テレワークを実施する皆様へ

2020 年 4 月 13 日

在宅勤務での家庭内 PC の取り扱いについて

一般社団法人コンピュータソフトウェア協会
セキュリティ委員会/Software ISAC

在宅勤務をする際に、ご家庭の PC で業務メールやファイルを取り扱うことがあります。その際、ご家庭の PC のセキュリティの確保が大変重要です。以下を遵守いただき、安心安全な在宅勤務の維持をお願いいたします。

1　マルウェア対策ソフトの設定

世界中のマルウェア（ウイルス、スパイウェアなどの悪意のあるプログラムの総称です）の 96%は一度だけ出現し、それ以降は利用されないというマイクロソフトの調査[1]があります。これはアンチウイルスソフトの検出を免れるための攻撃側の戦略で、本質的な機能は同じでも、ファイルを少し変えるなどして外見的に異なる「亜種」を大量に作るためのものです。亜種は、マルウェア作成プログラムによって自動的に作成され、電子メールなどに添付され送信されるため、攻撃側の負担はわずかで、マルウェア対策ソフトの検出を免れるには効果的な攻撃手法です。

1.1 マルウェア対策ソフトの更新を確認しましょう

これに対抗するには、アンチウイルスソフトの更新を 1 日 1 回以上行って、常に最新の状態に保つ＝最新の攻撃を防御する体制を整えることが重要です。自動更新やリアルタイムスキャンが ON になっていることを確認してください。

1.2 ドキュメントやピクチャーは昼休みにクィックスキャンしましょう

また、ドキュメントフォルダーやピクチャーフォルダーは 1 日 1 回、お昼休みを利用してクィックスキャンしてください。これによって、メールやチャットソフトでやり取りしたファイルに潜むマルウェアを検出できるかもしれません。データだけならスキャンの時間も短くて済みます。

1.3 週に一度、休日に完全スキャンの実施をお願いします

さらに、休日の PC を利用しない時間帯には、完全スキャンを実施しましょう。マルウェア対策ソフトの新しい定義ファイルで新たに発見される可能性があります。完全スキャンは、ハードディスクへの負担が多く、動作が遅くなるなどの弊害がありますが、休日ならば問題はないでしょう。完全スキャンを週に 1 度、確実に実施することで、システムの安全性は格段にアップします。

---

[1] https://msrc-blog.microsoft.com/2017/06/22/antivirus-evolved/

2　更新プログラムの適用し最新の状態を保つ

2.1　脆弱性を修正する更新プログラムは大変重要です、適用をお願いします

攻撃者が送り込んでくるマルウェアは、システムの脆弱性を利用してシステムに侵入し、管理者権限へ昇格し PC を乗っ取ることを最初の目的にしています。管理者権限が取得できれば、OS やアプリケーションのあらゆる機能設定が行え、データも自由に読み書きできるからです。もちろん、こうしたマルウェアの動作の多くは、アンチウイルスソフトによって検出・防御されますが、脆弱性を利用した侵入に対しては防御が困難なケースも存在します。従って、脆弱性を修正する更新プログラムの適用は大変重要です。最新のマルウェアでも、数年前に公表された脆弱性を利用するものがあります。つまり、攻撃者は管理されていない更新プログラムを適用していない PC を狙っているのです。最新にすることが安全につながります。

2.2　ブラウザ、Office、Acrobat、Java、スマフォ、ご自宅のルーターもお忘れなく

脆弱性は OS だけではありません。ご利用中の Chrome、Edge、FireFox、Safari、Office、Acrobat、Java、Flash、Thunderbird などのアプリケーションの更新プログラムもチェックしてください。スマートフォンやタブレットも更新プログラムの適用が必要です。また、ご自宅のルーターや無線 LAN 機器のファームウェアも更新プログラムが公表されていることがあります。メーカーのホームページをチェックしてみてください。

