中小企業・小規模事業者の皆様へ

情報セキュリティ6か条

ウチには秘密なんかないなあ・・・

いいえ、こんな情報があるはずですよ！

- 従業員のマイナンバー、住所、給与明細
- お客様や取引先の連絡先一覧
- 取引先ごとの仕切り額や取引実績
- 新製品の設計図などの開発情報
- 取引先から“取扱注意”として預かった情報

秘

サイバー攻撃といっても、被害など知れているのでは？

漏れたら大変！　こんなダメージが！

- 被害者への損害賠償などの支払い
- 取引停止、顧客流出
- ネットの遮断などによる業務効率のダウン
- 従業員の士気低下

情報セキュリティ対策と言っても、何をやれば良いのか分からない組織では、
裏面の6か条を守るところから始めてみましょう。

裏面をご覧ください

1 OSやソフトウェアは常に最新の状態にしよう！

OS やソフトウェアを古いまま放置していると、セキュリティ上の問題点が解決されず、それを悪用したウイルスに感染してしまう危険性があります。お使いの OS やソフトウェアには、修正プログラムを適用する、または最新版を利用するようにしましょう。

対策例

- ●WindowsUpdate（WindowsOSの場合）、ソフトウェア・アップデート（macOSの場合）などベンダの提供するサービスを実行する。
- ●Adobe Reader、ブラウザなど利用中のソフトウェアを最新版にする。
- ●利用中のソフトウェアに脆弱性が存在しないか、MyJVN バージョンチェッカ※で確認する。
- ●脆弱性が存在した場合は、手順に沿って修正パッチを適用する。
- ●サポートのあるOS、ソフトウェア、ネットワーク機器を利用する。

※パソコンにインストールされているソフトウェア製品が最新かどうかを簡単な操作で確認できるツール　https://jvndb.jvn.jp/apis/myjvn/

2 ウイルス対策ソフトを導入しよう！

ID・パスワードを盗んだり、遠隔操作を行ったり、ファイルを勝手に暗号化するウイルスが増えています。ウイルス対策ソフトを導入し、ウイルス定義ファイル※（パターンファイル）は常に最新の状態になるようにしましょう。

対策例

- ●パソコン等の情報機器にウイルス対策ソフトを導入し、ウイルス定義ファイルを最新の状態にする。
- ●ウイルス定義ファイルが自動更新されるように設定する。
- ●統合型のセキュリティ対策ソフトの導入を検討する。
- ●OSやアプリケーションに標準搭載されているセキュリティ機能を有効活用する。

※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

3 パスワードを強化しよう！

パスワードが推測や解析されたり、ウェブサービスから流出した ID・パスワードが悪用されたりすることで、不正にログインされる被害が増えています。パスワードは「長く」、「複雑に」、「使い回さない」ようにして強化しましょう。

対策例

- ●パスワードは10文字以上で「できるだけ長く」、大文字、小文字、数字、記号含めて「複雑に」、名前、電話番号、誕生日、簡単な英単語などは使わず、推測できないようにする。
- ●同じID・パスワードを複数サービス間で使い回さない。
- ●特にVPNや重要なシステムを利用する場合は、強固なパスワードを設定し、可能な場合は多段階認証、多要素認証、パスキーなどの認証強化機能を利用する。
- ●初期設定パスワードを見直す。

4 共有設定を見直そう！

データ保管などのウェブサービスやネットワーク接続した複合機の設定を間違ったために、無関係な人に情報を覗き見られるトラブルが増えています。無関係な人が、ウェブサービスや機器を使うことができるような設定になっていないことを確認しましょう。

対策例

- ●ウェブサービス、ネットワーク接続の複合機・カメラ、ハードディスク（NAS）などの共有範囲を限定する。
- ●従業員の異動や退職時には速やかに設定を変更（削除）する。
- ●使用するパソコン等は他者と共有しない。共有せざるを得ない場合は、別途ユーザーアカウントを作成する。
- ●外出先でフリーWi-Fiを使うときにはパソコンのファイル共有をオフにする。

5 バックアップを取ろう！

故障や誤操作、ウイルス感染などにより、パソコンやサーバーの中に保存したデータが消えたり、暗号化されたりしてしまうことがあります。事業が継続できるようバックアップを取得しておきましょう。

対策例

- ●重要情報のバックアップを定期的に行う。
- ●バックアップに使用する装置・媒体は、バックアップ時のみパソコンと接続する。
- ●バックアップの取得方法を決める。（オンラインバックアップの活用等）
- ●バックアップしたデータを安全な場所に保管する。
- ●バックアップしたデータを戻せるか定期的に確認する。

6 脅威や攻撃の手口を知ろう！

取引先や関係者と偽ってウイルス付のメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げたりして ID・パスワードを盗もうとする巧妙な手口が増えています。脅威や攻撃の手口を知って対策を取りましょう。

対策例

- ●IPAやNCO※などのセキュリティ専門機関のウェブサイトやメールマガジンで最新の脅威や攻撃の手口を知る。
- ●利用中のインターネットバンキングやウェブサービスなどが提供する注意喚起を確認する。
- ●管理者が従業員に適宜注意喚起し、従業員はセキュリティの懸念は速やかに報告する。

※参考：IPA 情報セキュリティ関連サイト　https://www.ipa.go.jp/security/guide/keihatsu.html
※参考：NCO 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.cyber.go.jp/

IPA 独立行政法人 情報処理推進機構 セキュリティセンター

IPA セキュリティセンターは誰もが安心、安全な頼れる「IT 社会」を目指して、国民の皆様に情報セキュリティに関する注意喚起や対策情報・対策手段の提供、届出制度や相談窓口を設けるなどセキュアな社会の整備に貢献するための活動を行っています。

URL　https://www.ipa.go.jp/security/

SECURITY ACTION
セキュリティ対策自己宣言

中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度です。「情報セキュリティ 6 か条」に取組むことを宣言することで、1段階目「一つ星」を使用することができます。

URL: https://www.ipa.go.jp/security/security-action/

2026.4 Version 1