サイバー攻撃の考察

2022 年 11 月 29 日　吉倉洋治

NO	ネットワークを利用している社内サービス	社内ネットワーク	社外ネットワーク	パスワード・ログイン	IP アドレス制限	サイバー攻撃の可能性
1	社内共有フォルダ（NAS）	○				×
2	発注管理システム		○	○	○	×
3	点検リード		○	○		○
4	日報		？	？		○
5	会社ホームページ		○			○
6	会計ソフト（弥生）		○	○		○
7	メール		○	○		○
8	ドライブ運航記録（KITARO）		○	○		○
9	ドコモのドコデスカ		○	○		○

1. 社内共有フォルダ（NAS）について

外部のネットワークに接続されていないので、サイバー攻撃を受ける可能性はないです。
但し、メールから社員 PC にウイルス感染した場合、社内共有フォルダはウイルス感染し、全滅ます。　メールのウイルス感染については後で説明します。

社内共有フォルダ内のファイル盗難について、悪意ある社員が行えば可能性があります。
これを防止対策として、

① 社内共有フォルダをパスワード・ログインに変更する（ただしパスワードは同一ではダメです）
② 定期的（1～3日）に社内共有フォルダのファイルを削除することが必要です。必要ファイルは自 PC にコピーして使う。　特に社内共有フォルダはゴミ箱化になりやすいので必要です。

私のＰＣから社内共有フォルダは閲覧できないよう設定されているので利用状況はわかりません。

2.発注管理システム

外部ネットワークに接続されていますが、会社の IP アドレスからしかアクセスできないようにしているので、サイバー攻撃を受けることがありません。

3.その他の社外ネットワークを利用しているサービスは、パスワード・ログインに頼っているので
何らかのサーバー攻撃対策が必要です。対策としては、

① 例えば５回以上のパスワード・ログインがあった場合、そのパスワードを失効する。
② パスワード・ログインを２段階認証する（メール、ショートメッセージの利用）。
現在、２段階認証が主流になっています。
③ VPN（仮想専用線）の利用、コストがかかる。

4.メールについて

メール経由でウイルスが送られてきますので、怪しいメールは開かずに削除したり、不審な URL や添付ファイルはクリックしなかったりするように、社員教育を行う必要があります。
特にランサムウェアのウイルスに感染すると、全ファイルが暗号化され、暗号を解くために身代金要求されます。これが①社内共有フォルダに及ぶと大変なことになります。

また、社員の PC にウイルス対策ソフトをインストールすることで、ある程度ウイルスは防げますので、全ＰＣにインストールする必要があります。
現在、社員の PC にどれくらいウイルス対策ソフトがインストールされているかはわかりませんが、一部のＰＣにウイルスバスターが入っているのを確認した。
ちなみに私のＰＣにはインストールされていない。

以上、早急にサイバー攻撃等の対策をする必要性があると思います。