

長岡技術科学大学 情報セキュリティチェックリスト

一般利用者向け

全教職員（非常勤、派遣を含む）

休暇期間前の対応

- セキュリティインシデント発生時における緊急連絡先の確認
- 業務で使用するパソコンやスマートフォンの OS やソフトウェアに最新のセキュリティ更新プログラムが適用されていること
- 容易に推測可能な文字列（名前、生年月日、電話番号、アカウントと同じ文字列）や安易なパスワード（12345、asdfg、qwerty 等）を設定していないこと。安易なパスワードを設定していた場合は速やかに変更する。
- 業務等で使用する Web サービスで使用する ID やパスワードを他の Web サービスで使い回したりしていないか
- 個人情報などの重要情報をパソコンや USB メモリ等外部記録媒体に入れて、安易に外部に持ち出し等を行わない。（学内規則等の定めに従い、適切な情報管理を行うこと）
- ウィルス対策ソフトを最新のパターンファイルにアップデートした上でフルスキャンを行い、使用しているパソコンにウィルスが潜んでいないか
- 休暇期間中に利用しないパソコンやプリンタ、ファイル共有サーバ等は電源を切る

休暇期間中の対応

- パソコン等の機材、USB メモリ等外部記録媒体等による情報の不要な持ち運びは避け、万一、必要に迫られ持ち運んだ場合には、盗難や置き引き、紛失等の事件が発生しないよう十分に注意する

休暇期間後の対応

- 休暇明けに出勤した後は、まず、ウィルス対策ソフトを最新のパターンファイルにアップデートした上でフルスキャンを行い、使用するパソコンにウィルスが潜んでいないか確認
- 休暇期間中に持ち出したパソコンや USB メモリ等外部記録媒体等は、使用する前に必ずウィルス対策ソフトでフルスキャンを行う
- 休暇期間中に受信する電子メールの中には、ウィルス付きの不審メールが含まれている可能性があるので、確認が出来ていない添付ファイルは、絶対に開封しない。また、不審メール本文に記載された身元不明な URL リンクも絶対にクリックしない。