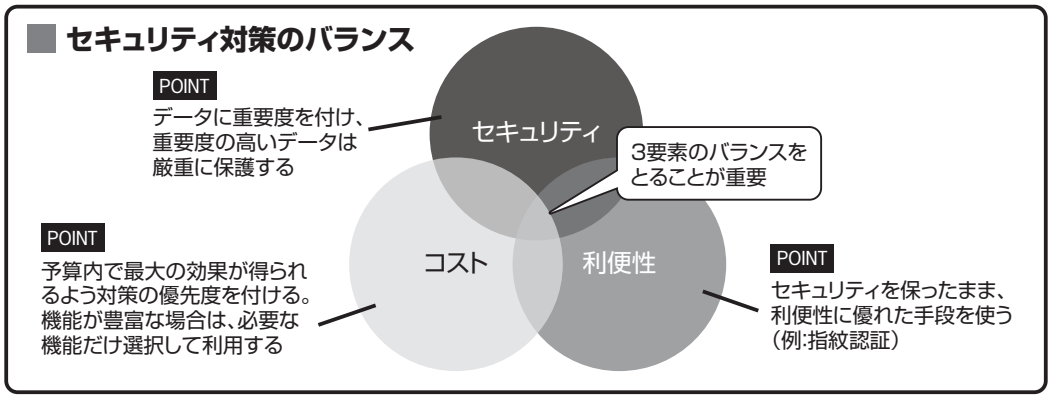
人的脅威への対策としては、家族や社員ごとに使用するパソコンを分け、個人がそれぞれID・パスワードを設定すれば、お互いのパソコンのデータは簡単に盗めません。基本ソフト（OS）標準の暗号化機能を使えば、万が一ハードディスクなどを盗まれても内容は読み取れません。

物理的脅威への対策としてはバックアップがあげられます。インターネット上にデータを保管する「クラウドストレージ」が便利ですが、全てのデータをバックアップするのはコストがかかるため、重要なファイルだけ保管すれば、コストを下げられます。

個人レベルでは、セキュリティソフトのようなツールを除くと、個人の素養に頼ったセキュリティ対策になりがちです。例えばWebサービスの会員登録でパスワードを決める際、サイトごとに異なるパスワードを設定するよう求められますが、サイトごとに全て覚えておくのは難しいでしょう。だからといって紙にメモして保存すると、盗難の危険性があります。その場合はパスワード管理ツールを導入すると効果的です。有料のツールが多いものの、年間数千円から導入できるため取り入れやすいでしょう。

セキュリティ対策のコストは金銭だけでなく、設定作業など人間の手間も重要です。つい利便性を高めるために安全性を下げてしまいがちなので、守るべきところ、ツールでカバーできるところを判断し、コストとのバランスを見たセキュリティ対策をしましょう。

セキュリティ対策のバランス



5
セキュリティの重要性を認識する

ラブレターにも注意――セキュリティ事件簿①

学習のポイント

POINT ❶ 人の心の隙を突くラブレターウイルス

POINT ❷ 正しい知識を持って慎重に対応すれば感染は防げる

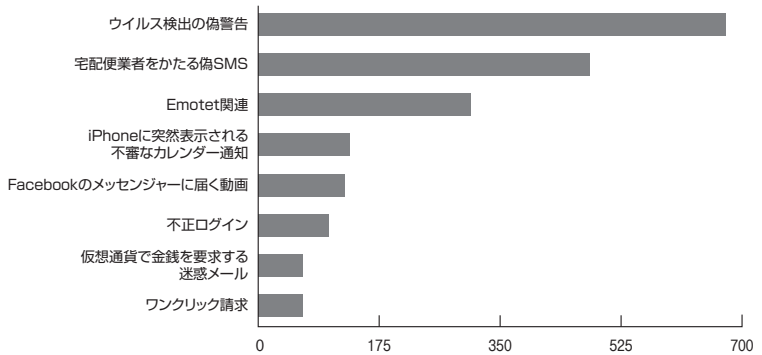
「ラブレターウイルス」と呼ばれるウイルスがあります。2000年にフィリピンに住む24歳の学生が作成した、最も有名なコンピュータウイルスの一つで、メールのタイトル（件名）が「I Love You」となっていることからこう呼ばれています。迷惑メールへの対処に不慣れな人が多かった時代、刺激的なタイトルに誘惑され、添付されている「LOVE-LETTER-FOR-YOU…」というファイルをクリックしたが最後、コンピュータウイルスに感染してしまうというものでした。

ウイルスに感染すると、パソコンに保存したファイルが破壊されます。さらにこのウイルスは、感染したパソコン内のメールソフト「Outlook」のアドレス帳に登録された全てのメールアドレス宛に、ウイルスを含むメールを送りつけるというやっかいな性質を持ち、感染が急速に拡大しました。その被害総額は少なく見積もっても50億ドル、多ければ100億ドルにのぼるとみられています。高度な技術が使用されたウイルスではなかったものの、メールがラブレターを装っていたことから興味本位で開いてしまうケースや、知らない送信元ではなく知人から届くメールのため、油断して引っかかる被害者が多くいました。

このように人の心理的な隙や行動のミスを突いて機密情報を入手したり、ウイルスに感染させたりする手口は、インターネットが普及し始めた時期から存在するポピュラーなもので、現在でもこうした被害が後を絶ちません。しかし、不審なURLはクリックしない、知らない送信元から届いたメールの添付ファイルは開かないなど、その多くは利用者が正しい知識を持って対応することで防げるものです。

「いつもと違う」「何かが変」と感じたときは、行動を起こす前に一呼吸置いて確認することが、コンピュータやインターネットを安全に活用する上で何よりも重要です。

情報セキュリティ安心相談窓口の相談件数



「情報セキュリティ安心相談窓口の相談状況[2020年第3四半期]」（情報処理推進機構）をもとに作成