Ksisnetだより
発行:Ksisnet事務局
令和4年 4月26日
Vol.105

GWなど長期休暇時中の情報セキュリティ対策について

GWなど長期休暇の時期は、ウイルス感染や不正アクセス等の被害が発生した場合の対処が遅れる可能性があります。
そのような事態とならないよう、システム管理者が長期不在になる場合は必ず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】

1　緊急連絡体制の確認

不測の事態に備えて、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）

2　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】

1　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。

2　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。

3　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下さい。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。

攻撃再開したEmotetに注意してください！

2021年11月より活動を再開したEmotetの感染が、2022年２月以降急速に拡大しています。
不用意にメール添付のファイルやメール本文のURLは開かず、必ず相手に確認しましょう。

利用者向け対策

【長期休暇前の対策】

1　機器やデータの持ち出しルールの確認と遵守

長期休暇中、社外で業務に当たる必要があるなど、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。

2　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メモリ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。

3　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】

1　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】

1　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。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。

2　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。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。

3　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メモリ等の外部メモリ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ください。

4　不審なメールに注意

実在の企業などを装った不審なメールに注意して下さい。メールの添付ファイルを開いたり、本文中のＵＲＬにアクセスしてダウンロードしたファイルを開いたりすることでウイルスに感染してしまう可能性があります。年末年始といった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。不審なメールを受信していた場合は各組織のシステム管理者に報告し、指示に従ってください。

参考　ＩＰＡ（情報処理推進機構）