テレワーク勤務のサイバーセキュリティ対策！

更新日：2020年3月31日

テレワークで勤務をされる方へ

テレワークでの勤務は、オフィスのサイバーセキュリティの環境とは異なり、勤務先のシステム等へ外部からアクセスしますので、マルウェア（ウイルス）への感染リスクが高まります。
テレワークで使用するパソコン等（タブレット、スマートフォン）は、勤務先が導入したテレワーク専用のものであればサイバーセキュリティ対策が考慮されている場合がほとんどです。
しかしながら、急遽、テレワークをすることになり、普段勤務先で使用しているパソコンや自宅のパソコンを使用する場合は、サイバーセキュリティ対策が十分とは言えませんので、特に注意する必要があります。
サイバーセキュリティ対策を怠ると、使用しているパソコンがマルウェア（ウイルス）に感染して業務が行えなくなったり、重要なデータが流出し、業務に大きな影響を与えることが考えられます。
ここでは、上記のように急遽、テレワークで勤務する場合のサイバーセキュリティ対策上の注意すべき点を紹介します。

テレワーク勤務のサイバーセキュリティ対策チラシ（PDF形式：579KB）

サイバーセキュリティ対策

テレワークで使用するパソコン等（タブレット、スマートフォン）

サポートが終了しているOS（オペレーティングシステム）のパソコンを使用しない。

Windows7、WindowsVista、WindowsXPは、すでに脆弱性等に対するサポートがされていないため、マルウェア（ウイルス）に感染するリスクが高くなります。

ウイルス対策ソフトを必ず導入する。

マルウェア（ウイルス）の感染防止のために必ず導入しましょう。

毎日の業務を始める前に、使用するパソコン等のOS、ウイルス対策ソフト、アプリケーションを最新の状態にする。

日々変化をしているマルウェア（ウイルス）に感染しないように、更新しましょう。

テレワークで使用するパソコンは、自分以外に使用させない。

一つのパソコンを複数人や別アカウントで共有し、インターネットに接続すると、マルウェア（ウイルス）に感染するリスクが高くなるので、家族や友人とも共有しないようにしましょう。

不特定多数が利用するパソコンの使用を避ける。

たとえば、インターネットカフェや空港のラウンジ等の不特定多数が利用するパソコンは、キーボードで入力した文字が記録される悪意のあるプログラム（キーロガー）が仕込まれていたり、情報を盗み見される等のリスクがあります。

データを暗号化して保存する。

マルウェア（ウイルス）感染による情報流出やパソコンの紛失に備えて、パソコン本体内にデータを保存するときは、暗号化をしましょう。

ファイル共有機能をオフにする。

Wi-Fiスポット（公衆無線LAN）等のネットワーク内では他のパソコンからアクセスされるおそれがありますのでファイル共有機能をオフにしましょう。

注目情報

テレワーク勤務のサイバーセキュリティ対策！

ようこそ情報セキュリティ広場へ

ランサムウェアに要注意！

東京中小企業サイバーセキュリティ支援ネットワーク(Tcyss)

Tcyss参加団体

不測の事態に備え、データのバックアップを！

不確かな情報に惑わされないために

コンピュータ・ウイルスに対する自己防衛

考えよう見えない画面の向こう側

運転免許に関する情報

FAQ　よくある質問

情報が見つからないときは

通信経路

使用するパソコンから勤務先等の接続先までの通信経路が、VPNで暗号化されているか否かを勤務先のネットワーク担当者に確認してから業務を行う。

通信経路が暗号化されていないと情報を盗み見されるおそれがあります。

VPNサービスを利用するときは、運営者が明確であり、かつ情報が健全に取り扱われるものを利用する。

VPNサービスの中には、通信の盗み見や改ざん、マルウェア（ウイルス）の組み込みがされている場合があるので信頼のあるものを利用しましょう。

パスワード

他人に推測されにくい複雑なものにする。

簡単なものは、他人に不正アクセスされるリスクが高くなります。

他のサービスと使い分け、テレワーク専用にする。

他のサービスと同じパスワードを使用していると、そのサービスがサイバー犯罪の被害によって情報が流出した場合、テレワークのシステムに不正アクセスされるおそれがあります。