3　Windows 10 は Windows8.1 に比べてはるかに堅牢です

3.1　Windows 8.1 ユーザー様へ

Windows8.1 以前の OS はマルウェアの侵入をいかに防ぐかという考え方で作れられていますが、Windows 10 は侵入を防ぎつつ、万一、マルウェアに侵入されても攻撃を成功させない緩和機能が搭載されており、Windows 8.1 に比べてはるかに安全な OS ということがいえます。もし、Windows 8.1 の PC を使用中であるならば、Windows 10 PC への移行を検討してください。

3.2　Windows 7 PC を保有されている方へ

Windows 7 はすでにセキュリティサポートが終了していることから、現時点で Windows 7 を運用すること自体、大変危険です。在宅勤務では Windows 7 PC を絶対に使用せず、スマートフォンで代替してください。この場合、スマートフォンも PC 同様に更新プログラムの適用を必ずお願いします。

4　重要情報資産の暗号化

4.1　個人情報や顧客データは必ず暗号化しましょう

企業の情報資産の漏洩を防ぐためには、様々な対策が必要ですが、最も簡単な防御方法は情報資産を確実に暗号化することです。これによって、たとえ情報資産が漏洩しても復号化ができない、または膨大な手間がかかることから、攻撃側のメリットがなくなります。また、顧客や取引先に対しても、データは流出したが、実際の情報は漏洩の可能性は極めて低い、という説明ができます。

4.2 Office ならばパスワード設定、テキストファイルや CSV なら Zip 暗号化で

個人情報や重要情報資産が入った Excel、Word、PowerPoint、PDF ファイルは、推測困難で総当たり攻撃が困難な、覚えやすい長いパスフレーズ（次項をご参照ください）を設定しましょう。

Office： [ファイル]>[情報]>[文書の保護]>[パスワードを使用して暗号化]

Acrobat: [ファイル]>[パスワードを使用して保護]

7zip： [圧縮]>[暗号化]

5 長いパスフレーズの勧め

5.1 総当たり攻撃

暗号化された Office 文書のパスワードを取得するために、総当たり攻撃という攻撃手法があります。ありとあらゆる組み合わせを試行しログオンしようというものです。では、この総当たり攻撃に対するパスワードの強さを考えてみましょう。

8 桁の大文字・小文字・記号・数字の入った「複雑なパスワードパスフレーズの例：

sakamotoryouma_to_katsukaishuu 30 桁（坂本龍馬_と_勝海舟）

miyamotomusashi-to-sasakikojirou 32 桁（宮本武蔵-と-佐々木小次郎）

パスフレーズは記号や大文字、小文字を混ぜる必要はありません。重要なのは長さです。また、作成者名や企業名などの推測しやすいキーワードを含めないことで、攻撃が困難になります。

また、電子メールにファイルを添付する場合は、別途、電子メールでパスワードを連絡せず、電話、FAX、SMS などの他の経路で送信することで、格段に安全性が高まりますし、万一、Office 文書などが漏洩しても、解析は困難という事が正しく説明できます。

5.2 長いパスフレーズでも漏洩したらアウトです、だから使いまわしは禁止！

安心なパスフレーズも、Web サイトから漏洩してしまえば、安心とはいえません。従って、同じパスフレーズを（業務/プライベートを問わず）使いまわすことは絶対にやめましょう。でも、クラウド化が進んでいろんなサイトにアクセスしなければなりませんね。

Dropbox の場合： xobpord-miyamotomusashi-to-sasakikojirou （サイト名をさかさまに）

miyamotomusashi-to-sasakikojirou-Dbox （サイト名を省略）

Office365 の場合： 563ecffo-miyamotomusashi-to-sasakikojirou

miyamotomusashi-to-sasakikojirou-Of3

サイトごとに自分の好きなルールでサイト略称をパスフレーズに付与すれば、そのサイトからパスフレーズが漏洩しても、他のサイトへのログインできません。これで、使いまわし対策もできました。ただし、ルールを部門や組織で統一すると、それが脆弱性になる可能性があります。ルールはご自身で考えてみてください。

