# 令和４年度情報セキュリティ監査セルフチェック　解説
# システム（一般）利用者用

令和４年度（令和５年１月３０日～２月２６日）に実施しました表題の監査セルフチェックについて、以下正解、望ましい回答と、その解説をまとめました。

ご一読の上、情報セキュリティを守る上でご自身のとるべき行動について、再度ご理解・ご認識いただければ幸いです。

## ■ 1 システム（一般）利用者用

### ■ 1-1 組織／規則編

**■ 1-1-1 パスワードガイドライン遵守**

業務用 E メールアドレス(@yamanashi.ac.jp)に設定しているパスワードについて、山梨大学では使用する文字列に関する注意事項を規定しています。
あなたのパスワードはその規定を満たしていますか。
（末尾のプルダウンから「はい」「いいえ」を選択）

[解説：1-1-1]

学内総合案内 e-Office Navi、
└常設情報
　└情報セキュリティポリシー
　　└利用者パスワードガイドライン
（http://intra.yamanashi.ac.jp/secpolicy/docs/第 7 条 2 号-6_利用者パスワードガイドライン.pdf）
のページに掲載しておりますので、ご一読下さい。

**■ 1-1-2 パスワード再設定**

1-1-1 で「いいえ」を選択した方は、メールを送受信する時に必要なパスワードを再設定（変更）してください。

[解説：1-1-2]

単純なものや、簡単に推測可能なパスワードを使っていたために、メールアカウントを乗っ取られ、そのアカウントからスパムメールを送信された、といった例がいまだに確認されています。ご自身や大学の信用の失墜、他者の迷惑になるだけでなく、情報漏洩のリスクにもつながります。該当者には始末書の提出をしていただくことになります。、パスワードは本学ガイドラインに従って十分に複雑なものにしてください。

■ 1-1-3 電子メールの安全性（情報秘匿性）
あなたは、電子メールは第三者に対して秘匿性の高い通信手段であると思いますか。

正答：
いいえ

[解説：1-1-3]
電子メールを使って学外へメールを送信すると、学外にあるメール転送サーバ機を中継して転送されます。メールは暗号化されずに送信されるため、中継点で傍受されると文面はそのまま覗ける状態です。
このため個人情報等を本文へ記載したり、添付ファイルとそのファイルに必要なパスワードを同一メールで送ったりすることは避けるべきです。

学内のアドレス間でのメール送受信は暗号化されますが、送信先の相手が学外のアドレスへ転送をしたら、学外への送信時と同じ状態になるため、原則、メール本文に重要・機密情報は記載しないようにしてください。

■ 1-1-4 E メール送信時の宛先指定
複数の人に E メールを送信する際、宛先の方々の間でアドレスを知られないようにするためには、どの種類の宛先指定が適していますか。

正答：
BCC

[解説：1-1-4]
BCC とは、Blind Carbon Copy（ブラインドカーボンコピー）の略で、BCC に指定したアドレスは、受信した人には見えません。
複数の宛先へメールを送る場合、送信者にとって支障はなくても、メールの受信者の間ではアドレスや、そのメールの内容が誰に送信されているのかを、他者に知られることは不適切なケースが考えられます。
送付先を全て BCC に指定し、TO に自分のアドレスを指定することで、受信者の間でアドレスやメール内容の共有を避けることができます。多数の宛先にメールを送るときは、配慮をお願いします。

■ 1-1-5 機密情報（個人情報等）の E メール送信
あなたは、個人情報等のデータを E メールに添付して送信することがありますか。

■ 1-1-6
質問 1-1-5 で「はい」と回答した場合、メールそのものを暗号化したり、添付ファイルを暗号化したり、パスワードを設定したりしていますか。

期待される回答：
はい

■ 1-1-7 添付ファイルのパスワード：その伝達方法
パスワード付きの添付ファイルをメールで送信する場合、添付ファイルを開くときに必要なパスワードを送るとき、どのようにしていますか。

