Ksisnetだより
発行:Ksisnet事務局
令和2年7月29日
Vol.82

お盆などの長期休暇時における情報セキュリティ対策について

長期休暇の時期は、システム管理者が長期不在になりやすく、ウイルス感染や不正アクセスの被害が発生した場合に対処が遅れる可能性があります。
本年は新型コロナウイルスの影響に伴い、テレワーク等新たなシステムを導入する企業が増え、例年とは異なる状況での長期休暇となりますが、今一度長期休暇に当たって、以下の対策を行ってください。

システム管理者向け対策

【長期休暇前の対策】

○ 緊急連絡体制の確認

不測の事態が発生した場合に備えて、委託先企業を含めた緊急連絡体制や対応手順等が明確になっているか確認してください。

- 連絡体制の確認（連絡フローが現在の組織体制に沿っているか等）
- 連絡先の確認（各担当者の電話番号が変わっていないか等）

○ 使用しない機器の電源OFF

長期休暇中に使用しないサーバ等の電源をOFFにしてください。

【長期休暇明けの対策】

○ 修正プログラムの適用

長期休暇中にOS（オペレーティングシステム）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ります。修正プログラムの有無を確認し、必要な修正プログラムを適用してください。

○ 定義ファイルの更新

長期休暇中に電源を切っていたパソコンは、セキュリティソフトの定義ファイル（パターンファイル）が古い状態のままになっています。利用者に使用させる前に定義ファイルを更新し最新の状態にしてください。

○ サーバ等における各種ログの確認

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、各種ログを確認してください。もし、何らかの不審なログが記録されていた場合は、早急に詳細な調査等の対応を行ってください。

利用者向け対策

【長期休暇前の対策】

○ 機器やデータの持ち出しルールの確認と遵守

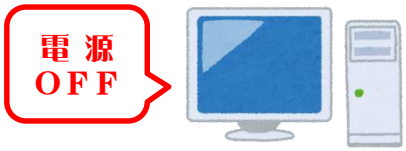
長期休暇に社外での対応が必要となるなどパソコン等の機器やデータ等の情報を持ち出す場合は、持ち出しルールを事前に確認し遵守してください。

○ 社内ネットワークへの機器接続ルールの確認と遵守

ウイルス感染したパソコンや外部記憶媒体等を社内ネットワークに接続することで、ウイルスをネットワーク内に拡散してしまうおそれがあります。長期休暇中にメンテナンス作業などで社内ネットワークへ機器を接続する予定がある場合は、社内の機器接続ルールを事前に確認し遵守してください。

○ 使用しない機器の電源OFF

長期休暇中に使用しない機器は電源をOFFにしてください。



【長期休暇中の対策】

○ 持ち出し機器やデータの厳重な管理

自宅等に持ち出したパソコン等の機器やデータは、ウイルス感染や紛失、盗難等によって情報漏えい等の被害が発生しないよう、厳重に管理してください。

【長期休暇明けの対策】

○ 修正プログラムの適用

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ります。修正プログラムの有無を確認し、必要な修正プログラムを適用してください。なお、修正プログラムの適用については、システム管理者の指示に従ってください。

○ 定義ファイルの更新

長期休暇中に電源を切っていたパソコンは、セキュリティソフトの定義ファイルが古い状態のままになっています。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し、最新の状態になっていることを確認してください。

○ 持ち出し機器のウイルスチェック

長期休暇中に持ち出していたパソコンや、データを保存していたUSBメモリ等の外部記憶媒体にウイルスが感染していないか、組織内で利用する前にセキュリティソフトでウイルスチェックを行って下さい。

○ 不審なメールに注意

実在する企業などを騙った不審なメールは、誤って添付ファイルを開いたり、本文中のURLにアクセスしたりすることでウイルス感染したり、フィッシングサイトに誘導されたりしてしまう可能性がありますので注意してください。

マルウエア Emotetの感染に繋がるメールにも注意！！

Emotetは、情報窃取を行うだけでなく、感染端末から窃取した情報を用いてスパムメールを送信し、更に感染拡大を試みる機能などを有するマルウエアです。

令和元年10月頃から、国内でEmotetの感染事例が相次いでいましたが、一時Emotetの感染に繋がるメールは減少し、大きな動きは見られませんでした。しかし、本年７月頃から、Emotetの感染に繋がるメールが再び確認されていますので、注意してください。

参考　ＩＰＡ（情報処理推進機構）・JPCERT/CC