情報セキュリティの脅威と対策②
(実務編・最新の脅威と中小企業者が取るべき対策)

独立行政法人　情報処理推進機構
セキュリティセンター　研究員
中小企業診断士
江島　将和

パソコンやスマートフォンを業務で利用される組合が増えています。スケジュール確認や組合員管理など業務効率が大幅に改善できる一方、セキュリティ対策を行うことも重要になってきます。そこで今回は、パソコンやスマートフォンで押さえるべきセキュリティ対策を5つのポイントに絞って解説します。

No.1 パソコン・スマートフォンについて

重要な情報を扱うパソコンやスマートフォンでトラブルが発生すると業務が出来なくなるだけでなく、場合によっては情報漏えいが発生して組合員にご迷惑をおかけすることもあります。コンピュータウイルスに感染したり、外部からの不正アクセスあるいは単なる故障によっても業務が停滞したりします。そのため、常日頃のメンテナンスやセキュリティ対策が重要となります。

■パソコンのセキュリティ対策
✓ウイルス対策ソフトを導入し、正しく運用する
✓ソフトウェアの脆弱性を解消する（Windows Updateの実行やソフトウェアパッチの適用）
✓No.2～5に挙げる運用上のセキュリティ対策を実施する

■スマートフォンのセキュリティ対策
✓スマートフォンを小さなパソコンと考え、パソコンと同様に管理する
✓勝手に使われないようスクリーンロックをかける
✓信頼できる場所（メーカー公式サイト等）からアプリをインストールする
✓アプリをインストールする際は、アクセス許可を確認する

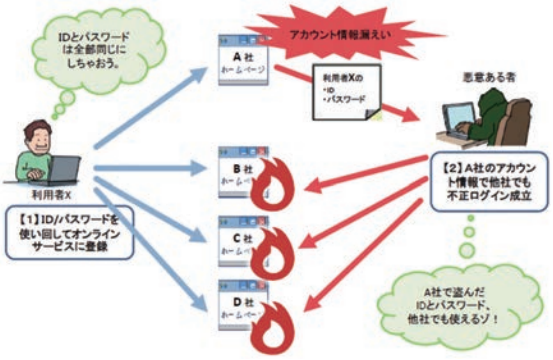
No.2　パスワードについて

パソコンやスマートフォンを利用しているとログインパスワードだけでなく、社内システムやインターネットサービスなどで多くのパスワードが必要になってきます。パスワードの重要性は理解されていると思いますが、安易なパスワード設定やパスワードの使いまわしなど、パスワードの運用･管理上危険な取り扱いを多く見受けます。

インターネットサービスを利用するためのパスワードが推察され、本人に成りすまして不正利用されてしまうといった被害が多く確認されています。成りすまし被害に遭わないようにするために、パスワードを安全に設定・管理しましょう。

■パスワード設定のポイント
✓他人に推測されやすいパスワード（名前や誕生日等）は使わない
✓大文字・小文字・数字・記号を組み合わせる
✓長いパスワード（推奨は8桁以上）
✓パスワードを使いまわさない

なお、最近はパスワードリスト攻撃の被害報道が続いています。パスワードリスト攻撃とは、インターネットサービス利用者の多くが複数サイトで同一のIDとパスワードを使い回している状況に目をつけ、不正取得したIDとパスワードのリストを流用し、連続自動入力プログラムなどを用いてIDとパスワードを入力しウェブサイトへのログインを試行する攻撃です。パスワードリスト攻撃の被害者にならないためにも、パスワードの使い回しを避けてインターネットサービス毎に異なるパスワードを設定するようにしましょう。



パスワードリスト攻撃による被害のイメージ図

No.3　クラウドサービスについて

クラウドサービスが注目を集めています。クラウドサービスをうまく活用すると、従来よりも少ない負担で IT を利用したり、ITのより高度な活用が図れたりする可能性があります。

一方で、自分でITシステムをコントロールできないことや、安易な設定ミスによりトラブルを招くことがあります。サービス内容や特徴をきちんと理解してサービスを安全に利用する術を身につけましょう。

■クラウドサービス利用のポイント
✓一般的契約条件やサービスの稼働率、障害発生頻度、障害時の回復目標時間等のサービスレベル（SLA）を確認する
✓パスワードの適切な設定を行う
✓サービス公開範囲等の適切な設定を行う
✓サービス停止や終了に備えて、重要情報を手元に確保しておく

No.4　電子メールについて

電子メールの宛先間違いによる情報漏えい事故が多発しています。間違って電子メールを受け取った人が良い人であれば問題にはならないかもしれませんが、宛先間違いされた本人にとってはあまり呑気なことはいってられません。やはり、これも情報漏えい事故となります。

普段から、そういったうっかりミス的な事態を起こしやすいと考えるならば、電子メールの宛先間違いを起こさないための工夫が必要でしょう。例えば、メールソフトには誤送信防止機能として、送信後、数秒以内なら送信を取り消すことができる設定ができるものがあります。宛先間違いや、入力ミスに気付いて取り消すことができるので利用を検討してみるのもよいでしょう。

■電子メールのセキュリティ対策のポイント
✓送信前に宛先と内容を再確認する
✓メールソフトのセキュリティ機能を活用する
✓重要な情報はメール本文ではなく、文書ファイルに記述し暗号化して添付ファイルとして送信する
✓身に覚えのない添付ファイルは開かない

No.5　バックアップについて

パソコンやスマートフォンは、壊れないと考えている方が多いようです。確かになかなか壊れません。でも、机の上から床に落下させたり、パソコンの前で飲んでいた飲み物をパソコンにかけてしまったり、耐用年数を過ぎてしまったハードディスク装置が異音をたてて止まってしまったとか、いろいろな原因で壊れることがあります。また、誤ってデータを消してしまったとか、別のデータで上書きしてしまったとか、うっかりミスや誤操作によって業務に必要なデータを消失させる可能性もあります。

『バックアップは最後の砦』と言える重要な対策です。OS標準のバックアップ機能を利用すれば無料で実施することが可能です。万が一の場合に備えて、バックアップを取るようにしましょう。

■バックアップのポイント
✓定期的なバックアップを実施する
✓戻す（リストア）ことができることを確認
✓バックアップ媒体からの情報漏えい（紛失・盗難）を防ぐ

なお、最近はランサムウェアというウイルスが増加傾向です。ランサムウェアとは、「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語で、ファイルを勝手に暗号化するなどパソコンに制限をかけ、その制限の解除と引き換えに金銭を要求するウイルスです。基本的に、ランサムウェアによって暗号化されたファイルは金銭を支払っても復元できません。やはり、重要なファイルは定期的にバックアップを取っておいた方が良いでしょう。

ファイルを暗号化した後に表示されるメッセージ例

情報セキュリティに関するさらに詳しい情報は以下のサイトでご確認ください。
https://www.ipa.go.jp/security/