長岡技術科学大学 情報セキュリティチェックリスト

システム担当者・管理者向け

休暇期間前の対応

□ セキュリティインシデントやシステム障害の発生時等、緊急時に迅速かつ円滑に対応できるよう、関係者間で緊急時の対応要領について確認

□ 特に各担当者の連絡先（携帯電話、メールアドレス）等必ず連絡がとれる連絡先を事前に確認して、関係者間で共有する

　　○報告／連絡すべき担当者（機関内、文部科学省所管担当者）
　　○情報システム運用管理担当部門の担当者
　　○システムベンダー（保守業者等を含む）の担当者
　　○回線業者、データセンターの担当者
　　○その他、必要と思われる（警察、自治体窓口等）連絡先

なお、ホームページの改ざんや個人情報の漏えい等の重大なインシデント発生時は、文部科学省所管課担当者まで迅速に報告すること。

□ 休暇期間中に稼働させておく必要の無い機器（サーバ、システム等）は電源を切る。なお、休暇期間中も稼働しておく必要がある場合は、セキュリティアップデートの実施、パスワード設定、アクセス制御等について見直し、セキュリティインシデント等を発生させないよう注意する。

□ 主要、重要なデータは休暇前にバックアップを実施。またバックアップしたデータが正常に復元できるか確認

□ OS やソフトウェア、CMS やプラグイン等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を確認

□ ウイルス対策ソフトが最新のパターンファイルにアップデートされていることを確認した上でフルスキャンを実施

□ 管理者権限を持つアカウントやパスワードに容易に推測できる文字列（名前、生年月日、電話やアカウントと同じ文字列等）や安易な文字列（test、12345、qwerty 等）が設定されていないことを確認し、問題がある場合は速やかに変更する。

□ Web サイトの管理システム(CMS：WordPress、Joomla!等)のログイン画面に部外者がアクセスできてしまうことが無いか確認。IP アドレスによるアクセス制御や管理者アカウントのパスワードが安易に設定されていないか確認

□ システムの利用者に対して、OS やソフトウェアのセキュリティアップデートを実施するよう周知

□ システムに使用されていないアカウントや退職者アカウント（不要アカウント）が存在していないか確認。存在した場合は、速やかにアカウント削除、無効化を実施

□ タスクスケジューラや cron の設定を確認し、不審なタスクが存在していないか確認。確認された場合は、速やかに調査する。

休暇期間中の対応

□休暇期間中にウイルス感染や不正アクセスの疑い等インシデントの発生を確認した場合は、速やかに当該パソコンやサーバをネットワークから切り離し、所定の連絡先へ報告。判断が出来ない場合でも、所定の連絡先へ報告相談すること。

休暇期間後の対応

□ システムの利用者に対して、休暇明けに出勤した後は、まず、ウイ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イルスが潜んでいないか確認するよう周知

□ 休暇後、電子メールを確認する際には、不審な添付ファイルを開封しない、また、本文に記載された不審な URL にアクセスしないように注意

□ OS やソフトウェア、CMS やプラグイン等に最新のセキュリティアップデートプログラムが公開されていないか確認し、もし公開されている場合はシステムへの適合性を確認した上で速やかに適用する

□ 休暇中に利用者等が持ち出したパソコンや USB メモリ等外部記録媒体等は、使用する前に必ず最新のパターンファイルにアップデートされたウイルス対策ソフトでフルスキャンを行った後で使用させるよう周知

□ 休暇期間中におけるシステムの挙動について不審な点が無かったかどうか、ログ等から確認（例えば、想定されていない IP アドレスからのログインや深夜時間帯のログイン、Web サーバや CMS 等の脆弱性を狙った攻撃が無かったか、不審なファイルが設置されていないか、など）

□ Web サーバで公開しているコンテンツについて休暇前のデータと比較し、改ざんされていないか確認（コンテンツが書き換えられていないか、ウイルスを配布したり、感染させたりするような不正なページに遷移するコードが埋め込まれていないか、など）

□ タスクスケジューラや cron を確認し、不審なタスクが存在していないか確認。休暇前と差異がないか確認。

□ 業務再開時に意図しない不正なアカウントが稼動していないか確認