令和３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３年度（令和４年２月～令和４年３月）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、その添付データにパスワードを設定したり暗号化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ファイル共有（P2P）ソフトをインストールして利用していますか。

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 等の不特定多数が利用する機器を利用して、山梨大学内の情報システムにアクセスすることは、パスワードを詐取される危険性が高いため、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]
山梨大学内の情報システムのいくつかは、外部から利用することが可能ですが、一般に、フリーWi-Fi を使用すると、ID とパスワード等の情報が傍受され、パスワードを窃取される危険があります。
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
1) パスワードの変更方法がわかる手順を掲示して欲しいです。

学内ネットワークサービス全般の利用手順等については、本学総合情報戦略機構の WEB サイトに載っています。
パスワードの変更方法（手順）については、
https://sojo.yamanashi.ac.jp/manuals/password/
をご覧ください。

2) ホテルが提供する Wi-Fi を使用するしか選択肢が無い場合に、PC で業務用メールを安全に確認する方法を教えて下さい。

事前に、ホテル等が提供する無料 Wi-Fi 以外を利用する選択肢を持つようにしてください。[解説：1-1-20、1-1-21]にありますように、モバイルルータやスマートフォンのテザリング等の使用を検討してください。短期使用が可能な、モバイルルータのレンタルサービス等もあります。
業務用メールのみであれば、Web 版、アプリ版共に HTTPS(SSL/TLS)により通信が暗号化されているので安全ですが、HTTP（非 SSL/TLS）で学内のサーバにアクセスする場合は通信内容が傍受される可能性があり危険です。また、つい他のサービスにアクセスし、そのサービスが暗号化を実装していない、という可能性もあり得ます。
さらに、ホテル等が提供する Wi-Fi と同じ SSID を持たせた Wi-Fi 局を立て、本物とよく似たログインページを用意する等、ID とパスワード等の情報を窃取しようとする試みは巷にあふれています。
利用者がそれとわからずに情報を盗み取られるリスク全般を防ぐため、無料 Wi-Fi の利用はしないようにお願いしています。

3) 情報セキュリティについて、わかりやすい行動指針のようなものがあるとありがたいです。（既にあるのでしたら、保管場所等が知りたいです。）

本学 e-Office Navi の常設情報、情報セキュリティポリシー、手順等に「PC/インターネット利用ガイドライン」を掲載しています。また、体験型セキュリティ予防訓練ツール「セキュアプラクティス」https://spractice.yamanashi.ac.jp/spractice/index.php も公開していますので、是非ご覧ください。

4) もう少し忙しくない時期に実施していただけると良いと思います．夏休み中とか．

時期についてはご提示の夏頃の実施をする方向で見直しの予定です。

5) ・一度答えて保存して提出したはずのものが、何度も「やっていないからやれ」とメールが来たため、もう一度やりました。設問が多く、やり直すのは大変です。どうにかしてください。

・順番に最後まで入力していき、『戻る』等していないはずだが、『複数の操作がされた』というエラーで再入力となった。途中で急ぎのメール対応があり、30 分以上かかったため、タイムアウトの可能性もあるが、もしそうなら事前に示していただきたい。

他にも複数の方に同様の問合せをいただいていますが、回答後の「確認」ボタンを押下後、次に表示される「回答」ボタンを押し忘れているケースがほとんどです。大多数の方が問題なく回答を終えていますので、誠に恐れ入りますが、回答時にご確認いただければ幸いです。
また回答に時間を要する場合は、お手数ですが随時保存をしてくださいますようお願いいたします。期限前でしたら続きの回答や、回答の修正も可能です。

6) 解答者へのわかりやすいフィードバックをお願いいたします。

令和元年度よりフィードバックを実施していますので、ご確認ください。
セキュリティ監査の解説
https://sojo.yamanashi.ac.jp/facilities/inside/security-inspection/

7) 他大学同様に、月に一度程度、訓練メールなどを行った方が良い

以前は実施しておりましたが、慣れが出てきたため、ここ 1 年は訓練ツールの公開等、代替策を実施しています。今後は複数の訓練でバリエーションを設ける等、検討していきたいと思います。

8) （設問「1-2-2 外部記録媒体の利用と管理」等について）の質問事項で申し訳ありません。業務上 USB、外部記録媒体を使用するような業務ではありません。一応「準備中」と回答しましたが使用することはないと思います。

お申し出ありがとうございます。

個人として USB や外部記録媒体を使用する業務がない場合でも、所属部署全体では取り扱うことはないでしょうか。所属部局の状況をお答えいただければと思います。

9) 業務用パソコンというものを与えられておらず、業務用＝個人用となっているため答えづらいところがあった。

質問数を抑えるためもあり汎用的な質問としているため、回答しづらい点がありましたことはお詫びします。業務用＝個人用で同一の機器であれば、業務用と個人用で同じ回答としていただいて結構です。

10) 今年度より、講座の Web サイト責任者および担当者も「情報セキュリティ監査セルフチェック」の「3 部局情報システム運用担当者対象」へ回答することとなりましたが、質問の多くはサーバーまたはネットワーク管理者を対象としており、大学が管理しているサーバー内で Web サイトのみを運営している者には回答できない項目がいくつかあります。

ご自身としては Web コンテンツのみを取り扱い、サーバ管理は他者がしている、ということかと思います。サーバ管理を委託している場合は委託先に、設問にあるような対策を依頼していれば「はい」でお答えください。レンタルサーバの場合は、設問にあるような対策が取られていることを確認してください。本学が契約し、学内に提供しているレンタルサーバについては、全て対策を実施している、でご回答ください。

11) 事務職員対象の質問の回答に、「所属部局は、部局情報システム管理・運用責任者の指導の下、規程・手順に沿った運用を行っているが、当職は使用していないので回答対象外」が必要。

所属部局の状況をお答えいただければと思います。

12) 電子カルテにログインするパスワードの変更（60 日間ごと？）は不要なのでは？パスワード変更後そのパスワードを忘れると、電子カルテにログインできないというデメリットがあります。実際、身の回りにそのような状態になった職員がいました。総務省からパスワードを定期的に変更する必要はないと示されています（https://www.nisc.go.jp/security-site/handbook/index.html）が、どうでしょうか？

（医療情報課　回答）

ご意見のとおり、内閣サイバーセキュリティーセンターや総務省から、パスワードを定期的に変更する必要はない旨が示されております。
他方、厚生労働省が定める「医療情報システムの安全管理に関するガイドライン第 5.2 版」において、パスワードについて以下のとおり要件が定められております。

a. 英数字、記号を混在させた 13 文字以上の推定困難な文字列
b. 英数字、記号を混在させた 8 文字以上の推定困難な文字列を定期的に変更させる（最長でも２ヶ月以内）
c. 二要素以上の認証の場合、英数字、記号を混在させた 8 文字以上の推定困難な文字列。ただし他の認証要素として必要な電子証明書等の使用に PIN 等が設定されている場合には、この限りではない。

現在本院では、「パスワードは８桁以上の英数記号を組み合わせたものとし、パスワードの有効期限は、原則２ヶ月以内とし、利用者が更新すること。」と規定しておりますが、次の電子カルテシステム更新に併せて、二要素認証の導入も含め検討してゆきたいと思います。

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