サイバーセキュリティの置き薬

2021年 第5号

メールの送受信時における注意点

メールで添付ファイルを送付する場合、まず、「資料の添付ファイルを暗号化」、次に「暗号化した添付ファイルをメール送付」、その後に「解凍パスワードをメール送付」といった、いわゆる「PPAP方式」が用いられていますが、次のようなセキュリティ上のリスクが考えられます。

⚠ WARNING

こんなリスクがあります

P Password付きのファイルを送ります
P Passwordを送ります
A 暗号化
P プロトコル

リスク１　情報が漏洩する

○　攻撃者にメールが盗聴・転送されている場合や送付先のメールアドレスの宛先が間違っている場合、パスワードも漏洩し、ファイルの情報が漏洩する

リスク２　ウイルスチェックができない

○　ZIPファイル等に暗号化することで、サーバ等でのウイルスチェック機能が働かず、組織内ネットワークの感染リスクが高まる

リスク３　セキュリティ対策の形骸化

○　同一のパスワードを使い回す等、セキュリティ対策が形骸化してしまう
○　Emotetウイルスのように、暗号化ファイルとパスワードが記載されたメールが感染の手口とされるタイプの攻撃に警戒心が薄れてしまう

対策

○　暗号化ファイルとパスワードを同一経路で送信しない

- 事前にパスワードを決めておく
- 電話でパスワードを通知する

○　添付ファイル付きのメールを受信した場合

- 身に覚えのない添付ファイルは開かない、URLリンクは接続しない
- 自分が送信したメールへの返信であっても、不自然な点があれば添付ファイルを開かず、電話等で相手に確認する

○　暗号化ファイルとパスワードが記載されたメールを受信した場合

- Emotetウイルスや IcedIDウイルスでは、暗号化ファイルとパスワードが記載されたメールが感染の手口として確認されていることから、添付ファイルを開かず、電話等で相手に確認する

参考:IPA「Emotet」と呼ばれるウイルスへの感染を狙うメールについて（https://www.ipa.go.jp/security/announce/20191202.html）