期待される回答
△想定外の相手に誤送信した場合にパスワードがわかってしまうことを避けるため、添付ファイルを送ったメールとは別にパスワードを記載したメールを送信する。
○メールの本文は第三者が読める状態で送信されるため、パスワードはできるだけメールとは別の方法（携帯電話、SMS 等）で伝える。

[解説：1-1-5、1-1-6、1-1-7]
1-1-3 の説明通り、メールは一般に平文（暗号化されない状態）で伝送されます。このため、個人情報等の機密データを E メールで送ることは避けましょう。
もしどうしても E メールで送付しなければならない場合は、少なくとも「ファイルにパスワードをかけ」て「添付ファイルで送信」するようにしてください。
ただ、パスワードを、ファイルを添付したメール本文に書いてしまっては、そのメールを傍受した誰でもがファイルの中身を見ることができてしまい、パスワードをかけた意味がありません。メールとは別の方法（携帯電話、SMS 等）で伝えるか、もしどうしても困難な場合は、最低限、添付ファイルとは別のメールで伝えるようにしましょう。本学ガイドラインに沿った複雑なパスワードを郵送等で事前に関係者で共有しておき、以後パスワードのやり取りを一切 E メールでは行わない、というのも一つの方法です。

■ 1-1-8 有害（フィッシング、マルウェア感染）メールでないかチェックしているか
あなたは、届いたメール中にリンクや添付ファイルがあった場合、どのように扱いますか。

期待される回答

・ファイルの拡張子や、URL の正当性を確認してから開く（わからないときは情報システム課に照会する）。

■ 1-1-9 ファイル拡張子を表示しているか(必須)

ウィルス付きの添付ファイルがメールで届くことがあります。そのようなファイルは実行アプリ（～．exe）や、マクロが埋め込まれたエクセル（～．xls/xlsx）や、ワード（～．doc/docx）等、であることが知られています。

これらの「ファイル拡張子」が確認できるよう、パソコンでファイルの拡張子が表示されるように設定することができますが、あなたはどのようにしていますか。

期待される回答

・表示されない状態だが、方法がわかれば表示されるように設定したい

・表示される状態に設定している

[解説：1-1-8、1-1-9]

受信したメール中にリンクや添付ファイルがあった場合、

・リンクは偽装したものでないか

・ファイルが実行可能形式のものでないか

を確認してから開くようにしてください。

外部から山梨大学に直接侵入しようとする攻撃は、ファイアウォールと各サーバによって防がれています。一方メールを使って、不正なファイル（マルウェア）を実行させたり、有害なサイトにアクセスさせたりして情報を盗み取る攻撃は、利用者が十分注意することでしか防げません。

宅配業者の不在連絡や、インターネットバンキング、Amazon や楽天等の通販サイト、クレジットカード会社を騙った「アカウント不正利用を警告」するメッセージ、メールが届くことがあります。

本物そっくりの画面で ID とパスワードを入力させ、アカウントを盗む手口だったりするので、決してクリック（タップ）しないようにしてください。

一方、届いたメッセージが正規のものかどうか、不正なリンクや有害な添付ファイルの見分け方を次に示しますが、もしご自身で判断が難しい場合は情報システム課へご相談ください。

**《不正リンクの見分け方》**

**メール本文に書かれたリンクにマウスポインタをかざすと、実際のジャンプ先 URL がわかります。（またはメールの書式を「HTML」から「テキスト」形式に変更し、該当のリンクが指す URL を確認**

します。）
その URL の「http(s)://」～「直後の/」にある文字列が、企業や組織の正しいドメイン（例：文科省「～.mext.go.jp/」佐川急便「～.sagawa-exp.co.jp/」三菱 UFJ 銀行 「～.mufg.jp/」等）かどうか確認します。
これらが不正な場合は、ほぼ有害なサイトです（アクセスしてはいけません）。

