システム利用者向け

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を確認願います。 □ 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を確認願います。 □ 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を確認願います。安易なパスワードを設定していた場合は速やかに変更願います。 □ 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確認願います。 □ 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よう注意願います。（学内規則等の定めに従い、適切な情報管理を行うようにして下さい。） □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、お使いのパソコンにウイルスが潜んでいないか確認願います。 □ 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、電源を切るようにしてください。

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願います。

休暇期間後の対応
□ 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願います。（休暇前には検出されなかったウイルスが検出される可能性があるため。） □ 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イルス対策ソフトでフルスキャンを行うようにして下さい。 □ 休暇期間中に受信する電子メールの中には、ウイルス付きの不審メールが含まれている可能性がありますので、確認が出来ていない添付ファイルは、絶対に安易に開封しないよう注意願います。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ように注意願います。 □ 万一、不審メールの添付ファイルを開封した場合や、身元不明なＵＲＬリンクをクリックした場合は、速やかにパソコンをネットワークから切り離し、システム管理者に連絡して下さい。

※ キーボードの配列を左から入力したもの

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、今一度確認願います。

□ 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、関係者間で共有願います。

〇報告／連絡すべき担当者（機関内、文部科学省所管担当者）
〇情報システム運用管理担当部門の担当者
〇システムベンダー（保守業者等を含む）の担当者
〇回線業者、データセンターの担当者
〇その他、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、本通知末尾に記載する文部科学省所管課担当者まで迅速に報告願います。

□ 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）は電源を切ってください。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願います。

□ 主要、重要なデータは休暇前にバックアップを実施願います。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をお奨めします。

□ 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願います。

□ 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願います。

□ 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願います。

□ 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願います。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願います。

□ 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徹底願います。

□ 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願います。存在した場合は、速やかにアカウント削除、無効化を実施願います。

□ 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願います。もし確認された場合は、速やかに調査することをお奨めします。

□ ２０１７年１月１日の閏秒の影響について、システムベンダ等に確認しておくことをお奨めします。

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願います。判断が出来ない場合でも、所定の連絡先へ報告相談するよう注意願います。

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徹底願います。（休暇中にウイルス感染したパソコンがシステムに悪影響を与える可能性があるため。）
□ 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願います。
□ 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願います。
□ 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徹底願います。
□ 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、ログ等から確認願います。（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願います。（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願います。休暇前と差異がないか確認願います。
□ 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願います。