TCSP Toyama Prefectural Police Cyber Security Personnel
サイバーセキュリティの置き薬
2020年 第32号

年末年始のセキュリティ対策について

長期休暇の時期はシステム管理者が不在となることも多く、被害が発生した場合に対処が遅れたり、場合によっては関係者に対しても被害が及ぶ可能性がありますので注意してください。

長期休暇前及び休暇中の対策

○　緊急連絡体制の確認

委託先企業を含めた連絡体制や対応手順が明確になっているか確認する。

○　テレワーク等の際の機器やデータの持ち出しルールの確認と遵守

・社内用PCを持ち出す際は、**移動時の置き忘れ、紛失を防止**し、万が一紛失等した際のことを考え、**HDDやSSD全体を暗号化**する。
・私用PCを使用する際は、**マルウェア感染による重要情報の外部漏えいを防ぐ**ため、**OS、各種ソフトウェアの修正プログラムを適用**する。

○　社内ネットワークへの機器接続ルールの確認と遵守

○　使用しない機器の電源ＯＦＦ

長期休暇後の対策

○　修正プログラムの適用

○　定義ファイルの更新

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公開されている場合があるため、システム管理者の指示に従い、必要な修正プログラムを適用する。

電子メールの送受信やウェブサイトの閲覧等を行う前に定義ファイルを更新する。

○　サーバ等における各種ログの確認

○　持ち出し機器のウイルスチェック

サーバ等の機器に対する不審なアクセスが発生していないか各種ログを確認する。

○　不審なメールに注意

組織内で利用する前にウイルススキャンを行う。

「Ｅｍｏｔｅｔ」（エモテット）と呼ばれるウイルスへの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。長期休暇後は、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かない、本文中のＵＲＬにアクセスしないように注意してください。

参考

IPA 「長期休暇における情報セキュリティ対策」 https://www.ipa.go.jp/security/measures/vacation.html
IPA 「テレワークを行う際のセキュリティ上の注意事項」https://www.ipa.go.jp/security/announce/telework.html
IPA 「日常における情報セキュリティ対策」https://www.ipa.go.jp/security/measures/everyday.html
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