5.3 私のパスワードは漏れていない？

過去、多くの Web サイトが攻撃され、ID、電子メールアドレス、パスワードが漏洩しました。そして、漏洩した ID、電子メールアドレス、パスワードが売買され、もしくは、公開されています。過去最大の漏洩は 11 億 6000 万の一意の電子メールアドレスとパスワードのセットといわれています。これらの漏洩したパスワードの一部を入手し分析を進めていますが、明らかに日本人の姓、名と思われるものや、国産のブランドや企業名、都道府県、政令指定都市が多数検出されています。

漏洩したパスワードを使い続けることは非常に危険です。そこで、電子メールアドレスやパスワードの漏洩を判定してくれるサイトをご紹介します。電子メールアドレスを入力するだけで、漏洩を判別できます。

https://haveibeenpwned.com/

漏洩していなければ Good news — no pwnage found! と表示されます。もしも、Oh no — pwned! と表示されたら漏洩した Web サイトが表示されますので、至急、パスワードを変更してください。ご家族のアドレスもご確認ください。

6 電子メールに添付された Office 文書、PDF 文書の取り扱い

マルウェアの侵入経路の大半は、電子メールに悪意のあるマクロプログラムを仕込んだ Office 文書や PDF 文書を添付するものです。また、電子メールに偽のリンクを貼って悪意のある Web サイトに誘導する方法もよく使われます。従って、本当に信頼できる相手方以外からの添付ファイルや、Web リンクを開かなければ被害にあうことはありません。

6.1 言葉巧みに騙しにきます

ところが攻撃者は、「至急」、「調査協力のお願い」、「アカウントが停止されます」などと言葉巧みにファイルを開かせようとしたり、リンクをクリックさせようとします。また、何回かメールでやり取りを行い、相手を信頼させたところで悪意のある Office 文書や PDF 文書を送り付け、侵入を試みるケースもあります。これらは、ソーシャルエンジニアリングと呼ばれる攻撃手法です。また、Emotet と呼ばれるマルウェアは、電子メールのアドレス帳のデータを窃取し、組織内の人になりすまして電子メールを送信してきます。

