



長期休暇を狙ったサイバー攻撃に注意!!

年末年始などの長期休暇は、セキュリティ担当者が不在となることや、休み明けの業務が煩雑になることなどを狙って、サイバー攻撃が多くなる傾向があります。年末年始の長期休暇前後に必要な情報セキュリティ対策を実施し、被害防止に努めてください。

○ システム管理者が取るべき対策例

- ◆ ランサムウェアなどへの感染に備え、**重要ファイルのバックアップを行う**
- ◆ 管理しているパソコンやサーバで使用している**ウイルス対策ソフトのパターンファイルが自動更新されるように設定する**
- ◆ 休暇中に使用しない**サーバやパソコンの電源を切る**
- ◆ 不測の事態に備え、委託先企業を含めた緊急連絡体制や対応手順を明らかにしておく
- ◆ 自宅で仕事を行うためにデータなどを持ち出す場合、持ち出すデータを最小限にしたり、暗号化するなどのルールを明らかにし、従業員に再徹底する
- ◆ 休み明けには、OSやソフトウェアに修正プログラムを適用し、**最新の状態にする**
- ◆ 休暇中に不審なアクセスがなかったかログを確認する



○ パソコン利用者が取るべき対策例

- ◆ 休暇中、パソコンの電源が切れていたため、ウイルス対策ソフトのパターンファイルが自動更新されていない可能性があるため、**電子メールの受信前及びWebサイトの閲覧前に、パターンファイルを最新の状態にする**
また、OSやソフトウェアについても修正プログラムを適用し、**最新の状態にしておく**
- ◆ ウイルス対策ソフトのパターンファイル更新後に**フルスキャンを行う**
- ◆ 連休中に受信した多数のメールの中に攻撃メールが紛れ込んでいる可能性があるため、**安易に添付ファイルを開いたり、メール本文内のURLをクリックしない**
- ◆ 持ち出したデータなどを会社のパソコンに戻す場合は、必ず**ウイルスチェックを行う**



サイバー犯罪（インターネットに関する犯罪）の通報やご相談は・・・

石川県警察本部生活環境課サイバー犯罪対策室



076-225-0110



cyber@police.pref.ishikawa.lg.jp