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、もしくは最新版を利用するようにしましょう。

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. セキュリティ製品を導入しよう!

ID・パスワードを盗む、遠隔操作を行う、勝手にファイルを暗号化するといったウイルスが増えています。悪意を持ってにネットワークに侵入し通信・サーバ機器全体を脅威にさらす行為を防ぎましょう。ウイルス対策ソフトやＵＴＭ*1を導入し、常に最新の状態にしましょう。

対策例

- ウイルス対策ソフトを導入しウイルス定義ファイルが自動更新されるようにする
- ＵＴＭ*1等を導入し多層防御する環境を構築し統合脅威管理を検討する

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」、「使いまわさない」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まわさない

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された機器の設定が初期状態のままであるために不適格な人に情報を除き見られるトラブルが増えています。権限のない人がウェブサービスや機器を使えないように設定しましょう。

対策例

- ウェブ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取りましょう。

対策例

- IPA*2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

*1 ＵＴＭ「Unified Threat Management」とは：統合脅威管理を実現するハードウェア製品です。コンピュータウイルスやハッキングなどの脅威からコンピュータネットワークを効率的かつ包括的に保護する管理手法を備え、ファイアウォール、VPN、アンチウイルス、不正侵入防御、コンテンツフィルタリング、アンチスパムなどの機能を1台で実現するセキュリティアプライアンス製品です。

*2 ＩＰＡ 独立行政法人 情報処理推進機構：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。
E-mail:isec-info@ipa.go.jp URL:https://www.ipa.go.jp/security/

DSK 株式会社 電算システム

2020.12.V01-2