CyberCrime Control Project

令和３年 第２号

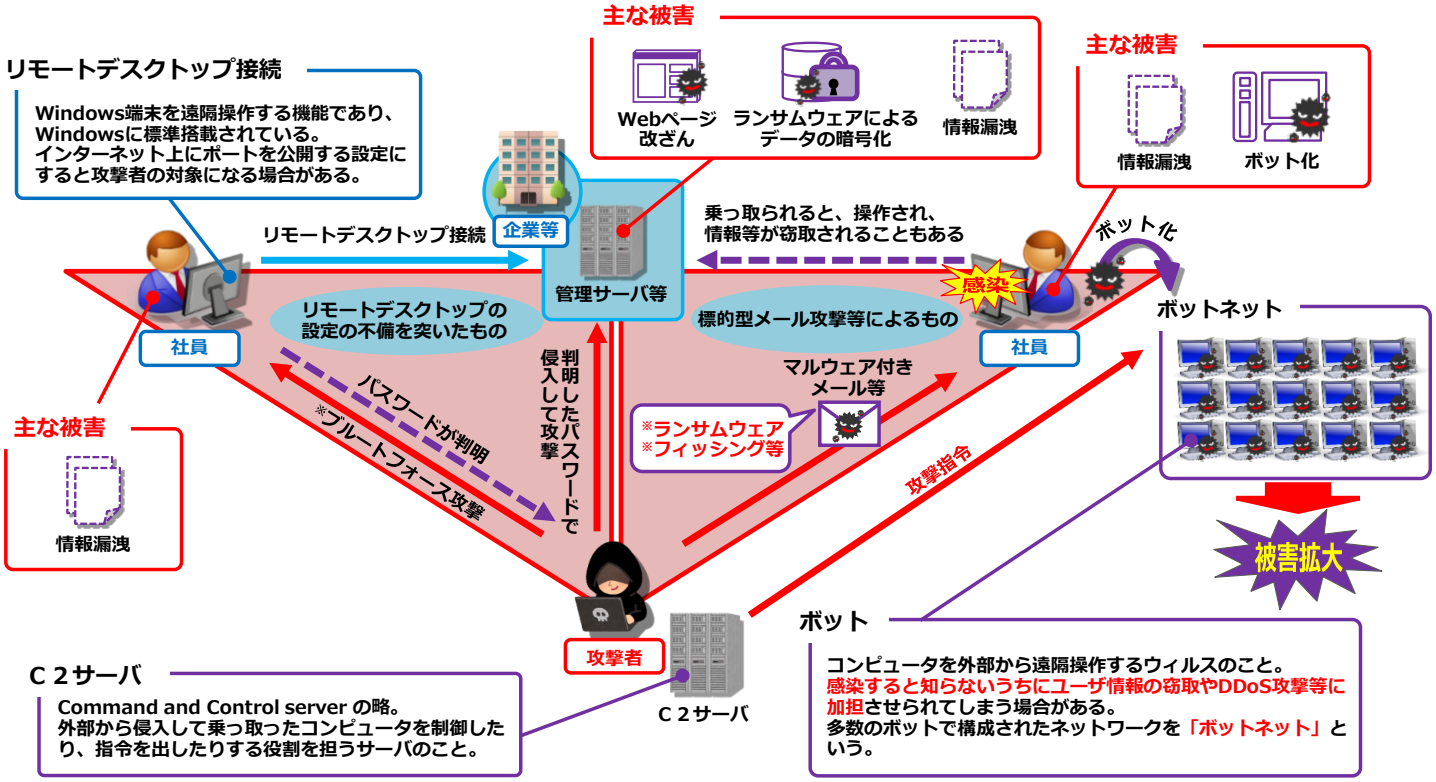
広島県警察本部
サイバー犯罪対策課
082-228-0110
（内線 705-586）

― テレワーク勤務でサイバー攻撃の標的にならないために ―

新しい年度になりましたが、未だコロナ禍の影響もあり、テレワーク勤務を継続する企業等が多いと思われます。
セキュリティ対策が不十分なままテレワーク勤務を行うと、**サイバー攻撃の標的**になってしまうことがあります。
今一度、セキュリティ対策を見直しましょう。

テレワークを狙った主な攻撃

標的型メール攻撃、ランサムウェア攻撃、Webページ改ざん、フィッシング 等々



※ランサムウェア：サーバ等のデータを暗号化する等して使用不可にし、暗号化したデータの復旧と引き換えに身代金を要求するメッセージを表示するマルウェアの総称。
※フィッシング：銀行等の企業を装ってメールを送り、偽のWebサイトにアクセスさせ、IDやパスワード等を入力させる等不正に個人情報を入手する行為のこと。
※ブルートフォース攻撃：総当たり攻撃とも呼ばれ、パスワード等を解読するために可能な組み合わせをすべて試す攻撃手法のこと。

セキュリティ対策

テレワーク勤務をする際は、勤務で使用するパソコン等のセキュリティ対策をしっかりと行いましょう！

テレワーク勤務を始める前に
- 使用するパソコン等は、なるべく他人と共有で使用しないこと
  やむを得ない場合は、業務用のユーザアカウントを別途作成すること
- 社内ネットワークへの機器接続ルールを遵守すること
- サーバ等へアクセスする際のパスワードは複雑な設定にしておくこと
- 不具合が発生した場合の連絡先等の体制を確認すること

テレワーク勤務の注意点
- 自宅に設定しているルータのファームウェアを最新のものに更新すること
- カフェ等の公共の場で行うときは、画面ののぞき見や盗撮に注意すること
- 公衆Wi-Fiを利用する場合は、暗号化設定をよく確認すること
- 公衆Wi-Fiを利用する場合は、パソコンのファイル共有機能をオフにすること
- 公衆Wi-Fiを利用する場合は、必要に応じてＶＰＮサービスを利用すること
- デジタルデータ/ファイルだけでなく、紙の書類等の管理にも注意すること

パソコン等の設定
- サポートが終了しているＯＳのパソコンを使用しないこと
- 修正プログラムを適用すること
- セキュリティソフトの導入及び最新の定義ファイルにすること

データ・システムのバックアップ
- 重要なファイルは定期的にバックアップを取得すること
- バックアップに使用する装置等は、バックアップ時のみ対象機器と接続すること
- データのみならず、システムの再構築を含めた復旧計画を策定すること

不審なメール等を受信した場合
- 本文に記載されているＵＲＬにアクセスしない
- 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実行しない
- なりすましている恐れもあるため、送信元に電話等で確認する

セキュリティ対策は、定期的に見直しをすることが大切です

（引用） IPA https://www.ipa.go.jp/security/announce/telework.html, https://www.ipa.go.jp/security/announce/telework.html
（引用） cybereason https://www.cybereason.co.jp/blog/ransomware/5436 警視庁 https://www.keishicho.metro.tokyo.jp/kurashi/cyber/joho/telework.html