令和５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５年度（令和５年１２月１日～令和６年１月２３日）に実施しました、表題の監査セルフチェックについて、以下正解及び望ましい回答と、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

本学が付与するメールアドレス(@yamanashi.ac.jp)のパスワードについては、使用する文字列に関する要件を規定しています。
あなたのパスワードはその要件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、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、容易に推測可能なパスワードを使用することは、乗っ取り等の不正アクセス被害に遭うリスクの増大につながります。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。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 E メールの安全性（情報秘匿性）
あなたは、E 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]
E 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るため、通信経路上で傍受されるリスクが存在します。また、宛先を誤って送信するリスクも存在します。
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。

■ 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、アドレスが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、受信者間で意図せずアドレスが共有されること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（個人情報含む）の E メール送信
あなたは、個人情報等を含む機密情報を E メールに記載、または添付して送信することがありますか。

■ 1-1-6 E メールに機密情報を添付する場合の対応
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：

・1-1-5 いいえ

・1-1-5 はい→1-1-6 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

・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、個人情報等の機密データを E メールで送ることは避けるべきですが、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」し「パスワードをメールとは別の方法で共有」するようにしてください。

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もがファイルの中身を見ることができ、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）で伝えましょう。なお、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手法は、誤送信や傍受等のリスクに対して脆弱であり、推奨されません（添付ファイルを送付した際と同一の経路･手順を辿る可能性が高いため）。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、届いたメール中に添付ファイルやリンク（URL）の記載があった場合、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

ウイ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

・常時表示している

・必要に応じて表示している

[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。一方メールを使い、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等が確認されているため、正規のメッセージやメールであることを確認できない場合は、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）。

《ファイルの拡張子の表示方法･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。

Mac の場合：Finder を開いて「設定」の中の「詳細」を選択し、「すべてのファイル名拡張子を表示」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と種類を確認します。拡張子が.exe の場合や、ファイルの種類が「アプリケーション」で拡張子以外の部分に exe が含まれている場合は、ほぼ有害なファイルです（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 やマクロを含むもの）の場合でも、ApexOne（旧ウイルスバスター）やその他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関わらず、ページにあるバナー広告をクリックしたことで、有料サービス購入等を促すポップアップが繰返し表示されるケースや、外部から不適切なソフトウェアがダウンロードされるケース等が確認されています。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

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

・インストールしていない

[解説：1-1-11]

本学では、他の PC と直接ファイル交換ができる P2P ソフトウェア（Winny 等）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。

教育研究目的の場合、研究室内の閉じたネットワークで使用する等、P2P ソフトウェアの利用に係る問題が起きない環境に限り、使用することを許可しています。利用に際し安全を確保できない場合は 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）、保有す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、当事者には就業規則による懲戒処分が下されることがあります。規則に則った運用をお願いします。

■ 1-1-12 業務パソコンでのウイルス対策の有効化
あなたは「業務用パソコン」でウイ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、ウイ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、ウイルス対策ソフトのインストール、ウイルス対策機能の有効化をお願いします。

■ 1-1-13 業務用パソコンでのウイルス対策不使用の理由
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、ウイ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、インターネットに接続することがある PC なら、ウイ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（ウイルスバスター）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につきましては、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 にウイ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 個人所有パソコンの有無
あなたは、個人でパソコンを所有していますか。

■ 1-1-15 個人所有のパソコン（PC/Mac）でのウイルス対策の有効化
あなたは、「個人所有のパソコン」にウイルス対策を有効化していますか。

期待される回答：
・1-1-14 はい→1-1-15 している
・1-1-14 いいえ

[解説：1-1-4、1-1-15]

本学では、個人所有 PC の業務使用を制限していませんが、その代わり個人所有 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 と個人所有 PC との間で USB メモリを使用する場合、USB メモリを介したウイルス感染を避ける必要があります。

このような理由から、個人所有 PC にもウイルス対策を実施していただきますよう、お願いいたします。

大学の業務を個人所有 PC で一切しない、個人所有 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、個人所有 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、就業規則による懲戒処分が下されることがある点にご注意ください。

■ 1-1-16 個人所有のパソコンでのウイルス対策不使用の理由
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]

個人所有 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イ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、個人所有 PC であってもウイ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 パソコンのウイルス対策機能の更新（アップデート）
あなたは、利用する業務用パソコンや個人所有のパソコンのウイルス対策機能（ウイルスバスターや OS 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、端末にウイ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、ウイ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 パソコンのウイルス対策機能の更新（アップデート）実施
実際に、業務用パソコンや個人所有のパソコンのウイルス対策機能（ウイルスバスターや OS 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：
・実行している

[解説：1-1-18]
ウイ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、新しいタイプのウイルス、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、ウイルス対策ソフトウェアやパターンファイルの更新、OS の更新プログラムの適用をしてから 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 パソコンのウイ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「実行してしない」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 や個人所有 PC がない場合は問題ありません。
但し、業務用 PC や個人所有 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、それらの媒体を介してウイルスに感染する可能性があるため、対策を講じておく必要があります。
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 やウイルス対策ソフトが最

新になっている PC でウイ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 にウイルスを感染させた事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
あなたが外出先から本学のシステムにアクセスする必要がある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「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
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、情報を窃取される危険性があるため、業務で使用することは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）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、正規の Wi-Fi になりすまして利用者の接続を誘導し、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、機密（重要）情報公開の禁止
あなたは、X（旧 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
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 X（旧 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。
広報担当としての業務による掲載を除きます。

期待される回答：
・〇掲載しない
・△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は禁止していませんが、「掲載して問題ない」と判断した情報でも、その掲載により意図しない影響が他者に及ぶ可能性や、機密情報が漏洩する可能性があるため、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 個人所有モバイル端末利用実態

