2022/02/28　成形課　奥野

2022年２月１日～３月１８日は
「サイバーセキュリティ月間」です。
2022年 キャッチフレーズ 「#サイバーセキュリティは全員参加」です。

"情報セキュリティのリスク要因＝脅威"　について紹介します。

1）人的脅威
人により引き起こされる脅威

・誤操作によるデータ消失
・クラッキング
　悪意と持ちコンピューターへの不正侵入、データの盗み見、データ破壊など

・ソーシャルエンジニアリング
　心理的隙間を利用しての秘密情報の取得
　ショルダーハック：肩越しに盗み見る
　トラッシング：捨てられた書類などから、情報を盗み取る

2）物理的脅威
災害、機器破壊など物理的な手段による脅威

3）技術的脅威
技術的手段により引き起こされる脅威（最終的な手段が技術によるもの）
マルウェア：悪意あるソフトウェアの総称（Malicious悪意ある+Softwareソフトウェアの造語）

・スパイウェア
　利用者に気づかれないよう情報収集をする。
　Spy（諜報員）+Software

・ランサムウェア
　PCやファイルを使用不能にしたうえで、回復のための金銭を要求する
　感染するとファイルやデータが暗号化されてしまい、正常にアクセスできなくなります。
　Ransom（身代金）+Software

・フィッシング
　金融機関を装い、利用者を誘導し、暗証番号やクレジットカード情報を不正に取得する。
　Phreaking（回線の不正使用）+Fishing（釣る）

・トロイの木馬
　有用でるように見せかけてインストールさせ、コンピューターに侵入するソフトウェア。

・DoS攻撃
　電子メールやWebサービスへ要求を大量に送り付け、ネットワーク上のサービスを提供不能にする攻撃。
　Denial of Service（サービスの妨害）

・ゼロデイ攻撃
　システムやネットワークの脆弱性を攻撃。

・SPAMメール

受信者の承諾なく、無差別に送られるメール。

大量に送られるため、メールサーバーへの負荷が大きくなる。

その他にも…

・クロスサイトスクリプティング

Webページ上から悪意のある簡易プログラムを埋め込み、データを盗み出す攻撃。

・総当たり攻撃、辞書攻撃、リスト攻撃

パスワードなどを割り出す攻撃。

…等々

技術的脅威の中には、個人として対策しにくいものもあります。

一方で、人的脅威・メール等の扱いは個々で取り組むことができます。

小さなことからでも、知る事・気にする事が対策への一歩となるのではないでしょうか。