



# サイバーセキュリティの置き薬

2020年  
第5号

## 異動期におけるセキュリティ対策

何かと慌ただしくなる年度末ですが、この異動期につけ込んだ巧妙な標的型メールが懸念されます。フィッシングサイトへの誘導やビジネスメール詐欺などの被害に遭わないよう、今一度ご注意ください。また、情報流出等が発生しないようにセキュリティ対策についても確認をお願いします。



### 1. 標的型メール

昨今の標的型メールはますます巧妙化しており、世間での話題のテーマや受信者が興味を持ちそうなテーマを盛り込むなど、様々な手口で受信者を騙そうとします。最近では、新型コロナウイルス感染症に関するメールを装ったものも確認されています。

人事異動期における標的型メールも懸念されます。異動期の慌たらしさにつけ込み、添付ファイルの確認を急がすような内容のメールには十分にご注意ください。



### 2. セキュリティ対策

人事異動により、使用するパソコンや USB メモリ等の外部記録媒体が変更になることがあるかと思えます。不要データの削除や保存データの整理を行うとともに、外部記録媒体の紛失にも十分に気を付け、情報流出（情報漏えい）の被害に遭わないように注意が必要です。

また、利用するパソコン等の引き継ぎを行う場合は、パスワードを変更するなどしてセキュリティ対策を講じることも大切です。特に管理者権限を取り扱っている場合は引き継ぎ後、速やかにパスワード変更をしましょう。



### 《情報提供（通報）をお願いします》

今後、社会情勢に乗じたサイバー犯罪の発生が懸念されます。新型コロナウイルスや東京オリンピック・パラリンピック競技大会を装ったフィッシングメールやウイルスメール等のサイバー犯罪等を確認した際は、警察まで情報提供（通報）をお願いします。

【富山県警察サイバー犯罪対策課 076-441-2211】