**《有害添付ファイルの見分け方》**

# Windows の場合：エクスプローラを開いて「表示」タブを選択し、（右方にある）「□ファイル拡張子」にチェックを入れ、ファイルの拡張子を表示させます。
添付ファイルを PC に一度保存し、エクスプローラでそのファイルの拡張子を確認します。
拡張子が.exe の場合は、ほぼ有害なファイルです（Wクリックしてはいけません）。
よく使う Office のファイル（xls/xlsx、doc/docx や、マクロの含まれるもの）の場合でも、ApexOne（旧ウィルスバスター）やその他の対策ソフトでスキャンをかけてください。

■ 1-1-10 業務中の WEB 閲覧(必須)
あなたは、業務に関係のないホームページにアクセスしたり、好奇心や興味本位でリンクやバナー、ボタン等をクリックしたりしてしまうことがありますか。

期待される回答
・業務上必要な情報を騙った不正なリンクの場合があるので、すぐにはクリックしないように注意している
・業務上無関係な情報は、クリックしない

[解説：1-1-10]
業務 PC で、業務に関係のない WEB サイトにアクセスしないようにしてください。業務に無関係なサイト（WEB ページ）を閲覧することは適切ではありません。
また業務との関係の有無によらず、ページにあるバナー広告をクリックしたことで、不適切なソフトウェアがインストールされ、有料サービス購入等を促すポップアップが繰り返し表示されるようになったり、外部から不適切なソフトウェアがダウンロードされたりといったケースが見つかっています。バナー広告にはアクセスしないよう、ご注意ください。

■ 1-1-11 ファイル共有（P2P）ソフトウェアの使用(必須)
あなたは、業務用パソコンや自宅のパソコンに「P2P 型ファイル共有ソフト」をインストールして利用していますか。（ファイルサーバでファイルを共有する方法は除きます。）

正答

・いいえ

[解説：1-1-11]

本学では、有名な Winny に代表される、他の PC と直接ファイル交換ができる P2P ソフトウェアの使用を禁止しています。これは、著作権侵害の恐れがあることに加えて、保有する情報の漏洩や、マルウェア感染等の危険性があるためです。

もし教育研究目的で使用する場合であっても、例えば研究室に閉じたネットワークで使用する等、問題が起きない環境で使ってください。これが守れない場合は PC へインストールしないでください。

本学の規程に反する行為が原因で（禁止事項を守らず）、保有している機密情報が本学から外部へと漏洩する等があった場合、本学の社会的信用が大きく損なわれるだけでなく、当事者には罰則が適用されることになります。規則に則った運用をお願いします。

■ 1-1-12 ウィルス対策（ワクチン）ソフトウェアの使用(必須)
あなたは「業務用パソコン」でウィルス対策を有効化していますか。

期待される回答：

・している

[解説：1-1-12]

本学では、学内で利用する PC について、ウィルス対策ソフトの使用を規定により義務付けています（『情報機器取扱ガイドライン』5 条、5.2 項）。原則、ウィルス対策ソフトのインストール、ウィルス対策機能の有効化をお願いします。

■ 1-1-13 ウィルス対策（ワクチン）ソフトウェア不使用の理由
前問で「していない」と回答した場合、その理由を記入してください。

[解説：1-1-13]

業務で PC を使用していない場合や、業務用のファイルを一切使用しない場合、病院用端末等でインターネット不使用の場合は、ウィルス対策ソフトウェア不使用でも問題ありません。

一方、使用頻度が低くても、USB メモリ等で他の PC からファイルを持ち込んだり、業務用のファイルを扱ったり、インターネットにつないだりする PC なら、ウィルス対策ソフトをインストールしておく必要があります。業務用の PC であれば、大学が公開している ApexOne（ウィルスバスター）のインストールが可能ですので、ご利用ください。

インストールの手順がわからない、という回答が複数寄せられましたが、総合情報戦略機構の WEB ページ：https://sojo.yamanashi.ac.jp/services/software/virusbuster/
に公開されていますのでご覧ください。

