経理担当者が自宅でテレワークを行う場合のセキュリティの注意点

令和２年５月１日

認定 NPO 法人 NPO 会計税務専門家ネットワーク

◎ はじめに

新型コロナウイルス感染症(COVID-19)の影響により、ICT を用いて自宅でも業務が行えるような環境を整えて、社員等を出社させずに事業継続を図る動きが急速に進んでいます。３月決算の NPO 法人では、この時期は決算業務が集中しますが、法人の経理担当者が、法人の事務所への出勤や、無理な残業を避けて、自宅で決算業務などができるように、テレワークを行う際のセキュリティに関する注意事項を案内します。

セキュリティは、個人情報を含めた法人の大事な情報が、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ますし専門的にもなります。ここでは、最低限必要と考えられる点に絞って説明しますので、ここに書かれている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ないでください。
必要に応じて、この案内の作成の元とした、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　など、各種の情報を参考としてください。

テレワークには様々な利用環境があります。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。
一方でそのような本格的な環境が提供されていない状況で、自宅勤務を実施されている場合もあると思います。ここでは、そのような場合、つまり、法人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する場合における注意事項を説明します。

◎ テレワークを行う際のセキュリティ上の注意事項

･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 にそれほど詳しくない、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ください。

·そのために、以下の項目を確認し実施してください。

１．紙の資料やファイルなどのデジタルデータの紛失や情報流出の防止

法人の事務所から紙の資料を持ち出す際の電車の車内などへの置忘れや、郵送の途上での誤配や紛失を防止してください。郵送の際は書留や宅急便などの使用を検討してください。ファイルなどのデジタルデータを格納したUSBメモリの紛失も同じです。自宅のパソコンなど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。メール添付などでファイルを送付する際は、必要に応じて、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ください。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。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てください。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は、例えば、以下のサイトを参照してください。この他にも、説明しているサイトは多数あります。

「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/

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います。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ください。

WindowsXPやWindows 7を使用しているパソコンを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）を常に最新な状態になるように

設定し、最新の状態になっているか定期的に確認してください。

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ください。大小英字、数字および記号を混在させて最低でも 8 文字にしてください。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ください。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てください。

以上が原則ですので、テレワークを始める際に、パスワードを確認して、必要な場合は変更してください。パスワードの保管は、紙への印刷やノートなどへの記入にしてください。

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いたり、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ください 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など、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ください。海外のドメインだったり、件名や日本語が、ちょっとおかしいなどが注意点です。

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、所有者が不明などの USB メモリ等はパソコンに接続しないでください。また、法人のパソコン以外に自分の USB メモリ等を接続しないでください。

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ください。特にセキュリティ機能は積極的に活用してください。例えば、ZOOM を使用する場合は、４月中旬以降に提供された最新版をダウンロードしてください。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）の使用をしてください。