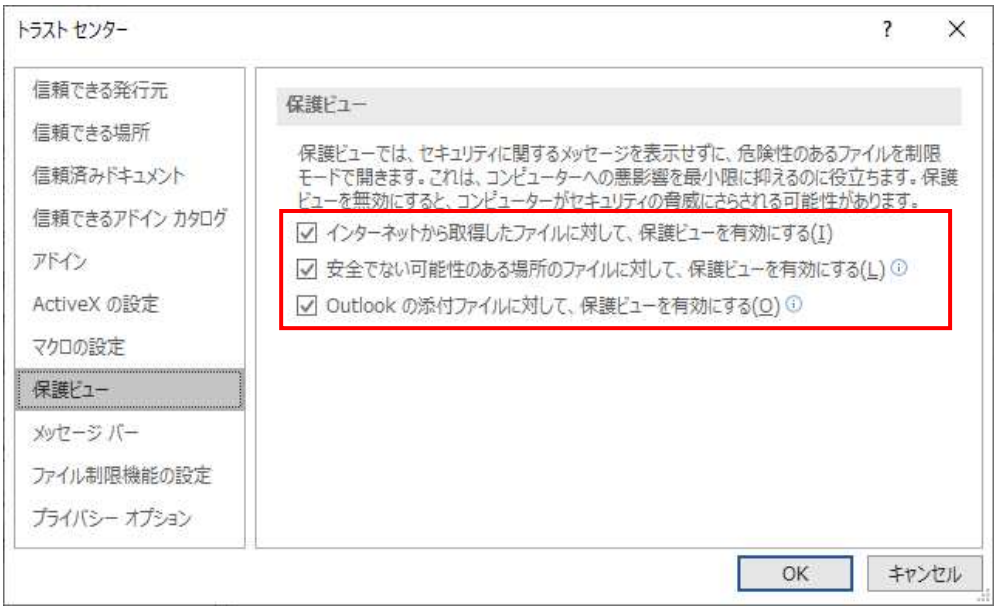
6.2 保護されたビューで対抗

このような攻撃の防御に有効なのが「保護されたビュー」です。「保護されたビュー」は、悪意のあるマクロプログラムを実行せずに、文書を閲覧することができます。一方で、「保護されたビュー」では印刷や編集をすることはできません。従って、まず「保護されたビュー」で内容を確認し、信頼できると確信に至ったら編集や印刷を行って下さい。マルウェアの侵入口は電子メールです。もし、迷った場合は、電話かメールでメールの送信元に確認するのが良いでしょう。

ぜひ、「保護されたビュー」の設定が正しくされているか、ご家庭の PC の設定を確認してください。

6.3 Word、Excel、PowerPoint 共通

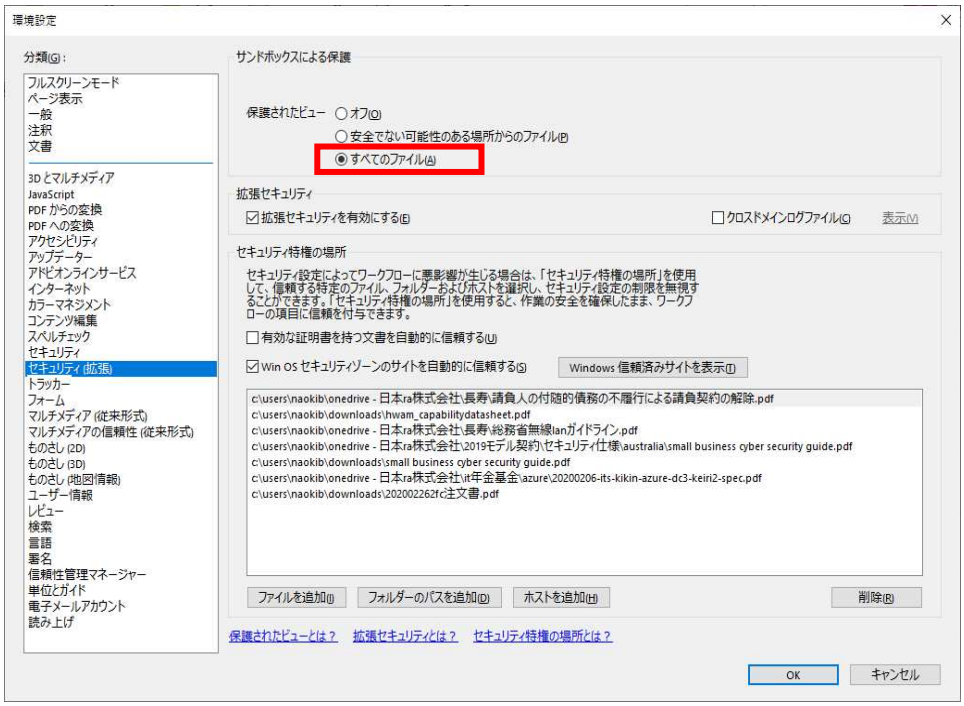
[ファイル]をクリックします。次に[オプション]をクリックします。続いて、[トラストセンター]>[トラストセンターの設定]>[保護ビュー] の順にクリックします。



赤枠の 3 つの項目にチェックボックスが入っていることを確認して[OK]をクリックしてください。

6.4 Acrobat Reader

[編集]>[環境設定]をクリックします。[カテゴリー]>[セキュリティ(拡張)]をクリックします。[サンドボックスによる保護]で[保護されたビュー]のオプションから[すべて]をクリックし、[OK]をクリックします。



7 License

以上