基本のキ。セキュリティ入門（第1回）

情報を守る！セキュリティ対策の種類と重要性を紹介

2020.03.11

昨今、さまざまなセキュリティトラブルが世間をにぎわせていますが、このトラブルは誰の身にも起こり得るものです。セキュリティトラブルについて理解し、適切な対策を施さなければなりません。

今回は、気を付けたいセキュリティトラブルから、セキュリティ対策の重要性・具体的な対策について解説します。

よくあるセキュリティトラブルとは

セキュリティ対策を施すためには、具体的にどのようなセキュリティトラブルが存在するのかを知らなければなりません。ここでは、気を付けたいセキュリティトラブルの例と合わせて、情報処理推進機構（IPA）が報告する情報セキュリティ10大脅威についても解説します。

＜気を付けたいセキュリティトラブルの例＞
情報セキュリティトラブルとして、よくあるトラブルの例は次の通りです。

・ウイルス感染
・不正侵入
・情報漏えい
・災害による機器障害

2000年代前半までは、愉快犯的なウイルス感染が多く見られましたが、現在では個人や企業の金銭に関わる情報や、個人情報を搾取する目的のウイルス感染が多くなっています。

不正侵入を行うためにウイルス感染を足掛かりとし、情報漏えい事件に発展するケースは珍しくありません。現代においてはあらゆる情報に価値があり、攻撃者は価値ある情報を盗み出して悪用する目的でセキュリティトラブルを起こすため、十分気を付ける必要があります。

また、セキュリティトラブルは悪意のある第三者からの攻撃だけでなく、自然災害によっても引き起こされます。災害による機器障害が起これば、企業は多大な損失を被ることを覚えておきましょう。

＜IPAが報告する情報セキュリティ10大脅威＞
IPAが報告する「情報セキュリティ10大脅威2019」では、気を付けるべきセキュリティトラブルをランキング形式で紹介しています。その一部を見てみましょう。

順位	個人	組織
1位	クレジットカード情報の不正利用	標的型攻撃による被害
2位	フィッシングによる個人情報等の詐取	ビジネスメール詐欺による被害
3位	不正アプリによるスマートフォン利用者への被害	ランサムウエアによる被害
4位	メール等を使った脅迫・詐欺の手口による金銭要求	サプライチェーンの弱点を悪用した攻撃の高まり
5位	ネット上の誹謗・中傷・デマ	内部不正による情報漏えい

引用元:IPA（情報セキュリティ10大脅威2019）

ウイルス感染（マルウエア感染）や情報漏えい、不正利用に関するセキュリティトラブルが上位にランクインしているのが分かります。同データでは、昨年の順位も併せて紹介されています。セキュリティトラブルの手法は年々巧妙化し、順位が大きく変動しているものもあります。

このことからも、セキュリティ対策はただ施すだけでなく、セキュリティトラブルに合わせて常に対策し続ける必要性があることが分かります。

セキュリティ対策の必要性について

セキュリティトラブルの例を紹介しましたが、具体的にセキュリティ対策を施す必要性について、もう少し詳しく解説します。企業などの組織では情報セキュリティポリシーを策定することが重要であるため、情報セキュリティポリシーの概要についても紹介していきます。

＜セキュリティ対策の必要性＞
昨今、さまざまな情報がインターネットを介してやり取りできるようになりました。その中でも、金銭に関わる情報や個人情報は、第一に守らなければならない情報です。

銀行の口座情報やオンラインバンキングのログイン情報、氏名・住所・電話番号などの個人情報は、常に悪意のある第三者に狙われると考えてよいでしょう。もし、あなたがセキュリティ対策を施していないと、あなたの情報だけでなく、あなたの知人や友人・家族、顧客にまで影響が及ぶ可能性があります。セキュリティ対策は、あなた自身を守るためだけでなく、あなたの周りの人たちを守るためにも必要なのです。

＜企業のセキュリティ対策効果の高め方（情報セキュリティポリシー）＞
情報セキュリティポリシーとは、組織全体のルールや情報資産をどのように守るのかといった基本方針から、情報セキュリティを確保するための体制、運用規定、対策基準を具体的に示すものです。

