Joho System linkai
情報通
2017.June　6月号
発　行：東京税理士会 情報システム委員会
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。）

会計事務所ではセキュリティ対策とバックアップはどこまでやれば良いのか？

情報システム委員会委員　杉山　靖彦

5月13日頃から、Wanna Cryptorというランサムウェアによる世界規模の感染が続いていることは、ニュースでも報道されていましたので、ご存知の方も多いと思います。「続いています」というのは、一度配布されたウイルスは、感染したパソコンやサーバが世の中から1台も無くならない限り、いつまでも消滅しないためです。つまり、ほぼ永遠に無くならないのです。

大手ウイルス対策ソフトウェアのブログには、英国で医療機関のパソコンが感染したため急患の対応や手術ができなくなったとか、製造業の工場で操業が停止したといった被害が掲載されていたと聞いています。幸運なことに日本においては、深刻な被害報告はさほど耳にしていませんが、大手スーパーやメーカー、役所など、さまざまな箇所での感染は報告されています。

そこで今回は、会計事務所において、これらのセキュリティ対策とバックアップはどこまでやれば良いのか？ウイルスに感染したらどうしたら良いのか？ということをあらためて考えてみたいと思います。

1．ランサムウェア「Wanna Cryptor」とは？

今回大規模に感染が報告された「Wanna Cryptor」とは一体どんなウイルスかというと、ある特定の脆弱性のあるパソコンに感染し、そのパソコン内のデータを暗号化して、拡張子を「.wcry」に変換し、その暗号化を解除するために300米ドル相当のビットコインを要求するというマルウェアです。

しかもIPA（独立行政法人　情報処理推進機構）によると、このWanna Cryptorは、1台のパソコンにとどまるのではなく、同じネットワーク内のパソコンに同様の脆弱性がないかを探し、脆弱性を見つけた場合はその端末へ侵入。同じようにパソコンを感染させ、自身の活動領域を広げていくため、特に企業では被害が拡大する恐れがあります。

ちょっと専門用語が入りましたので少し解説をしますと、「マルウェア」とは、【悪意がある】という意味のマリシアス（malicious）＋ソフトウェアの造語であり、不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアの総称です。

そして、マルウェアの種類は、いろいろと分け方はあるとは思いますが、大きく分けると次の4つに分類されます。

マルウェアの分類	特　　徴
ウイルス	他のプログラムに寄生して、動作を妨げたり、有害な作用を及ぼす。感染機能や自己拡散機能を持つが、単独では実行したり、自己増殖をすることができない。
ワーム	単独で動作を妨げたり、有害な作用を及ぼす。また、単独で感染機能や自己拡散機能をもつ。
トロイの木馬	自らを有益なソフトウェアだと偽り、インストールや実行するよう仕向けるが、実際は侵入先で秘密裏に攻撃を行う。寄生や増殖活動は行わない。
スパイウェア	感染したパソコンの「ID、パスワード、クレジットカード、銀行口座」といった内部情報を外部に勝手に送信する。

一般的にはウイルス対策と言いますが、ウイルスはマルウェアの一種でしかありませんので、本来はマルウェア対策と言った方が良いのかもしれません。

そして、「ランサムウェア」とは、ファイルを勝手に暗号化し、読みとれない状態にした後に金銭を要求する（増殖活動をしますが）トロイの木馬型のマルウェアのことを言います。

2．Windows 10なら大丈夫？有償のウイルス対策ソフトを入れていれば大丈夫？

Wanna Cryptorの感染が騒がれている中、「Windows 10なら大丈夫らしいよ」というお話をされている、とある先生の言葉を耳にしました。

思わず「それは違います！」と言ってしまいました。サポートが終了しているWindows XPは感染しやすかったでしょうが、Windows 10を使っているユーザーは、脆弱性を補うWindows Updateを定期的に行う人が多かっただけであり、そうでなければ、どのOSであったとしても感染する可能性はあります。

ただ今回ばかりは、マイクロソフト社もWindows XPを対象とする脆弱性を補うプログラムも配布したようですので、現時点ではそのプログラムを実行したWindows XPでは、感染の可能性はなくなっているようではあります。

では定期的にWindows Updateを実行して、有償のウイルス対策ソフトを導入していればマルウェアに感染する可能性はないかというと、実はそんなに簡単ではありません。

と言うのも、マルウェアは日々変化、進化しており、次々と新しいマルウェアが配布されているからです。日々、新種のマルウェアを発見してはその対策を行っているウイルス対策ソフト会社でも知らない新種のマルウェアには、誰もが感染する可能性があります。そのため、極力、マルウェアに触れる可能性を減らすことが一番の対策となるわけです。

マルウェアの多くは、メールかwebサイト経由で感染をしますので、私的なメールは事務所のパソコンでやり取りさせない。特に怪しいメールは開かせないことを徹底すべきでしょう！あと、仕事用のパソコンではネットサーフィンをしないことを提案したいと思います。

3．マルウェアに感染したらどうしたら良いのか？

しかし、もし自分のパソコンが感染してしまった場合はどうしたら良いのでしょうか？既に対策が確立しているマルウェアであれば、ウイルス対策ソフトが自動的に駆除してくれます（実際は感染した場合の多くはこのパターンです）。

しかしながら、対策の立てられていない、自動的に駆除できないマルウェアに感染してしまった場合は、まず感染したパソコンをネットワークから切り離してください。その上で、OSから完全に消去、つまりハードディスクを初期化して、再インストールをし直すことが一番の駆除方法です。

もし、マルウェアに感染する前のバックアップがあれば、ハードディスクを初期化した後に、バックアップから復元すれば環境を素早く戻すことができることでしょう。一般的にはデータをバックアップするように言いますが、データのバックアップだけでは、パソコンの仕事でできるような元の環境に戻すのに相当時間が掛かってしまいます。ハードディスクのイメージを丸ごとバックアップしておくのが一番です。

パソコンが安くなった今であれば、環境を構築してある予備のパソコンを用意しておくのも良い方法だと思います。

4．マルウェア対策としてのバックアップ

皆さまはバックアップをどの程度行っていますか？作業中のExcelファイルが、入力していた会計データがどの程度壊れても大丈夫でしょうか？

1日でしょうか？1週間でしょうか？まさか1か月でしょうか？そんなにデータがなくなっても大丈夫な方がいるはずがありません。この1時間作業をしたExcelデータですら、なくなってしまったら頭に来たり、がっかりしたりしませんか？

そこで私の事務所では、お昼と夜に毎日サーバーデータのバックアップを取っています。つまり、最悪データがなくなってしまったとしても、半日前には戻れるということです。

また、クライアントパソコンのハードディスクのイメージも、丸ごと1週間に1回バックアップを取っています。これによって、ハードディスクが壊れてしまったとしても、ウイルスに感染してしまったとしても、1週間前までの環境には戻れるということになります。

バックアップは、やってやり過ぎることはありません。マルウェア対策としても、是非ともできる限りの定期的なバックアップ計画の導入をお勧めします。

【弊所のバックアッププラン】

事務所サーバ
- 会計データ、文書ファイル…
  お昼と夜にバックアップ→半日前までは戻れる。
- 環境…
  1週間に1回ハードディスクを丸ごとバックアップ→1週間前まで戻れる。

クライアント
- 個人データ…
  移動プロファイルを利用することによって、ログオフ時に自動的に個人の環境をサーバにバックアップ→前回ログオフ時までの環境に戻れる。
- 環境…
  1週間に1回ハードディスクを丸ごとバックアップ→1週間前まで戻れる。