第１０９回 維持管理研究会 議事録

１．開催日時 ： ２０２０年 8月２０日（木）１５：３０～１７：１０

２．場　　所 ： Zoom リモート開催

３．出席者（敬称略） ２０名

相原、石渡、井上、小田、大塚、葛西、金子（幸）、久保、澤田、清水、守護、菅谷、高橋、徳山、橋川、福島、柳本、柳谷、山下、中谷（記）

４．研究テーマ

新型コロナウイルス感染症（COVID-19）の感染が蔓延期に、複数の災害が同時に発生する複合災害（マルチハザード）の可能性がある。特に COVID-19 感染期において大地震・台風・集中豪雨による風水害が発生した場合の企業の対応について情報交換を行った。

With コロナの現状では、テレワーク中心になっており、社内には 10～20%程度が出勤されている状況での最適な対策本部とはどのような体制がベストなのか？

①自衛消防隊としての対応は出来るのか？ （避難・通報・初期消火・応急救護）

②公共インフラ停止状態での最適な行動が取れるのか？ （電気・水道・交通機関停止等）

③災害対応用品備蓄品は、容易に準備できるのか？

④通信インフラが途絶えている状況で、代替本部での情報収集・対応が十分可能なのか？

《各社対応事例》

●緊急時の対応 BOX（赤色）に、緊急時に対応手順・役割等、及び備蓄品の保管庫のカギを格納しており、従業員の誰でもが対応できるように日頃から説明している。

●緊急時の対応状況を整理し、レッドファイルとして従業員の目につきやすい場所に保管している。初動の備蓄補品については、各人の机に設置しており、いつでも使用できるようにしている。

●部屋の出入口に基本行動を掲示（フローチャート）しており、誰でもが行動できるようにしている。また全社員への通知を行い、定期的に意識付けを行っている。

●総務部門の担当者は、交代で出勤しており、緊急時に対応できるように配慮している。

※出勤率が低下している中での災害発生を想定していなかった企業も多くみられた。今後の課題として、対応を検討していく企業も多くあった。

《今後の課題》

テレワーク環境化における訓練を検討する必要がある。

次回は、現状の勤務状況に適した最適なリモート訓練について研究していくこととした。

《添付資料》

警視庁サイバーセキュリティ対策本部（抜粋）発行のテレワークで使用するパソコンなどのサイバーセキュリティーに注意！

テレワークで使用するパソコンなどのサイバーセキュリティーに注意！

警視庁サイバーセキュリティ対策本部（抜粋）

※注目されるテレワーク！

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ーの環境とは異なり、勤務先のシステムなど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など（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ー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、急きょ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ー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ー対策を怠ると、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。

1. テレワークで使用するパソコンなど（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、すでに脆弱性など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）に感染する恐れがあります。

□**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、使用するパソコンなどの 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、複数人で使用しない**

複数人で使用すると、自分以外の人がネットサーフィンなどでマルウェア（ウイルス）に感染した場合、それを知らずに業務で使用してしまうこともあるので注意しましょう。

□**インターネットカフェなどに設置されているパソコンの使用を避ける**

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）が仕込まれている場合があるので注意しましょう。

□**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）などのネットワーク内の他のパソコンからアクセスされる恐れがありますので、ファイル共有機能をオフにしましょう。

2. 通信経路

□**使用するパソコンから勤務先など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恐れがあります。

□**VPN サービスを利用する時は、運営者が明確で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、信頼できるものを利用しましょう。

3. Wi-Fi スポット（公衆無線 LAN）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」セキュリティーが不十分な Wi-Fi スポット（公衆無線 LAN）では、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恐れがあるのでネットバンキングなど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 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、情報を盗み見されてしまいます。VPN で暗号化することによって、万が一、偽 Wi-Fi スポットに接続してしまってもそれを防ぐことができます。

4. 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**

ルーター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恐れがありますので、変更してから使用しましょう。

□**SSID（AP 名、アクセスポイント名）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、設置者の個人名など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、盗み見される恐れがあります。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。

5. 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恐れがあります。

□**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恐れがあります。

□**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。

6. 電子メール

□**メールに添付されている Word ファイルなどのマクロ機能を安易に起動したり、メール本文や**

PDF など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、ネットバンキングなどのログイン情報など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」など、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または、通知をする**

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」など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などがマルウェア（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初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可能性があります。普段から知っている連絡先に連絡しましょう。

3．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ーが保たれなくなり、サイバー攻撃を受けやすくなるので注意しましょう。

□**USB メモリーなどの外部記録媒体は、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、スマートフォンなどの充電や他の機器を接続しない**

接続した機器からマルウェア（ウイルス）に感染する恐れがありますので接続してはいけません。

□**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ときも、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。