また、業務に使用している PC にウィルス対策ソフトが入っているかどうかは、ご自身で認識しておいてください。PC 管理担当や上司などに聞く等して確認することを推奨します。

■ 1-1-14 自宅パソコンの有無(必須)
あなたは、自宅用のパソコンを持っていますか。

■ 1-1-15 自宅パソコン（PC/Mac）でのウィルス対策（ワクチン）ソフトウェアの使用(必須)
あなたは、「自宅のパソコン」にウィルス対策を有効化していますか。

期待される回答：
・はい

[解説：1-1-15]

本学では、自宅 PC の業務使用を制限していませんが、その代わり自宅の PC を仕事に使ったり、大学のメールを扱ったりする場合、学内で利用する PC と同等のセキュリティ対策を講じていただく必要があります。

また学内の PC と自宅の PC との間で USB メモリを使用する場合、USB メモリを介したコンピュータウィルス感染を避ける必要があります。

このような理由から、自宅の PC にもウィルス対策を実施していただきたいと考えています。

大学の業務を自宅 PC で一切しない、自宅 PC で大学のネットワークサービス（メール、その他）に一切アクセスしない場合はこの限りではありませんが、自宅 PC での十分な対策を怠って、本学に影響するセキュリティ上の事故等を引き起こした場合は、就業規則による罰則が適用されることがある点にご注意ください。

■ 1-1-16 自宅パソコンでのウィルス対策（ワクチン）ソフトウェア不使用の理由
前問で「していない」と回答した場合、その理由を記入してください。

[解説：1-1-16]

自宅に PC を所持していない場合や、インターネットに一切接続しない場合は問題ありません。一方メールしか使用しない場合でも、添付ファイルのやり取りが発生する場合はウィルス対策ソフトウェアのインストールが必要です。

その他も含め、[解説：1-1-14]に記載した理由から、自宅 PC であってもウィルス対策ソフトのインストールを規定しています。

■ 1-1-17 不正ソフトウェア対策機能の更新（アップデート）(必須)
あなたは、利用する業務用パソコンや自宅のパソコンのウィルス対策機能（ウィルスバスターやWindows Update の更新プログラム等）を最新の状態になるよう更新する必要があることを知っていますか。

期待される回答：
・はい

[解説：1-1-17]
本学では『情報機器取扱ガイドライン』5 条、5.2 項で、利用している端末の OS、アプリケーションを定期的に最新の状態にアップデートすること、端末にウィルス対策ソフトウェアをインストールし、ライセンスの有効期間に注意して、ウィルス情報データベースは常に最新に保っておくことを義務付けています。

■ 1-1-18 パソコンのウィルス対策機能の更新（アップデート）実施(必須)
実際に、業務用パソコンや自宅のパソコンの不正ソフトウェア対策機能（ウィルスバスターやWindows Update の更新プログラム等）を最新の状態になるよう実施（自動更新の設定も含む）していますか。

期待される回答：
・はい

[解説：1-1-17、1-1-18]
ウィルス対策ソフトをインストールしたり、Windows Defender を有効化したりしていても、最新でなければ、新しいタイプのウィルス、不正ソフト（マルウェア）に対処できません。
このため、PC 起動後はインターネットに接続し、ウィルス対策ソフトウェアやパターンファイルの更新、Windows Update の実行をしてから PC を使用するようにしてください。インターネットへの常時接続環境で使用する場合は、自動更新を ON にして使用してください。

■ 1-1-19 パソコンのウィルス対策機能の更新（アップデート）を実施しない理由
前問で「実施してしない」と回答した場合、その理由を記入してください。

[解説：1-1-19]
利用する業務用 PC や自宅の PC がない場合は問題ありません。
但し、業務用 PC や自宅の PC をインターネットに接続しない場合でも、USB メモリや他の外部記憶媒体を使用することがあれば、対策を講じておく必要があります。

