

情報セキュリティ **5** 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



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生産効率のダウン
- 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5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 

情報セキュリティ 5 か条

1 OSやソフトウェアは常に最新の状態にしよう!

OSやソフトウェアのセキュリティ上の問題点を放置していると、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やソフトウェアに修正プログラムを適用する、もしくは最新版を利用しましょう。

対策例

- Windows Update(Windows OSの場合)/ソフトウェア・アップデート(Mac OSの場合) OSバージョンアップ(Android の場合)
- Adobe Flash Player/Adobe Reader/Java実行環境(JRE)など利用中のソフトウェアを最新版にする

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

- 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(ファイアウォールや脆弱性対策など統合的なセキュリティ機能を搭載したソフト)の導入を検討する

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窃取したID・パスワードが流用されることで、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

- パスワードは英数字記号含めて10文字以上にする
- 名前、電話番号、誕生日、簡単な英単語などはパスワードに使わない
- 同じID・パスワードをいろいろなウェブサービスで使い回さない

4 共有設定を見直そう!

データ保管などのクラウドサービスやネットワーク接続の複合機の設定を間違ったため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。クラウドサービスや機器は必要な人だけにのみ共有されるよう設定しましょう。

対策例

- クラウドサービスの共有範囲を限定する
- ネットワーク接続の複合機やカメラ、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設定の変更(削除)漏れがないように注意する

5 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とりましょう。

対策例

- IPA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クラウドサービスなどが提供する注意喚起を確認する



独立行政法人 情報処理推進機構
技術本部 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、国民の皆様に関心・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。

E-mail: isec-info@ipa.go.jp URL: <https://www.ipa.go.jp/security/>

! コンピュータウイルスに感染したと思ったら

IPA情報セキュリティ安心相談窓口

電話番号: 03-5978-7509 (平日10:00-12:00, 13:30-17:00)

! 更なる対策強化に取組みたいと思ったら

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/>