サイバーニュース

R 1 年 第 1 2 号
奈良県警察本部
サイバー犯罪対策課

年末年始の長期休暇における情報セキュリティ対策について

多くの人が年末年始の長期休暇を取得する時期は、企業では「システム管理者が不在になる」、家庭では「友人や家族と旅行に出かける」等の状況になりやすく、ウイルス感染や不正アクセス等のトラブルが発生した場合に対処が遅れてしまったり、場合によっては関係者に対して被害が及ぶ可能性があります。

「Emotet」（エモテット）と呼ばれるウイルス感染を狙う攻撃メールが、国内の組織へ広く着信しています。長期休暇明けはメールが溜まっていることが想定されますので、誤って不審なメールの添付ファイルを開いたり、本文中のURLにアクセスしたりしないよう注意してください。

【参考】独立行政法人情報処理推進機構IPA
「年末年始における情報セキュリティに関する注意喚起」
https://www.ipa.go.jp/security/topics/alert20191219.html

～長期休暇の対策～

✓ 偽のセキュリティ警告に注意！

ウェブサイト閲覧中に「ウイルス感染した」等の警告画面が突然表示され、いざという時の相談窓口が休止となっている為、表示されたメッセージに従い、遠隔操作を許してしまうなどの手口により、金銭を要求されることがあります。
警告画面が表示された場合は、
　まずは、落ち着いて！
安易に表示の連絡先へ連絡しないようにしましょう。

✓ 不審なメールに注意！

実在の金融機関や企業を騙った不審なメールを受信した場合、真意を確認できる窓口が休止となっている場合があり、具体的な対処方法が確認出来ないまま被害に遭う可能性があります。
不審なメールの添付ファイルを開いたり、URLにアクセスすることがないよう注意しましょう！

✓ ソフトウェアを最新の状態に！

長期休暇中にOSや各種ソフトウェアの修正プログラムが更新されている場合があります。更新の有無を確認し、OS・ウイルス対策ソフトウェア・インストールプログラムを更新することで、最新の状態にしましょう！様々な被害に遭うリスクを軽減することが出来る第一の手段と言えます。

✓ 不必要な機器等の停止！

電源が入った状態のまま放置していると、外部からの攻撃を受けるリスクが高まります。リスクを軽減するため、休暇中使用しないパソコンやサーバ等の機器は電源をOFFにし、サーバの不必要なサービスは停止しておきましょう！