事務所News
2025.5
K-069
発行 ： ふじわら税理士事務所　兵庫県高砂市神爪1丁目12番18号 高田ビル2F　Tel.079(433)0030　Fax.079(433)0020

経営バイタルの強化書 KEIEI VITAL

サイバーセキュリティに関する基本的な知識の整理と対策

インターネットの安全・安心ハンドブック Ver 5.10

サイバーセキュリティに関する基本的な知識を理解し、誰もが最低限実施しておくべき基本的なサイバーセキュリティ対策を実行することで、さらに安全・安心にインターネットを利活用することができます。

サイバーセキュリティに関する基本的な知識を整理しましょう!

1 インターネットの安全・安心ハンドブック Ver 5.10

内閣サイバーセキュリティセンター(NISC)は2025年3月11日、「インターネットの安全・安心ハンドブック Ver 5.10」を改訂・公開しました※。

「インターネットの安全・安心ハンドブック」は、企業、学校、家庭向けに「サイバーセキュリティに関する基本的な知識を紹介し、誰もが最低限実施しておくべき基本的なサイバーセキュリティ対策を実行してもらうことで、さらに安全・安心にインターネットを利活用してもらうことを目的に制作したもの」で、最新版のVer 5.10は、サイバー空間の最新動向や、今特に気を付けるべきポイント等を踏まえて改訂されました。

同ハンドブックは、PDF・ePUB版を無料でダウンロードでき、内容に改変を加えない範囲で自由に利用できます。また、全体版の他「一般利用者向け抜粋版」「中小企業等向け抜粋版」も公開されており、今回の改訂では、家庭や職場等で特に気を付けたいサイバー攻撃の手口や基本的なサイバーセキュリティ対策について、クイズやチェックリスト等を用いてわかりやすく記載したリーフレットが作成されています(一般利用者向け、中小企業等向け)。

情報セキュリティについての説明資料は、専門用語が多くわかりにくいものが多いですが、今回新たに作成されたリーフレットは、イラストを多く用い、16頁と読みやすい内容になっており、各頁にインターネットの安全・安心ハンドブックVer 5.10における参照箇所を記載しているので、必要に応じて、ハンドブックの内容を確認し、理解を深めるとよいでしょう。

2 インターネットの安全・安心ハンドブック Ver 5.10 (一般利用者向けリーフレット)

一般利用者向けのリーフレットは、学校(中高生、先生)や家庭(こどもからシニアまで)を対象に作成されており、「身の回りのリスクチェック」「あなたの情報を守りましょう」の大きく2つから構成されています。

「身の回りのリスクチェック」では、よく見受けられる下記8つのサイバー攻撃のリスクがあげられており、このうちの1つでも該当した場合には、「あなたの情報は狙われているかも!?」と対策の必要性がわかるようになっています。

●リスクチェック

①忘れないようにするため、パスワードは同じものを使っている。
②家庭のネットワーク機器のパスワードは初期パスワードから変更していない。
③スマホのアプリは気が向いたときにアップデートする。
④公衆Wi-Fiの利用先は無料かどうかで決めている。
⑤公衆Wi-Fiを利用するために個人情報を求められたら、気にせず入力している。
⑥電子メールを受信したら、必ずメールを開封するようにしている。
⑦料金未払いの督促のお知らせが来たら、メールに記載されているリンクにアクセスする。
⑧サイバー攻撃なんて、めったに起こらないことだと思う。

「あなたの情報を守りましょう」では、上記のリスクについて3つの対策を取る必要があることが説明されています。

●リスク対策

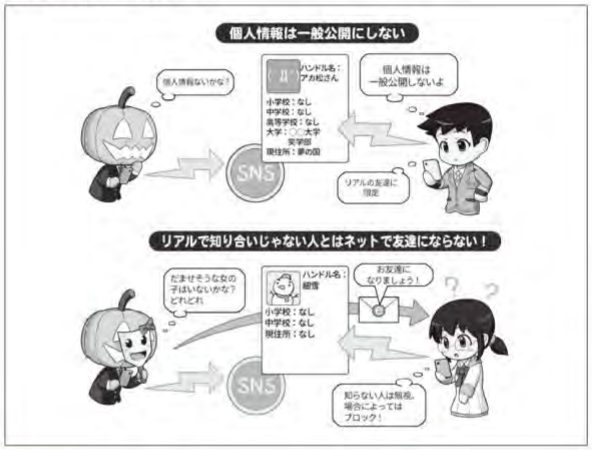
1. パスワードの適切な設定・管理(リスク①、②への対策)
2. スマホやPC、ネットワークを安全な状態にする(リスク③、④、⑤への対策)
3. 攻撃の手口を知り、被害を防ぐ(リスク⑥、⑦、⑧への対策)

また、「家族をサイバー攻撃から守るには」として、被害が増加しているフィッシング詐欺やSNSでの注意点が末尾に記載されており、困ったときの連絡先についても記載されています。