パソコン本体内に保存しない。

ウイルス感染時、外部に流出し、不正利用されることがあります。

自宅のWi-Fiルータを使用するとき

ファームウェアを最新のものにアップデートする。

ルータに欠陥があった場合、修正プログラムが配信されている場合がありますので、最新のものに更新しましょう。

管理用IDとパスワードを購入したままの状態で使用しない。

初期設定のまま使用した場合、外部から不正アクセスされるおそれがありますので、変更してから使用しましょう。

SSID（アクセスポイント名=AP名）は、個人が特定される名前などを設定しない。

モバイルルータも同様で、設置者の個人名等を周囲に知らせていることになるので注意しましょう。

WEPによる暗号化方式を使わない。

WEPによる暗号化は、容易に解読されてしまい、盗み見されるおそれがあります。また、WPAのTKIP方式は比較的短時間で解読されてしまうので使わないようにしましょう。

Wi-Fiスポット（公衆無線LAN)やサテライトオフィスを利用するとき

接続パスワード（キー）が、「ない」または「公開されている」Wi-Fiスポット（公衆無線LAN）では、セキュリティが不十分なため重要な情報のやり取りをしない。

通信経路がVPNで暗号化されていないときは、情報を盗み見されるおそれがあるのでネットバンキング等の利用をしてはいけません。

偽のWi-Fiスポットに注意する。

偽のＷｉ-Ｆｉスポットは、情報を盗み見するために悪意のある者によって設置されるものです。見知らぬＷｉ-Ｆｉスポットを利用する場合に注意するほか、同一のSSID（アクセスポイント名=AP名）接続パスワード（キー）を使ったなりすましの偽Ｗｉ-Fiスポットの場合、パソコンのＷｉ-Fiの接続設定が自動になっていると自動接続され、情報を盗み見されるおそれがあるので注意しましょう。

電子メール

メールに添付されているWordファイル等のマクロ機能を安易に起動したり、メール本文やPDF等の添付ファイルに記載してあるURLに安易にアクセスをしない。

マクロを起動したり、URLにアクセスするとマルウェア（ウイルス）に感染する恐れがありますので安易にクリックしないようにしましょう。

メール本文中に記載のURLから、ネットバンキング等のログイン情報等を求められても入力しない。

フィッシングの可能性があり、偽のページに誘導され、ログイン情報（ユーザーID、パスワード）を盗まれてしまいますので、「お気に入り」「ブックマーク」等、普段のアクセス方法を利用しましょう。

取引先から不審なメールを受けたときは、取引先に電話で確認をする。

取引先がマルウェア（ウイルス）に感染して、拡散しているかもしれません。不審なメールを受信したときは取引先に電話で連絡をして、直接確認しましょう。

取引先から「そちらからおかしなメールが送られてきた。」等と連絡を受けたときは、すぐにパソコンをネットワークから遮断する。

使用しているパソコン等がマルウェア（ウイルス）に感染して、マルウェア（ウイルス）付きメールを拡散している可能性があります。連絡を受けた時点でネットワークから遮断し、勤務先のネットワーク担当者に連絡して対処方法を確認しましょう。

メールで振込先の口座変更やはじめての振込先への送金を求められた場合は、メールを送った本人に電話で確認をする。

なりすましメールによる振り込め詐欺の場合がありますので、新しい振込先への送金は、依頼主に電話で確認してから行いましょう。

なお、メールに記載されている連絡先は偽物の場合がありますので、普段からやりとりをしている連絡先に連絡しましょう。

その他

パソコン内のデータが勝手に暗号化され、金銭を要求されたら、パソコンをネットワークから遮断する。

ランサムウェアに感染した可能性があります。すぐにパソコンをネットワークから切り離し、勤務先のネットワーク担当者に連絡をしましょう。

なお、金銭を支払ってもデータが復号される保証がありませんので、金銭を支払ってはいけません。

勤務先のシステムへログインするときは、定められた手順・方法で行う。

手順を逸脱するとセキュリティが保たれなくなり、サイバー攻撃を受けやすくなるので注意しましょう。

USBメモリー等の外部記録媒体は、テレワーク専用のものを使用する。

USBメモリー（新品を含む。）にマルウェア（ウイルス）が仕込まれている場合があるので注意しましょう。

テレワークで使用するパソコンでは、スマートフォンの充電をしない。

接続した機器からマルウェア（ウイルス）に感染するおそれがあります。

電車やカフェなどで業務を行う場合はのぞき見や盗撮に注意する。

のぞき見防止フィルターを装着するなど対策をしましょう。

テレワークのシステムの不具合が発生した場合に備えて、連絡先を確認しておく。

テレワークで勤務する時も、オフィスで勤務する時と同様にネットワーク担当者の連絡先を確認しておきましょう。