サイバーセキュリティの置き薬　2021年 第4号

異動期におけるセキュリティ対策

人事異動や組織改編等、何かと慌ただしくなる年度末ですが、この時期につけ込んだ巧妙な標的型メール攻撃が懸念されます。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。

標的型メール、なりすましメール

昨今の標的型メール攻撃はますます巧妙化しており、世間で話題のテーマや、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だまそうとしてきます。2020年には、取引先担当者になりすましたメール、経営層になりすましたメール、オンラインミーティングの招待メールを装うフィッシングメール等の事例が確認されました。

人事異動期の慌ただしさにつけ込み、添付ファイルの確認を急がせるような内容のメールには十分にご注意ください。

【参考】サイバー情報共有イニシアティブ（J-CSIP）運用状況［2020年10月～12月］（https://www.ipa.go.jp/security/J-CSIP）

セキュリティ対策

◆アカウント、アクセス権限の適切な設定と確認

異動したユーザー、担当業務が変わったユーザー、退職したユーザー等のアカウントやアクセス権限は、速やかに適切な処理を行いましょう。特に、特権ID（管理者権限を有するアカウント）については、確実に適切な処理を行うことが肝要です。

※ クラウドサービス、オンライン会議システム、VPNサービス等の確認も忘れずに！

◆情報機器からの情報漏えい対策

情報機器の引継ぎを行う際は、不要データの削除や保存データの整理を行うとともに、USBメモリ等の外部記録媒体の紛失にも十分に気を付けましょう。

また、情報機器の廃棄や返却に当たって、データの削除やハードディスクのフォーマットだけを行った場合、特殊なソフトウェアを使用して、削除されたデータが復元されるおそれがあります。データ消去用のソフトウェアや専門業者のデータ消去サービス等を利用して、データを確実に消去するよう注意してください。