令和２年８月７日

教職員各位

総括情報保護管理責任者（CISO）
山　田　　賢

夏季一斉休暇中における緊急時の体制等の再確認と教職員への注意喚起について（依頼）

各教職員におかれましては、日頃から情報セキュリティ対策の維持・向上に取り組まれているところですが、夏季一斉休暇を控えておりますので、再度情報セキュリティ対策を徹底されますようお願いいたします。

夏季休暇中は、業務担当者やシステム管理者、外部委託の業者等が長期に渡り不在になることが想定され、有事の際の対応において予期しない問題が生じることが懸念されます。

また、長期の休暇期間中に教職員が職場外へ業務に関係するデータを持ち出す機会も多くなるものと考えられます。

つきましては、下記記載の事項について遺漏のないよう確認いただくとともに、緊急時における体制について今一度ご確認の上、適切にご対応いただきますようお願いいたします。

記

【全教職員（非常勤、派遣を含む全てのシステム利用者等）向け】
※在宅勤務により困難な場合は、可能な範囲で対応願います。

休暇期間前の対応
(1) セキュリティインシデント発生時の報告に必要な貴部局における緊急連絡先を再確認すること。夜間、休日の対応についても、必要に応じて確認すること。
(2) パソコンやスマートフォンの OS やアプリケーションソフトウェア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すること。
(3) 容易に推測可能な文字列（名前、生年月日、電話番号、アカウントと同一の文字列等）や安易な文字列（12345、asdfg 及び qwerty 等）をパスワードに設定していないことを確認すること。
(4) 業務の Web サービスで利用する ID やパスワードを、他の私的なウェブサービスで使い回していないことを確認すること。併用している場合は、前項(3)を踏まえ、速やかにパスワードを変更すること。
(5) パソコンや USB メモリ等外部記録媒体について、持出しや持込みに関する内規を遵守し、適切に管理すること。また、不要な情報は持ち出さないこととし、媒体に保存する情報は必要最小限にすること。特に要機密情報については、部局情報保護管理者の許可を得ることなく学外に持ち出さないこと。

なお、持出可能な一部の機密情報において、教職員に限り学外のクラウドストレージサービスの利用が認められているのは千葉大 OneDrive のみです。(部局内で定められた利用手順書を参考)

（６） ウイルス対策ソフトを最新のパターンファイルに更新し、フルスキャンを実施して、不正なプログラム等がインストールされていないか確認すること。

（７） 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、電源を切っておくこと。

休暇明けの対応

（１） 出勤後は直ちにウイルス対策ソフトを最新のパターンファイルに更新し、フルスキャンを行うこと。

（２） 休暇期間中にパソコン、スマートフォンの OS やアプリケーションソフトウェア等にセキュリティ更新プログラムが公開されていた場合は、速やかに更新プログラムを適用すること。

（３）休暇中に持ち出したパソコンや USB メモリ等外部記録媒体について、使用前に必ずウイルス対策ソフトでフルスキャンを行うこと。

（４） 休暇中に受信したメールの中には不審なメールが含まれている可能性があるため、添付ファイルは安易に開封しないこと。また、身に覚えのない差出人（メールアドレス）等、少しでも不審を抱いたメールの本文に記載された URL のリンクはクリックしないこと（※差出人は、実在の人物を騙る場合もあります）。

不審なメール報告用アドレス：mail-check[アットマーク]chiba-u.jp

（５） 不審なメールの添付ファイルを開封した時や URL リンクをクリックした場合、パソコンのファイルが意図せず暗号化される等、平常時とは異なる状態に変わる場合があります。このような現象を確認した場合、速やかにパソコンをネットワークから切断し、電源は切らずにシステム管理者へ相談すること。

（６） 業者や関係者、システム管理者等を装って利用者のパスワードや個人情報等を聞き出そうとする問合せ等が発生する可能性があるため、未確認の相手に不用意に情報を伝達しないこと。

◇システムやサーバ等の管理者は、秘密保持契約を締結している事業者に周知願います。
【システムやサーバ等管理者、秘密保持契約を締結している事業者向け】
※在宅勤務により困難な場合は、可能な範囲で対応願います。

