TCSP Toyama Prefectural Police Cyber Security Personnel
サイバーセキュリティの置き薬
2022年 第5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、年度末は何かと慌ただしくなる時期です。この時期につけ込んだ巧妙なサイバー攻撃が懸念されますので、**従業員への注意喚起**をお願いします。また、業務量が増えることで注意力散漫になり、ミスが発生しやすい時期でもあります。情報機器の紛失や誤操作からの情報流出等を防ぐため、**セキュリティ対策**についても確認してください。

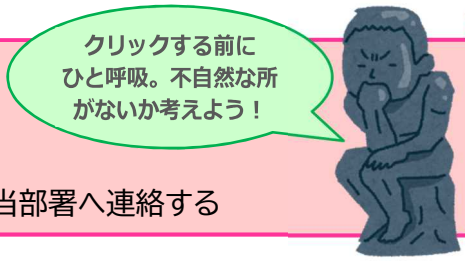
メールチェックは慎重に行いましょう

異動期はメール量の増加が予想されます。一件一件を慎重に確認するよう心がけてください。

- ランサムウェア
- Emotet(エモテット)等のウイルス
- ビジネスメール詐欺

等、標的型攻撃の可能性が考えられます。

【被害に遭わないための注意点】
- メールの添付ファイルや URL を安易に開かない
- マクロやコンテンツを安易に有効化しない
- 身に覚えのないメールを開いた場合は、すぐに担当部署へ連絡する



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。

アカウント、アクセス権限の適切な設定と確認

異動や退職等、権限に変更が生じる従業員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、確実に処理を行うことが肝要です。また、異動期の引継ぎに伴い、一時的に例外的な処理を行う場合は、引継ぎ作業が終わった時点で適切に処理できているか再確認しましょう。

※ 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！

出典･参考 ：「情報セキュリティ10大脅威 2022」
独立行政法人 情報処理推進機構(IPA) セキュリティセンター
https://www.ipa.go.jp/security/vuln/10threat2022.html