ウィルス対策をしていない PC は無防備な状態です。

USB メモリや他の外部記憶媒体を、インターネットに接続でき、OS やウィルス対策ソフトが最新になっている PC でウィルスチェックを行い、安全が確認できてからインターネットに接続しない PC へ挿すようにしてください。これを怠り、インターネット未接続の PC にウィルスを感染させたという例が実際に発生しています。

■ 1-1-20 外出先での無線ネットワーク（無線 LAN/Wi-Fi/モバイルルータ等）の利用(必須)
あなたが外出先から山梨大学内のシステムにアクセスする必要があった場合に使用するものを回答してください。

期待される回答：
○「eduroam」や持参した「モバイルルータ」

■ 1-1-21 ホテルの Wi-Fi やフリーWi-Fi 等の使用禁止(必須)
ホテルの Wi-Fi やフリーWi-Fi 等のネットワークは、通信が暗号化されていないことが多く、情報を詐取される危険性があるため、利用を禁止されていることを知っていますか。

[解説：1-1-20、1-1-21]

フリーWi-Fi の SSID(接続先 Wi-Fi サービスの名前(文字列)。)と同一の SSID を使った、悪意のある Wi-Fi アクセスポイントを設置して、利用者の個人情報を盗み取る手口が存在します。

このため本学では、フリーWi-Fi を使用することを禁止しています（『情報機器取扱ガイドライン』7 条、7.1 項、(3))。モバイルルータや、スマートフォンのテザリング等を使用してください。

■ 1-1-22 SNS/ブログ等への、秘密情報公開の禁止(必須)
あなたは、Twitter や Facebook/Instagram 等の SNS やブログに業務上知りえた機密（重要）を掲載してはいけないことを知っていますか。

■ 1-1-23 SNS への情報公開に関する判断(必須)
研究室で大きな成果が上がったり、関係していた患者の手術が成功したりといったうれしいことがありました。あなたはそれを Twitter や Facebook/Instagram、その他の SNS（Line/Mixi/他）に掲載したい衝動に駆られました。
実際に取るべき行動はどのようなものでしょうか。
# 広報担当としての正式な活動や、公式な業務による掲載を除きます。

期待される回答：
○掲載しない

△掲載したら誰にどんな影響が及ぶかわからないので、慎重に判断する。

[解説：1-1-22、1-1-23]

学内で得た情報を、SNS やブログ等の不特定多数の目に触れる媒体に公開することを禁止していませんが、「問題ないだろう」と思った情報でも、その掲載によって意図しない影響が他の人に及んだり、機密情報が漏洩してしまったりという可能性がありますので、原則公開しないようにしてください。

但し大学・学内組織の広報で、関係者の了解のもと、情報を公開する場合は除きます。

■ 1-1-24,25 私用モバイル端末利用実態(必須)
あなたは、（大学から与えられたアカウントの）業務用メールの確認などの業務に、個人所有のモバイル端末（PC/Mac を除く、スマートフォン、タブレット）を利用していますか。利用している場合、端末の種類についてお答えください。

■ 1-1-26 私用モバイル端末の OS 更新
モバイル端末を業務に利用している場合、「ＯＳ（ソフトウェア）の更新」のお知らせが届いた場合、どうしていますか。

[解説：1-1-24、1-1-25、1-1-26]

モバイル端末の使用に関しても、PC と同様、セキュリティ対策の徹底を規定しています。これは業務（仕事）用と自宅用の PC のところで説明したのと同じです。

■ 1-1-27 私用モバイル端末の OS 更新を実施しない理由
質問 1-1-26 で「実施していない」と回答した場合、その理由を記入してください。

[解説：1-1-27]

モバイル端末では、特にスマートフォンであればキャリア回線を通じて更新が通知されます。タブレットの場合はインターネットに接続した状態で更新が通知されます。更新の通知や更新の方法は、ネット検索等で確認し、各自行うようにしてください。

OS に、特にセキュリティ上の脆弱性が発見されると、修正版が公開されます。修正版リリースの通知を受けたら、速やかに適用し、セキュリティ上の脆弱性がない状態にしておいてください。