休暇期間前の対応

(1) インシデント発生時に迅速かつ的確な対応ができるよう、必要な対応を再確認すること。

(2) インシデント発生時の各担当者連絡先（休日でも連絡可能な電話番号、メール等）を確認して、関係者で共有すること。

○報告／連絡すべき担当者

（情報セキュリティインシデント全般）

C-csirt コアメンバー

内線：2100　E-Mail：c-csirt[アットマーク]chiba-u.jp

携帯：（教職員宛一斉配信メールを参照ください）

○各部局 C-csirt メンバーの連絡先、各部局内システム責任者の連絡先

○システムベンダー（保守業者等を含む）の担当者連絡先

○回線業者、データセンターの担当者連絡先
○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、C-csirt コアメンバー携帯まで迅速に報告願います。

（３） 不要な機器（クライアント、サーバ、システム等）の電源は切断しておくこと。なお、休暇期間中も稼働させる必要のある機器は、不要サービスが稼働していないか、サービスに不要な権限が付加されていないか、不要なアカウントが存在していないか等を確認し、必要に応じて設定を見直すこと。

（４） 万一に備え、重要データはバックアップを実施すること。

○可能であればバックアップデータは正常に復元できるか確認しておき、ネットワークからは隔離された媒体に保管しておくこと。

（５） システムで使用している OS やアプリケーションソフトウェア、ウェブサイト管理システム(WordPress 等の 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かを確認すること。

（６） システムで使用するウイルス対策ソフトを最新のパターンファイルに更新し、フルスキャンを行うこと。

（７） システム管理権限を持つアカウントやパスワードに、容易に推測可能な文字列（名前、生年月日、電話番号、アカウントと同一の文字列等）や安易な文字列（12345、asdfg 及び qwerty 等）を設定してしないことを確認すること。クラウドサービスの管理者権限を持つアカウントについても同様に確認すること。

（８） 管理者権限のアカウントやパスワードを記したファイルを、管理用の端末やストレージ領域の外に格納していないことを確認すること。

（９） ウェブサイト管理システム(WordPress 等の CMS) においてはログイン画面が外部からアクセス可能である場合が多いため、特に管理ログイン ID やパスワードの設定を安易なものにしていないか確認すること。

（１０） ID やパスワードを他のサービスと使い回ししていないか確認すること。

○併用している場合は、前項(7)を踏まえパスワードを変更すること。

（１１） システム利用者に OS やアプリケーションソフトウェア等に最新のセキュリティ更新プログラムを適用するよう、またウイルス対策ソフトの最新のパターンファイルに更新し、フルスキャンするよう周知すること。

（１２） パソコンや USB メモリ等外部記録媒体について、持出しや持込みに関する内規を遵守し、適切に管理すること。また、不要な情報は持ち出さないこととし、媒体に保存する情報は必要最小限にすること。特に要機密情報については、部局情報保護管理者の許可を得ることなく学外に持ち出さないこと。

休暇明けの対応

（１） 出勤後は直ちに各システムのウイルス対策ソフトを最新のパターンファイルに更新し、フルスキャンを行うこと。

（２） 休暇期間中に、システムで使用している OS やソフトウェア等に最新のセキュリティ更新プログラムが公開されているかどうかを確認し、もし公開されている場合は、システムの適合性を関係事業者に確認し、速やかに適用すること。

（３） 休暇中に持ち出したパソコンや USB メモリ等外部記録媒体について、使用前に必ずウイルス対策ソフトでフルスキャンを行うこと。

（４） 休暇中に受信したメールの中には不審なメールが含まれている可能性があるため、添付ファイルは安易に開封しないこと。また、覚えのない差出人（メールアドレス）

等、少しでも不審を抱いたメールの本文に記載された URL のリンクはクリックしないこと（※差出人は、実在の人物を騙る場合もあります）。

不審なメール報告用アドレス：mail-check[アットマーク]chiba-u.jp

（５） 休暇期間中にシステムに不審なアクセスが無かったかをログ等から確認すること。（深夜時間帯のログイン、Web アプリケーションを狙った脆弱性攻撃に関するログなど。）

（６） Web で公開しているコンテンツ等が改ざんされていないか確認すること。（コンテンツの書換え、マルウェア配布する不正ページに遷移させられるようなコードを埋め込まれていないかなど。）

（７） 業者や関係者、エンドユーザ等を装って利用者のパスワードや個人情報等を聞き出そうとする問合せ等が発生する可能性があるため、未確認の相手に不用意に情報を伝達しないこと。

【本件担当】
企画総務部情報企画課情報推進係
内線：2095,2099／Fax：2094
E-mail：jokikaku-suisin[アットマーク]office.chiba-u.jp

【情報セキュリティにおけるインシデント発生時の緊急連絡先】
情報危機対策チーム（C-csirt）
担当：情報企画課情報推進係
内線：2100
E-mail：c-csirt[アットマーク]chiba-u.jp