組織全体の情報資産をセキュリティトラブルから守るために策定することが最大の目的で、さらに情報セキュリティポリシーの導入や運用を通じて、組織のセキュリティ対策意識の向上や取引先などからの信頼性を向上させる、といったメリットもあります。

このように、組織が実施する情報セキュリティ対策の方針や行動指針となるため、企業などの組織において情報セキュリティポリシーを策定することは非常に重要です。

安全性を高めるセキュリティ対策の方法5つ

「セキュリティ対策を施す」と一言で言っても、対策方法はさまざまあり、具体的にどのようなセキュリティ対策を施せばよいか分からない場合もあるでしょう。ここでは、誰でもすぐに対応できる簡単で基本的なセキュリティ対策の方法について解説します。

＜対策方法1:OSやソフトウエアを常に最新バージョンにする＞
OSやソフトウエアは、随時アップデートが行われています。機能や不具合の修正のためのアップデートだけでなく、セキュリティ対策のためのアップデートもあることを知っておきましょう。

OSやソフトウエアのバージョンが古いものは、セキュリティ的に弱い部分（脆弱性）があるため、常に最新バージョンに更新することが大切です。

＜対策方法2:パスワード・アクセス制限の徹底＞
パスワードはさまざまなシステムで利用するものですが、システムごとにパスワードを変更して、同一のパスワードを使い回さないようにしましょう。パスワードを使い回していると、どこかのシステムからあなたのパスワードが知られてしまった場合に、あなたが利用するシステムのパスワードが、芋づる式に盗み出されてしまうからです。

また、企業などの組織においては、特定のシステムへのアクセスに、制限がかけられていることが多いものです。システムへのアクセスを制限することによって情報漏えいリスクを減らします。

＜対策方法3:バックアップを取得する＞
コンピューターのデータを人質として金銭を要求する「ランサムウエア」に感染すると、データが利用できなくなります。場合によってはコンピューターの廃棄や、初期化が必要となり、不要な出費を強いられることになります。

ほかにも、災害による機器障害でもコンピューター内のデータが利用できなくなることが考えられますので、バックアップを取得することは非常に重要です。クラウド上にバックアップを取得したり、別のコンピューターにバックアップを取得したりと、方法はさまざまですので、一度検討してみてはいかがでしょうか。

＜対策方法4:機器の紛失防止＞
特に企業などの組織においては、オフィスへの人の出入りが多いため注意する必要がある項目です。ノートパソコンなどの小型のコンピューターは、簡単に持ち出せます。物理的に持ち出せないように、ワイヤーロックを利用しましょう。

スマートフォンであれば、GPS機能を使った紛失防止機能を利用したり、強固なロック機能を利用したりして、仮に紛失しても情報漏えいのリスクを減らせます。

＜対策方法5:セキュリティ対策ソフトウエアの導入＞
ここまで紹介した対策方法の中でも、セキュリティ対策ソフトウエアを導入することが最も重要です。セキュリティを専門に研究している企業・機関から販売されているソフトウエアであるため、セキュリティ対策をする際には欠かせない存在といえるでしょう。

セキュリティ対策ソフトウエアについては、次の項目でもう少し詳しく解説します。

セキュリティ対策ソフトウエアを導入しよう

セキュリティ対策を施す際、セキュリティ対策ソフトウエアを導入することは非常に重要です。ここでは、セキュリティ対策ソフトウエアの概要や機能、選ぶ際のポイントについて解説します。

＜セキュリティ対策ソフトウエアとは＞
一昔前までは「ウイルス対策ソフトウエア」と呼ばれており、主にウイルス対策を行うためのソフトウエアでした。しかし、セキュリティトラブルの手口の複雑化・巧妙化に伴い、現在ではセキュリティ対策全般を行うためのソフトウエアとなっています。

