サイバーセキュリティパートナーシップだより

マルウェア感染をねらった標的型メール攻撃に注意！

本年10月24日付で、大学が保有するＰＣが昨年７月に受信した標的型メール攻撃でマルウェア（悪意のあるプログラム）に感染し、調査の結果、ＰＣ内の情報窃取の形跡が発見され、学生らの個人情報等が漏洩した可能性がある旨の報道がありました。

今一度、不審メールへの対策をよろしくお願いします。

【標的型メール攻撃の一例】

- 知らない送信元だが、受信者側の興味を引くもの
  （例：取材申込や講演依頼や件名が「重要」など）
- 過去届いたことのない公的機関からのお知らせ
- 組織の業務に関連のある内容　など

→　うかつに本文中のＵＲＬリンクや添付ファイルを開くと・・・

怪しいと思ったら

- **安易にメール文中のＵＲＬリンクやメールの添付ファイルを開かない！**
- **送信元の「メールアドレス」を確認**
  - ☑差出人に見覚えがあっても、登録外のメールアドレスやフリーメールではないか
  - ☑本文中の署名情報に記載のメールアドレスと異なっていないか
- **送信元に電話などで確認**
  - ☑確認する際は、受信メールへの返信以外の方法で！
- **一人で判断せず、組織内のセキュリティ担当などに報告・相談**

管理者の方は組織内の端末の確認を！

- **端末が感染していないか**
  - ☑最新の状態にしたウイルス対策ソフトでフルスキャンを実施
- **メールのアクセス履歴に不審点がないか**
  - ☑アクセス履歴に身に覚えのないログインがあれば、パスワードを変更

山口県警察サイバー犯罪相談窓口
入力フォーム

県警ホームページにて広報資料や動画を公開中です。
（詳しくはQRコード参照）

山口県警察本部サイバー犯罪対策課