あなたは、業務用メールの確認などのために、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 個人所有モバイル端末の OS 更新

個人所有の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（『情報機器取扱ガイドライン』）。これは PC に係る各項目で説明した内容と同じものです。

■ 1-1-27 個人所有モバイル端末の 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]

更新の通知や更新の方法は、ご利用の端末の種類に応じて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ください。

■ 1-1-28 個人所有モバイル端末での不正ソフトウェア対策

個人所有の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（ウイルスバスター等）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（『情報機器取扱ガイドライン』）。これは PC に係る各項目で説明した内容と同じものです。

■ 1-1-29 個人所有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]

個人所有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（ウイルス）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、ネットでウイ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、App 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る等の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 個人所有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）
個人所有の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（ウイルスバスター等）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（『情報機器取扱ガイドライン』）。これは PC に係る各項目で説明した内容と同じものです。

■ 1-1-31 個人所有モバイル端末での不正ソフトウェア対策機能について、最新化していない理由
質問 1-1-30 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：1-1-31]

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 個人所有モバイル端末での「供給元不明アプリ」インストールに関する設定
個人所有の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。

■ 1-1-33 個人所有モバイル端末で「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：1-1-32、1-1-33]

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」設定を行ってください。

ただし、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 App Store に公開できないため、App Store 以外からアプリをインストールしなければ問題ありません。

但し、iPhone/iPad で App 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。

■ 1-1-34 多要素認証の利用状況

総合情報戦略機構では、情報セキュリティの向上を図るため、2023 年 6 月 15 日から多要素認証を試験導入していますが（https://board.yamanashi.ac.jp/?b=102&k=2023061576384）、これを利用していますか？

■ 1-1-35 多要素認証を利用しない理由

質問 1-1-34 で「利用するつもりはない」と回答した場合、その理由を回答してください。

[解説：1-1-34、1-1-35]

同設問における多要素認証とは、従来の認証方式である ID と PW に加え、モバイルアプリや SMS や電話を介した本人確認を行う機能を指します。Microsoft が公開した情報によると、多要素認証を利用することで、アカウントに対する攻撃の内「99.9%」を防ぐことが出来るとされています。同機能の利用によりアカウントが盗用されるリスクを大幅に軽減出来るため、積極的な導入をお願いいたします。

なお、現在は試験導入段階にあり利用は任意となっておりますが、将来的には多要素認証の強制化も計画している為、その際にはご理解ご協力のほど、よろしくお願いいたします。

■ 1-1-36 「外部記録媒体取扱手順」、内容の確認状況

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]

難しい、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。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

あなたは重要な電子データについて、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』49 条により、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、適切な方法で実施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 情報セキュリティ監査に関する意見

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]

①内容が難しい・量が多い旨のご意見

- 日頃使わない言葉が多く、監査の意味が無い。情報関係が苦手な職員に向けて注書きをいれるべきだと思う。
- 知識不足でよく分からない。
- 素人にも分かる設問をお願いします。また、質問が難しい場合にも自由記述欄を設けてもらえると助かります。次の USB に関する設問も、全員が USB を使用して業務をしている体の回答になっており、業務上関わっていない人（USB を使用する必要のない人）が回答できる答えがありません。「そのような業務に携わっていない」という回答を準備してほしいです。
- 質問数が多くて手間がかかるので、もう少し簡素化していただけると助かります。
- やっぱり長い

【①への回答】

いただいたご意見を参考に、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。

②良い機会となった・内容が分かりやすい旨のご意見

・情報セキュリティについての資料を読んで、内容についての問いに答える課題が、以前必修とされたが、知らないことも多かったので良かった。ありがたかった。外部媒体等取扱手順など、校内の情報担当者から大事なことは周知する機会があると良いと思う。

・昨年までの物に比べ、答えやすい。

【②への回答】

ご感想、ご意見ありがとうございます。今後も工夫を重ねていけたらと考えております。

③改善提案（設問内容）

・メールでも回答方法を記載してほしい。掲示板から探すのは非常に手間がかかる。

・PC を使用した業務は行なっておりません。回答は毎回、スマホから行なっております。そのような職員に対応したセキュリティ監査の項目を増やしていただけたらありがたいです。

・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）の利用に関連して、VPN に関する設問がないのは確認が不足していませんか。また、スマホから携帯会社の回線を通してアクセスする場合に該当する選択肢がわかりません。

・①1-1-20 の回答一覧に「外出先からはアクセスしない」の選択肢があると良い。もしくはアクセスすることが前提条件の質問だとすると、「アクセスしたことがない場合や実際にはアクセスすることがない場合でも～」のような質問にした方が良い気がする。②1-1-38 の質問は少しわかりにくい。業務上のデータの事なのか、もしくは業務とは全く関係ないデータに関して普段はどうバックアップしているのかも含めた質問なのか迷った。回答としてはプライベート的な普段のことを答えた。

・自分の PC を使用していない人への配慮が足りない

・「1-1-5 機密情報（個人情報含む）の E メール送信」に関連して，DX を理由に，事務から個人情報（家族の氏名や生年月日等）の含まれたファイルがパスワードも付けずにメールに添付されてくることがありました．どこまでがこの「1-1-5」の範囲となっているのでしょうか？

【③への回答】

いただいたご意見を参考に、設問内容の改善を検討いたします。

④改善提案（システム面）

・業務効率を優先することを考えると、前職の企業に勤務していたころと比較してセキュリティがかなり甘い（危うい）と感じています。予算面で難しいとは思いますが、ICT 企業が社内で

行っている手段に準じるシステム面および体制面の強化を行うべきだと思います。

【④への回答】
いただいたご意見を参考に、改善を検討いたします。

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