ウイルスを含むマルウエアの感染を防ぐだけでなく、あらゆるセキュリティトラブルを防ぐためのソフトウエアが、セキュリティ対策ソフトウエアです。

＜セキュリティ対策ソフトウエアの機能＞
現在のセキュリティ対策ソフトウエアの機能として、代表的なものをいくつか挙げます。
・マルウエア対策（ウイルス含む）
・スパム、ウイルスメール対策
・不正Webサイトブロック
・個人情報漏えい対策（プライバシー保護）
・ファイアウォール機能
など

現在では、ウイルスだけでなくトロイの木馬やワーム、スパイウエアなど多種多様の不正なソフトウエアが存在します。これら不正なソフトウエアを総称してマルウエアと呼びます。このマルウエアの感染経路は多様化しており、インターネット上からダウンロードして感染するケースもあれば、メールを介して感染する場合もあります。そういった予期せぬ感染を防いでくれる機能が、セキュリティ対策ソフトウエアにはあります。

そのほかにも、アクセスした人の情報を盗み取る目的で公開される不正Webサイトのブロックや、プライバシー保護機能、不正アクセスを防ぐ目的のファイアウォール機能などが搭載されています。

＜セキュリティ対策ソフトウエアを決めるときのポイント＞
セキュリティ対策ソフトウエアは多くの種類が存在しています。その中から、あなたに適したものを選ぶために、次の3つのポイントを参考にしてみてください。

1.動作速度
動作速度に関しては、快適にパソコンを利用できるかどうかに直結します。多くの機能を持つセキュリティ対策ソフトウエアは安全性が高まりますが、あなたのパソコンが古く、スペックが低い場合には、動作が重くなる可能性があります。その場合は、必要な機能だけを持つソフトウエアを選ぶとよいでしょう。

2.セキュリティ対策ソフトウエアの性能の基準
マルウエア対策性能に関しては、セキュリティ対策ソフトウエアごとに性能が異なるため、できるだけ性能が高いセキュリティ対策ソフトを選びましょう。マルウエア対策性能を評価する第三者機関がレポートを公開しており、セキュリティ対策ソフトウエアごとに性能の比較が可能です。

3.価格・サポートの基準
価格・サポート体制に関しては、予算の範囲の中でバランスを見て選ぶ必要があります。できるだけ出費を抑えたいところではありますが、セキュリティ対策ソフトウエアにかけるお金は必要経費と考え、最低限必要な対策が取れるようにしましょう。また、セキュリティ対策ソフトウエアを導入していても、次から次へと新たなトラブルが生まれてきます。ですから100%安全ということはありません。問題が発生した際に十分なサポートを受けたいのならば、サポートが充実したセキュリティ対策ソフトウエアを選択するべきでしょう。

＜Windows10はセキュリティ対策ソフトウエアが不要？＞
Windows10を利用している場合、標準でWindows Defenderと呼ばれるセキュリティ対策ソフトウエアがインストールされています。Windows Defenderがインストールされていれば、市販のセキュリティ対策ソフトウエアを導入する必要はないのでしょうか？

結論としては、別途、セキュリティ対策ソフトウエアを導入するべきです。なぜなら、Windows Defenderはセキュリティ対策機能が豊富だとは言えないためです。

セキュリティ対策ソフトウエアを販売する企業・機関は、セキュリティに関するプロです。セキュリティ対策ソフトウエアは、あらゆるセキュリティトラブルを想定して作られています。より強固なセキュリティ対策を求めるならば、市販のセキュリティ対策ソ

フトを導入するべきでしょう。

対策して当たり前！セキュリティ対策ソフトウエアは必ず導入しよう

セキュリティトラブルは、誰の身にも起こり得ます。セキュリティ対策を施すのが当たり前の時代です。

NTT西日本では、進化し続ける脅威に対して、セキュリティ対策を複合的に組み合わせた「セキュリティおまかせプラン」をご用意しています。このプランでは、ゲートウェイでの防御や、企業向けセキュリティ対策ツール、サポートセンターでの通信監視・復旧支援など、手厚いサポートで脅威から企業を守ります。

※本機能はセキュリティに対するすべての脅威への対応を保証するものではありません
※掲載している情報は、記事執筆時点のものです