別紙

長期休暇中の情報セキュリティ対策に関する注意喚起

1．緊急時の連絡体制の確認

パソコン、データを保管したUSBメモリ等の外部記憶媒体の盗難・紛失といった事案を含む、不測の事態が発生した場合に備えて、緊急連絡体制などの対応手順を再確認してください。

2．コンピュータ及びデータを学外に持ち出す際のルールについて

パソコンやデータ等を学外に持ち出す場合は、許可が必要です。また、許可を得て持ち出す場合も、紛失した場合に備え、適切な暗号化を施してください。

また、学外で業務に使用するパソコンについても適切なセキュリティ対策がなされており、ファイル共有ソフトがインストールされていないことを確認してください。

3．休暇中に使用しないコンピュータ（パソコン・複合機）のシャットダウン

パソコンからログオフをし、必要のないパソコンや複合機は電源を切ってください。業務システムへログオンしたままですと、不正アクセス等のセキュリティインシデントが発生した場合に、被害が甚大となる恐れがあります。

4．ICHOの使用について

ICHOは学外からアクセスが可能となる便利なシステムですが、当該アカウント情報が外部に漏えいした際には、セキュリティ確保の上で大きな問題になります。旅先等でこれらの機能を利用することで、アカウント情報が盗み取られ、悪用される可能性があります。休暇期間中に通常時とは異なる環境からアクセスした場合には、パスワードの変更を行うことを推奨します。

5．修正プログラムの適用、パターンファイルの更新

管理しているサーバーやパソコンのアプリケーションソフトに修正プログラムを適用し、最新のバージョンに更新してください。また、セキュリティソフトの定義ファイル（パターンファイル）を最新な状態に設定すると共に、休み明けにも確認してください。

なお、事務情報ネットワーク接続PCは、シャットダウン時に最新のセキュリティ更新プログラムが適用される仕様となっていますので、業務終了時は必ずシャットダウンするようにしてください。

6．メールの取り扱いについて

休暇明けには、多くのメールを処理する必要があるかと思います。不用意に添付ファイルを開いたり、リンクをクリックしたりすることで、コンピュータウイルスに感染する可能性があります。

本学でもランサムウェアと呼ばれる、感染端末や共有フォルダ内のファイルを暗号化し、復元のための身代金を要求してくる不正プログラムの被害が発生しており、特に注意が必要です。少しでも不自然だと感じたメールの添付ファイルやリンクは、開いたりクリックしたりしないようにしてください。