Information System Department
情報通
2020.June　6月号
発　行：東京税理士会 情報システム部
題　字：神津　信一（四谷）
（税理士会員章の日輪と八重桜をイメージしています。）

情報セキュリティと事業継続
～最近のパソコントラブルの事例と対策～

エドコンサルティング株式会社　代表取締役／独立行政法人情報処理推進機構（IPA）研究員　江島　将和　氏

現在、私たちの業務にパソコンの使用は必要不可欠なものとなりました。しかしながら同時に、セキュリティや災害に関するトラブルが付き物です。実際に、突然のウイルス感染や災害に見舞われた場合、どのような被害が生じるでしょうか？
今回は、エドコンサルティング株式会社　代表取締役／独立行政法人情報処理推進機構（IPA）研究員の江島　将和氏に、このようなパソコントラブルの実例や、その事前対策方法についてご解説いただきました。

1．【事例１】ランサムウェア感染による業務停止

ある日、税理士A氏のもとに配送業者から不在通知メールが届きました。A氏がメール添付されていたファイルを開封すると、**デスクトップ上の文書ファイルや写真が次々と暗号化**されて開けなくなってしまい、更にはネットワーク接続された**サーバ１台とパソコン５台も次々暗号化**されてしまいました。そして突然、「暗号化を解除したければ仮想通貨を振り込んでください」といった旨のアラートが表示されました。

業務ができなくなって困ったA氏は、指示に従い約３万円の仮想通貨を振り込みましたが、暗号化は一向に解除されません。仕方がないのでパソコンを購入した事務機器販売店に相談したところ、**ランサムウェア（身代金要求型ウイルス）に感染**したことが分かりました。ランサムウェアに感染すると、お金を払っても暗号化が解けないことも多いらしく、結局パソコンのOSからソフトウェアまで全てを再インストールすることになり、**復旧作業で２日間の業務停止**となってしまいました。

【ランサムウェア感染画面例】

2．【事例２】洪水による業務停止

川沿いに事務所を構える税理士B氏。ある晩雨が降り続いて川が氾濫し、翌日事務所へ行くと**机の上まで浸水**していました。事務員と溜まった水を掻き出しましたが、書類もパソコンも水浸しになり、乾くのを待って電源を入れてみましたが全く動かないので、パソコンを購入した事務機器販売店に連絡しました。しかし事務機器販売店は同様の相談で**サポートがパンク状態、対応は数日待ち**との回答でした。

業務ができなくなって困ったB氏は、家電量販店でパソコンを購入し、ソフトウェアをインストール、必要なデータを書類から入力したり顧問先に送ってもらって、なんとか業務を再開しましたが、**１週間はまともに仕事ができません**でした。

3．2つの事例は他人事？

税理士事務所で起きた２つのトラブルを紹介しましたが、これらはあなたの事務所では発生しないと言えるでしょうか？

「うちはウイルス対策ソフトを入れているから大丈夫」と言う方もいますが、実はA氏のパソコンにもウイルス対策ソフトがインストールされていました。また、「うちの事務所は川沿いではないから洪水は大丈夫」と言う方もいますが、大地震で事務所が倒壊したり、パンデミック（感染症の世界的流行）で事務所へ行くことができなくなったりと、同様の想定外のトラブルに見舞われる可能性があります。このような事業継続を脅かす情報セキュリティ上の脅威にどのような対策を取っておけばよいのでしょうか。

4．税理士事務所に必要な情報セキュリティ対策

税理士業務を進めるうえでパソコンはなくてはならないツールになりました。パソコンをトラブルから守るために、まずは独立行政法人情報処理推進機構（IPA）が推奨する**「情報セキュリティ５か条」**を確実に実施しましょう。これは個人でも実施していただきたい最低限の対策です。

①OSやソフトウェアは常に最新の状態にしよう
毎月のWindows UpdateやOfficeソフト、Webブラウザ、PDFなどのソフトウェアの更新を怠らない
②ウイルス対策ソフトを導入しよう
ウイルス対策ソフトは必須！ウイルス定義ファイル（パターンファイル）は最新にする
③パスワードを強化しよう
パスワードは「長く」「複雑」にして、Webサービスなどで「使い回さない」ようにする
④共有設定を見直そう
無関係な人がWebサービスや機器を使えないようにするために、共有設定は必要最小限に絞る
⑤脅威や攻撃の手口を知ろう
脅威や攻撃の手口を知っておけば対策が打てる。公的機関のメルマガなどを購読する

さらに対策を強化する場合は、IPA**「５分でできる！情報セキュリティ自社診断」**に記載された25項目に取組みましょう。前述の５か条に加えて、電子メールやインターネットの利用、物理的な情報の持ち出しや保管、さらには従業員教育や取引先管理など組織として必要な対策が網羅的に挙げられています。このうち、事業継続のために取組んでいただきたいのが「バックアップ」と「事故への備え」です。

【参考】５分でできる！情報セキュリティ自社診断

バックアップのポイントは、**①データだけでなくシステム（OSやアプリケーション）のバックアップも取ること。**システムのバックアップをとっておけば、パソコンが故障しても迅速に復旧（リカバリー）をすることができます。**②バックアップは離れた場所に保管すること。**折角バックアップをとっていても、バックアップ対象のパソコンの近くに保管していると一緒に破壊・水没等の被害に遭ってしまいます。**③バックアップはネットワークから切り離しておくこと。**事例１のようなネットワーク越しに感染を拡大するウイルスも存在するため、普段はネットワークから切り離したところに保管しておくことが推奨されます。

事故への備えのポイントは、**①復旧の手順書を作成しておくこと。**トラブルが発生してから対処方法を考えたり、復旧手順を調べていると、復旧が遅れてしまいます。**②手順書通り実施できるかテスト（訓練）しておくこと。**システムやデータをいざ復旧してみようとすると、設定が間違っていてバックアップが取れておらず復旧ができなかったというケースがよくあります。

どんなに気をつけていても交通事故はなくなりません。同様に、パソコンに関わるトラブルも100%回避するということはできません。

可能な限りトラブルを避け、いざという時も事業を継続できるようにするためにも、事前の対策と事故への備えを行いましょう。