■ 1-1-28 私用モバイル端末での不正ソフトウェア対策
モバイル端末を業務に利用している場合、不正ソフトウェア対策機能（ウィルスバスター等）を使用していますか。

[解説：1-1-28]

モバイル端末の使用に関しても、PC と同様、セキュリティ対策の徹底を規定しています。これは業務（仕事）用と自宅用の PC のところで説明したのと同じです。

■ 1-1-29 私用モバイル端末での不正ソフトウェア対策機能、不使用の理由
質問 1-1-28 で「使用していない」と回答した場合、その理由を記入してください。

[解説： 1-1-29]

私用モバイル端末を所持していない場合は問題ありません。不正ソフトウェア（ウィルス）対策アプリがない、知らない、という場合は、端末を購入した販売店に相談する、ネットでウィルス対策ソフトを検索するなどして、適切なものを使うようにしてください。

iPhone の場合、Apple Store からダウンロードしたアプリについては、不正なアプリをインストールしてしまうリスクはほぼありませんが、SMS やメールで送りつけられるファイルや URL 等からフィッシングサイトにアクセスして重要情報を窃取されたりするリスクは抑えられません。

このため不正サイトへのアクセスをブロックする機能を備えたソフトウェアをインストールするようにしましょう。

■ 1-1-30 私用モバイル端末での不正ソフトウェア対策機能、最新化（更新）
私用モバイル端末での不正ソフトウェア対策機能を「使用している」と回答した場合、不正ソフトウェア対策機能（ウィルスバスター等）やパターンファイルのアップデートを行い、常に最新の状態にしていますか。

[解説：1-1-30]

モバイル端末の使用に関しても、PC と同様、セキュリティ対策の徹底を規定しています。これは業務（仕事）用と自宅用の PC のところで説明したことと同じです。

■ 1-1-31 私用モバイル端末での不正ソフトウェア対策について、最新化していない理由
質問 1-1-30 で「アップデートを行っていない」と回答した場合、その理由を記入してください。

[解説：1-1-31]

モバイル端末のセキュリティ対策アプリは、自動的更新の機能を持っていますので、可能な限り有効にしてください。面倒がらず、速やかに更新するようにしましょう。

■ 1-1-32 私用モバイル端末での「供給元不明アプリ」インストールに関する設定
モバイル端末を業務に利用している場合、「供給元不明アプリ」はインストールしない設定にしていますか。

[解説：1-1-32]

本学では『情報機器取扱ガイドライン』5 条 5.3 項で、「出所の定かではないソフトウェアをインストール、使用してはならない」と規定しています。Android 端末では「供給元不明アプリをインストールしない」設定とすれば OK です。

ただ正規のソフトウェアでも、供給元不明アプリのインストールを許可しないとインストールできないことがあります。その場合は一時的に許可して、インストールが終わったら不許可に戻す、ようにしてください。

一方 iPhone や iPad 等では、Apple 社による審査をパスしなければアプリを Apple Store に公開できないため、Apple Store 以外からアプリをインストールしなければ OK です。

但し、iPhone/iPad で Apple Store を経由せずにアプリをインストールすることは可能です。安易にインストールして事故につながることの無いよう、信頼できるアプリかどうか慎重に判断してください。

■ 1-1-33 私用モバイル端末で「供給元不明アプリ」をインストールする設定にしている理由

質問 1-1-32 で「インストールする設定にしている」と回答した場合、その理由を回答してください。

[解説：1-1-33]

上記[解説：1-1-32]に記載している通りです。

■ 1-1-34 「情報格付け取扱い手順」、内容の確認状況(必須)

平成 29 年 9 月 1 日に制定された「情報格付け取扱い手順」

（http://intra.yamanashi.ac.jp/secpolicy/docs/第 17 条-6_情報格付け取扱手順.pdf）

の内容を確認していますか。

[解説：1-1-34]

