サイバーセキュリティの置き薬

2020年
第29号

標的型メール、フィッシングメール、ウイルス付きメールなど、電子メールを手段としたサイバー犯罪の被害防止に向け、電子メール利用時の注意点をお知らせします。

◆ 不自然なタイミングでメールが届いていませんか？

○ 受信したメールが、“今”自身に届くべき内容のものか、注意を払うことが肝要です。不自然な点があれば、メールの送信者に直接確認することが大切です。

・ エモテットウイルスは、過去にやり取りしたメールの返信（Re:）を装うなどして、ウイルス感染を広げます。

・ ビジネスメール詐欺は取引先を装ったメールにより、急な振込先の変更が依頼され、支払い金を騙し取るものです。

・ スパムメールは不特定多数に送信されるもので、ウイルス感染やフィッシングの被害にあう可能性があります。

◆ メールチェックは慎重にしましょう！

○ 日々のメールチェックは大変な作業です。特に休日明け等において、大量のメールを確認する場合、粗雑に扱うことのないよう、慎重な取扱いを心がけてください。

○ 流れ作業的な確認で、安易にリンク先等をクリックすることは危険です。

◆ 送信者のメールアドレスは大丈夫ですか？

○ 心当たりのないメールアドレスから、メールを受信した際は注意が必要です。

○ フリーメールアドレスで取引先や知人を装った不審メールが確認されています。

○ 表示名と[*送信者のメールアドレス*]が一致していますか。

（不一致の例） 送信者：富山県警察[*detarame@example.com*]

◆ メール本文に不審な点はありませんか？

○ 不自然な日本語表記や文章に違和感はありませんか。

○ 緊急にリンク先への接続を促す記載がある場合は、よく確認する、周囲に相談するなど、一呼吸置いてみることが大切です。

○ 執拗にリンク先へ誘導する文言がある場合は要注意です。

○ メール内容を理解した上で、次のステップ（リンク先等をクリックする）に進むことが大切です。特に外国語で表記されたメール内容をよく理解しないまま、リンク先等をクリックすると、ウイルス感染やフィッシングサイトに誘導される可能性があり、危険です。

◆ リンク先のクリック、添付ファイルの実行は慎重に判断！

○ 心当たりのないメール、業務に関係のないメールを受信した場合、リンク先に接続しない、添付ファイルを実行しないことが大切です。興味本位のクリックは厳禁です！

○ エモテットウイルスは、ワードやエクセルのマクロ動作によって、ウイルス感染するものです。マクロの自動実行を無効化にし、感染防止に努めてください。