こんにちは。山田花子です。

新型コロナウイルス感染症の収束の見通しがたたない現状、中小企業においても、経理スタッフも含め、従業員の方のテレワーク（在宅勤務）が、進んできているようです。テレワークには様々な利用環境がありますが、代表的なものは、自宅のパソコン等を用いて リモートデスクトップや仮想デスクトップで社内での業務用端末と同じ利用環境（テレワーク環境）を実現する方法ですが、かたやそういった本格的な環境が提供されていない状況で、在宅勤務を実施している場合もあると思われます。今回はそのような場合、つまり、**法人等からテレワーク環境が提供されておらず、家庭で個人所有のパソコン等を使用して自宅にて勤務を行う場合におけるセキュリティ上の注意事項**をみていきたいと思います。

セキュリティは、個人情報を含めた法人等の大事な情報が、外部に流出したり、壊れたり消失してしまったりすることの防止が目的ですが、多様で多岐にわたり、専門的にもなりますので、今回は**最低限必要と考えられる点に絞ってみていきたいと思います。**

本格的なテレワーク環境が提供されておらず、自宅のパソコンや個人のスマホなどで業務に関わるメールの送受信や資料作成等を行う場合には、自身によるセキュリティ対策を強く意識する必要があります。自分は IT に詳しくない、相談できる人がいない等の状況にある方は、**普段使っている個人の環境のセキュリティ対策を見直すことから始めて下さい。そのために、以下の項目を確認し、実施しましょう。**

1. 紙の資料やファイル等のデジタルデータの紛失や情報流出の防止

法人等の事務所から紙の資料を持ち出す際の電車の車内等への置忘れや、郵送の途上での誤配や紛失を防止して下さい。郵送の際は書留や宅急便等の使用を検討しましょう。ファイル等のデジタルデータを格納した USB メモリの紛失も同様です。 自宅のパソコン等に格納したファイルも誤操作による削除や上書きにより消失してしまいますし、パソコン外への定期的なバックアップをしておかないと、パソコン本体が壊れた際にデータも消失してしまいます。メール添付等でファイルを送付する際は、必要に応じ、盗聴を防止するための開封パスワードの設定や暗号化を検討して下さい。開封パスワードを設定した場合、パスワードを伝えるメールは、添付ファイルを送るメールと別にすると安全です。

2. 業務用のユーザーアカウントの作成と不要なソフトウエアの不使用

テレワークでは、できる限り、私用や子供などの使っているパソコン等は使わず、別のパソコンの使用が望ましいところですが、同じパソコンを使わざるを得ない場合は、業務用のユーザーアカウントを別途作成しましょう。最近のパソコンでは、アカウントを設定し、1 台のパソコンを、使う人それぞれの専用のパソコンのようにして使用することができます。新しいユーザーアカウントを作る方法を説明しているサイトは多数あります。（例えば、「windows10 でユーザーアカウントを追加する方法を解説！」 https://samemai.com/entry/win_account_puls/ ）この解説にあるように、新しいアカウントの作成には、いろいろ選択肢がありますが、とりあえず、ローカルアカウント、その他のユーザー、管理者としての設定でよいと思われます。なお、作成した業務用のユーザーアカウントでは、テレワークの業務に必要なソフトウエアだけをインストールし、不要なソフトウエアはインストールしないようにしましょう。

3. 修正プログラムの適用

利用するパソコン、スマートフォン等の OS（オペレーティングシステム）や各種ソフトウェアに修正プログラムをこまめに適用し、最新のバージョンに更新して下さい。 WindowsXP や Windows7を使用しているパソコンは使用しないようにしましょう。

4. セキュリティソフトの導入および定義ファイルの最新化

利用するパソコン、スマートフォン等にセキュリティソフトを導入するとともに、セキュリティソフトの定義ファイル（パターンファイル）を常に最新の状態になるように設定し、最新の状態になっているか定期的に確認して下さい。

Windows10を使用しているPCの場合で、セキュリティソフトを導入せず、Windows のセキュリティ機能に依存している場合も、OS の最新のバージョンへの更新が必要です。

5. パスワードの適切な設定と管理

パスワードは可能な範囲で複雑な長い文字列を設定して下さい。大小英字、数字および記号を混在させ最低でも 8 文字にしましょう。他のシステムやインターネットサービスで同じパスワードを使い回さないで下さい。また、パスワードを初期設定のままで利用していないか確認します。以上が原則です、テレワークを始める際にパスワードを確認し、必要な場合は変更しましょう。パスワードの保管は、紙への印刷やノート等への記入にして下さい。

6. 不審なメールに注意

日々届くメールのなかには、ウイルスを組み込んだファイルが添付されていたり、ウイルスを仕掛けたサイトやフィッシングサイトへ誘導する URL が記載されていたりといった可能性があります。これらの添付ファイルを開く、URL をクリックすること等により被害にあう場合があります。少しでも不審をいだいたメールの添付ファイルや URL は不用意にクリックしないで下さい。なお、標的型攻撃メールのように、 実在の組織や人物を騙ったり、ごく自然な日本語表現で違和感がなかったり等、一見では不審をいだきにくい場合があります。冷静に送信者のアドレスを見て下さい。海外のドメインであったり、件名や日本語が、ちょっとおかしい等は特に注意点です。

7. USB メモリ等の取り扱いの注意

テレワーク専用の USB メモリの使用が望ましいところですが、ウイルス感染の可能性があるため、所有者が不明等の USB メモリ等はパソコンに接続しないで下さい。 また、業務のパソコンに私用の USB メモリ等を接続しないようにして下さい。

8. ウェブ会議についての注意

ウェブ会議（テレビ会議、オンラインでの打合せなど）のサービス等を新たに使い始める際は、事前にそのサービス等の初期設定の内容を確認して下さい。特にセキュリティ機能は積極的に活用して下さい。例えば、ZOOM を使用する場合は、2020 年 4 月中旬以降に提供された最新版をダウンロードして下さい。また、パスワードの設定や、待合室（ホストの許可がなければ仮想会議室に入室できない機能）の使用をして下さい。

イメージ

セキュリティについて、今回は**最低限必要と考えられる点に絞って**みてきました。

よって、**ここでご案内した注意点を守るだけでセキュリティが万全であるとは考えず、必要に応じ、今回ここで参考にした情報処理推進機構セキュリティセンターが公表した「テレワークを行う際のセキュリティ上の注意事項」** https://www.ipa.go.jp/security/announce/telework.html **等、その他、各種の情報を参考として下さい。**