本学で取り扱う様々な情報については、格付けを行い、その格付けに応じて適切な取り扱いをするよう規定しています。内容確認の上、実運用にのせるようお願いします。

■ 1-1-35 「情報格付け取扱い手順」に対するご意見

「情報格付け取扱い手順」に、今後必要に応じ、見直しをする予定です。より良い改定に向けて、ご意見がありましたらお願いします。（自由記述）

[解説：1-1-35]

この質問については、難読、難解、具体例がほしい、わかりやすく要点をまとめたものがほしい、

といったご意見、ご要望をいただきました。平易化、具体化に向けて対応を進めたいと考えています。

■ 1-1-36 「外部記録媒体取扱手順」、内容の確認状況(必須)
平成 30 年 12 月 1 日に制定された「外部記録媒体取扱手順」(http://intra.yamanashi.ac.jp/secpolicy/docs/第 7 条 2 号-8_山梨大学外部記録媒体取扱手順.pdf)の内容を確認していますか。

[解説：1-1-36]
本学では、外部記録媒体取扱手順により、USB メモリや外付け HDD の取扱に関する事項を定めています。この定めに従って適切な取り扱いをするようお願いします。

■ 1-1-37 「外部記録媒体取扱手順」へのご意見
「外部記録媒体取扱手順」については今後必要に応じ、見直しをする予定です。より良い改定に向けて、ご意見がありましたらお願いします。(自由記述)

[解説：1-1-37]
この質問についても、難しい、わかりやすく要点をまとめたものがほしい、教員向けの手順例がほしい、といったご意見、ご要望をいただきました。対応を進めたいと考えています。

■ 1-1-38 重要データのバックアップ(必須)
あなたは重要な電子データ（それがなくなると、仕事が継続できなくなったり、賠償責任が生じたりするようなもの）について、バックアップをどのように取っていますか。

[解説：1-1-38]
本学では、『情報システム運用・管理内規』「第４９条」にて、情報のバックアップを実施することを規定しています。情報の格付に応じて、適切な方法で取得するようにしてください。
またバックアップは、ファイルが入っている元の PC とはなるべく別の媒体に取得するようにしてください。PC が故障してしまうと元のファイルもバックアップも失われるためです。

■ 1-1-39 監査へのご意見
今回の情報セキュリティ監査に関して、ご意見等がありましたらお願いします。(自由記述)

[解説：1-1-39]

▽ご意見・ご要望

▼A.良い機会となった

1)監査を受けながら学習する機会になった。

2)最後の確認の項目のように申請・回答の中に研修的な内容が含まれるのは大変有効ですね。

3)コーヒーブレイクのような、対応に注意する事例などは、ありがたい情報です。

4)1-1-CFB はしりませんでしたので勉強になりました。ありがとうございます。

5)の監査のアンケートを踏まえて、自分のパスワードを変更した経験がある。監査のアンケートに回答しながら、自分自身のセキュリティに対する対策がどの程度安全で知識として不足していないかと心配に感じる。学校に情報担当者もいるので、セキュリティポリシーを学校として策定しているものの、大切な内容が周知できるよう、担当者を中心として確認する機会が必要だと感じた。

6)今後も逐一、自分の環境を確認していきたい。

回答）

ご感想、ご意見ありがとうございます。

この監査が、回答くださる皆さんにとって、いくらかでも有益と感じていただけるよう、今後も工夫を重ねていけたらと考えております。

▼B.分かりやすい（易しい）

1)"わかりやすい内容"

▼C.分からない内容が多い（難しい）

1)聞きなれない用語が多く、実際に自分は更新等ができているのかわからなかった。改めて確認していきたい。

2)まだよく分からないので何か機会があれば講演会？現在はユーチューブなどで講座してほしい

3)まったく解らない

4)"良くわからない事がおおい"

回答）

総合情報戦略機構、情報システム課では、本学教職員の皆さんの情報セキュリティに関する知識、スキル向上のため、学習教材の提供、講演会・研修会の開催、各種情報の提供を行っており、今後も継続いたします。そのような資料や機会を、是非ご活用ください。

