サイバーセキュリティの置き薬

2021年 第14号

年末年始のセキュリティ対策について

休暇期間中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機関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。

休暇前に確認！

＜利用者向け＞
- ○　機器やデータの持ち出しルールの確認と遵守
- ○　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

＜管理者向け＞
- ○　緊急連絡体制の確認
- ○　使用しない機器の電源 OFF
- ○　バックアップデータの確保

休暇中のサイバー攻撃によるランサムウェアの被害に備えて、バックアップデータをネットワークから切り離した状態で保管するなど、被害リスクの分散に努めてください。

休暇中に確認！

＜利用者向け＞
- ○　持ち出し機器やデータの厳重な保管

テレワーク時に注意すること

- ○　テレワークで使用するパソコン等はできる限り他人と共有して使わない
- ○　ウェブ会議のサービス等を使い始める際は、事前に初期設定の内容を確認し、特にセキュリティ機能は積極的に活用
- ○　公衆 Wi-Fi を利用する場合は、パソコンのファイル共有機能をオフにし、必要に応じて信頼できる VPN サービスを利用

休暇後に確認！

＜利用者向け＞
- ○　修正プログラムの適用
- ○　定義ファイルの更新
- ○　持ち出し機器のウイルスチェック
- ○　不審なメールに注意

＜管理者向け＞
- ○　修正プログラムの適用
- ○　定義ファイルの更新
- ○　サーバ等における各種ログの確認

実在する企業などを騙った不審メールが多く報告されています。

不審メールの添付ファイルを開いたり、本文中の URL にアクセスしたりすることで、ウイルスに感染したり、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。

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「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/alert20201217.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