CyberCrime Control Project

令和２年 第２号

広島県警察本部
サイバー犯罪対策課
082-228-0110
（内線　705-586）

― テレワーク勤務する際は、セキュリティ対策をしっかりと ―

テレワーク勤務者をターゲットにした攻撃が増加中！

新型コロナウイルスが拡散した影響で、テレワーク勤務が導入され、自宅のパソコン等で業務を行う場合、セキュリティ対策を十分に行わないと**企業の機密情報や個人情報等が流出**してしまうリスクが高くなります。

電子メールを利用したサイバー攻撃（なりすましメール）が増加しているので注意してください。

一般的なイメージ

イメージ図の説明

① 攻撃者が**業務メール等を装ったなりすましメール**を送信
- ○悪意のあるファイルを添付
- ○悪意のあるサイトへのリンクを貼付

② 添付ファイルを開封又はリンクをクリックしてウイルスに感染する。

③ 遠隔操作や悪意のあるサイトへアクセスされ、企業の機密情報等が窃取される。

不審なメールを受信したら

- ○ 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に安易にアクセスしない。
- ○ 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。
- ○ 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する。
- ○ 取引先から「そちらからおかしなメールが送られてきた。」等の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。
- ○ 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する。

引用 警視庁　https://www.keishicho.metro.tokyo.jp/kurashi/cyber/joho/telework.html

セキュリティ対策

テレワーク勤務をする際には、自宅のパソコン等のセキュリティ対策をしましょう！！

- ○ 修正プログラムの適用
- ○ セキュリティソフトの導入及び定義ファイルの最適化
- ○ パスワードの適切な設定と管理
- ○ 不審なメールに注意
- ○ 社内ネットワークへの機器接続のルールの遵守
- ○ USBメモリ等の取り扱いの注意
- ○ パソコン等の画面ロック機能の設定
- ○ ソフトウェアをインストールする際の注意
  ※フリーソフト等をダウンロードやインストールしたときに自動的にウイルス等がインストールされてしまう場合があります。
- ○ 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。
  ※接続した機器からウィルスに感染するおそれがあります。
- ○ サポートが終了しているOSのパソコンを使用しない。
- ○ 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。
- ○ 不特定多数が利用するパソコンの使用を避ける。
- ○ データを暗号化して保存する。
- ○ ファイル共有機能をオフにする。
- ○ 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。
- ○ テレワークのシステムに不具合が発生した場合に備えて連絡先を確認しておく。

引用 ＩＰＡ　https://www.ipa.go.jp/security/announce/telework.html
警視庁　https://www.keishicho.metro.tokyo.jp/kurashi/cyber/joho/telework.html

こんなメールも！！

新型コロナウイルス関連情報を装ったメール

新型コロナウイルスが拡散した影響により、緊急事態宣言も出され、多くの人が新型コロナウイルスの情報に敏感になっているため、その状況に乗じて、関連情報を装ったメールが多く送信されています。

中には、政府やWHO（世界保健機関）を装ったメールもあり、新型コロナウイルス対策について偽の援助情報等が書かれており、偽ホームページのリンクも含まれています。

クリックすると、正規のものと見分けのつきにくい偽ホームページが表示され、個人情報等を入力させられてしまうことがあります。

平成 28 年～令和２年
「めざそう！安全・安心・日本一」
ひろしまアクション・プラン

運動目標
県民だれもが穏やかで幸せな暮らしを実感できる
日本一安全・安心な広島県の実現

重点項目
- 身近な犯罪被害の抑止
- 子供・女性・高齢者等の安全確保
- 新たな犯罪脅威への対応

なくそう特殊詐欺被害 アンダー5作戦
なくそう交通死亡事故 アンダー75作戦