▼D.回答提出（確定）できたかどうかがわかりにくい、システムが良くない
1)回答 2 回目です。
2)一度回答したのに、未回答になっていた。
3)たくさんの質問に回答を終えてほっとして終了したと誤解し，自分の回答表示末尾の回答？ボタンを押さずに Web ページを離れてしまい未回答者リストに入るミスを複数回やってます．冒頭の回答指針に提出完了操作についてアドバイスを載せておいてほしいです．あるいはこの確認ミス自体にセキュリティのような緻密なチェックが必要な活動に対するスキル向上を狙っていますか？
4)クリック選択するには UI が悪すぎる
5)一度回答しおえましたが、クリック後に真っ白になったことから気力を削がれました。

**回答）**

回答を提出するには、「確認」ボタンをクリック後、さらに「回答」ボタンを押す必要があります。これは一度記入した内容を「確認」いただき、修正があれば戻るための仕組みですが、それが分かるよう、確認画面上に「※まだ回答は完了していません。最下部の[回答]ボタンを押してください」と表示するようにシステムを変更しました。

またいただきましたご意見を踏まえ、可能な限り今後も改善に努めます。

▼改善提案
1)以下の質問に「外部記録媒体登録管理者台帳」及びそれに関連する質問がありますが、そのようなものを使用する必要がありませんので「準備中」でもなければ「継続している」でもありません。回答として「その他」があればよかったと思います。
2)最初の方の質問項目は基本的事項なので，結果次第では質問項目に含めなくても良いのでは無いでしょうか。
3)パスワードを変更する場合は，こちら，など方法等も記載してもらえると助かります。今回は内線でお聞きしましたが。

**回答）**

いただきましたご意見を参考に、設問改善を検討いたします。

▼量が多い
1)重要な点ばかりだが設問が多いと感じました。

2)私が勝手に考えますに回答率が低いのは

・質問項目も文字数も多く業務時間中におこなうには時間がとられすぎる
・今や小中学校で習うような情報セキュリティの話が多く、それより上の世代でも講習で聞いたものばかりでチェックの意義を感じられない

以上の 2 点がネックなのではないでしょうか。

少なくとも 2023.2.22 の 23 時までもう一度回答しなおそうと考えられなかったのはこの 2 点があるからです。

以上、2 時間かけて回答を終え、返信いたします。"

3)確認事項が多すぎる。字数も多く頭に入ってこない。

4)この調査内容は長すぎて質問が多すぎて、何度も最後まで辿り着かず、再開して確定するとエラー表示となり、繰り返す必要が生じるため、多大な時間を要する。調査方法と内容を検討して頂きたい。質問の内容がわからず、回答に困ることや、わからない場合の回答方法がないが、必須で入力しないと進めないため、どこかに回答している。

**回答）**

いただきましたご意見を参考に、監査実施方法を含め、回答者の負荷軽減策を検討いたします。

一方「チェックの意義を感じられない」というご意見ですが、学内には様々な情報セキュリティ・スキルの方がおられることを念頭に設問を用意しております点を考慮いただければ幸いです。

▼職業倫理

1)業務中に長時間 Web サイト（Yahoo、漫画サイト等）を閲覧している人がいるので、時々履歴チェックを自動で行い監視している等、勧告して防止することを検討した方がよいように感じます。

**回答）**

情報システム課では、システム利用者の Web サイト閲覧歴を常時、監視しているわけではありません。また、大学職員の業務内容は様々であって、たとえば、ニュースのサイトなどを閲覧するのが業務外なのかどうか、一律に判断することは難しいです。

一方で、当該部署から依頼を受けて、特定の職員の Web サイトの閲覧歴の情報提供を監督者に対して行ったこともあります。今後も、監督者からの依頼があれば、可能な範囲で情報提供を行います。

末筆ながら、この度は情報セキュリティ監査セルフチェックにご協力をいただき、ありがとうございました。次回以降も、どうぞよろしくお願いいたします。

以上