【図1】フィッシング詐欺の手口

裏面へ続く→

【図2】SNS利用の注意点



3 インターネットの安全・安心ハンドブック Ver 5.10（中小企業等向けリーフレット）

中小企業等向けのリーフレットは、中小企業・小規模事業者等を対象に作成されており、「経営層・情報管理者向け」と「従業員向け」の大きく2つから構成されています。

近年、中小企業等ではITの利活用が進む一方で、サイバー攻撃手法の巧妙化、悪質化などにより事業に悪影響を及ぼすリスクが高まってきています。

サイバー攻撃などによりシステムがダウンしたり、情報流出が発生した場合は、事業活動の停止、取引先からの信頼低下等、甚大な損害が発生することがあります。

税理士業務では申告・申請期限があり、月末等に上記のような障害が発生した場合や業務で扱っている特定個人情報や個人情報が流出してしまった場合は、大きな損害が発生します。

このリーフレットでは、「経営層・情報管理者」が行うべき社内体制等の整備と「全ての従業員」が行うべきIT機器やネットワークの安全な利用についてわかりやすく記載されており、巻末に簡単なテストも記載されていますので、一読することをお勧めします。

●「経営層・情報管理者」が行う社内体制等の整備

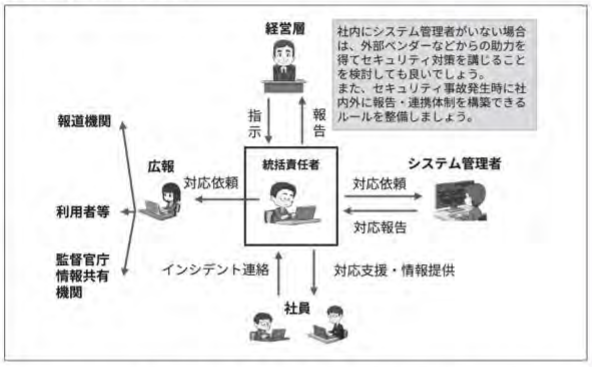
経営層・情報管理者が情報セキュリティの対応として、行うことは社内体制等の整備です。具体的には、下記4つの対応を行います。

①自社の情報資産の状況確認
②必要な体制や規程等の文書の整備
③従業員に必要な学習の機会の提供と訓練
④万が一の時の対応の整理と訓練

①**自社の情報資産の状況確認**では、自社のビジネスにおける損失や信頼の失墜等のリスクや、情報流出による法的責任に直面するリスクを避けるために、自社にどのような情報資産があるか情報資産の状況を確認します。情報資産には、ハードウェア、ソフトウェア、情報（顧客情報、技術情報等）そのもの等があり、重要度が変わってきます。費用の面からも全ての情報資産にリスク対策をすることは困難となるので、資産を重要度に応じて分類し、管理することが必要になります。

②**必要な体制や規程等の文書の整備**では、自社にある情報資産を守るため情報を取り扱う際のルールを整備し、権限の分散を図る体制を作ります。自社内に情報管理者がいない場合は、IT導入補助金等も活用しながら外部専門家と協力することも重要です。

【図3】社内体制の整備



③**従業員に必要な学習の機会の提供と訓練**では、自社にどのような重要な情報資産があるか、その情報資産はどのように取り扱いをするのか自社で取り決めてルールを従業員に周知することが必要になります。

業務で取り扱う情報資産は全て重要なものではありますが、全てを漏れなく管理することは困難であり、また、理解することも難しいため、このリーフレット等を活用して最も重要な情報資産を守るにはどうすればよいかから始め、徐々に従業員の意識を高めていくことも重要です。

④**万が一の時の対応の整理と訓練**では、事故やトラブルが発生した際の対応手順を予め作成しておき、災害等が発生した場合でも業務の継続ができるように対応をしておくことが必要となります。

●「全ての従業員」が行うIT機器やネットワークの安全な利用

全ての従業員が情報セキュリティの対応として、行うことは自社で利用するIT機器やネットワークの安全な利用です。

情報セキュリティの対策は誰か一人でもルールを守らなければ、そこから事故や情報流出が発生する原因となりかねないため、自社内で業務を行う方は非常勤役員やパート・アルバイト等も含めた全ての従業員が理解しておくことが必要となります。

全ての従業員がIT機器やネットワークを安全に利用するためには、基本的には一般利用者向けのリーフレットで記載されていた3つのリスク対策を行うことが必要になりますが、事業で利用する機器は家庭で利用する機器よりも一般的に多くなっており、また、取り扱う情報も重要性の高いものとなります。

このため、下記のような業務で利用している機器を全て最新（更新されている）状態にしておくことが必要となります。

【図4】業務で利用する機器の更新

●相談窓口と支援サービス

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、まずは社内の情報管理者に相談の上、必要に応じて各種窓口に相談することが重要です。障害に気付いた場合は機器の電源を落とさないままネットワークから切断し、なるべくわかる範囲で事象を記録しておくと障害からの復旧をスムーズに行うことができます。

※ インターネットの安全・安心ハンドブック（NISC）（URL：https://security-portal.nisc.go.jp/guidance/handbook.html）