令和元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

令和元年度、(令和 2 年) 1 月～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、といった例が複数確認されています。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ので、そういった事案の当事者にならないよう、パスワードは本学ガイドラインに沿った十分に複雑なものを使用してください。

■ 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。

学内のメール送受信は暗号化されるため、傍受されても比較的安心ですが、送信先の相手が学外のアドレスへ転送をしていたら、学外への送信時と同じ状態になるため、基本的にメール本文に重要・機密情報を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、ブラインドカーボンコピー（Blind Carbon Copy）の略で、CC と同様、メールを複数の宛先へ送信するときに使用します。BCC に指定したアドレスは、受信した側からは確認ができません。

複数の方へメールを送信する場合、送信者のあなたは全員のメールアドレスを知っているのが当然でも、送信先の方々の間ではお互いのアドレスを知られるのが不適切というケースや、メールの内容が送付先の間でお互いに知られたくないというケース等が考えられます。

送付先を全て BCC に指定し、TO には自分のアドレスを指定することで、宛先の人たちの間でアドレスが共有されてしまうことを避けることができます。多数の宛先にメールをするときはそういったケースへの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(必須)
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 でも解説した通り、メールは平文で伝送されます。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、できるだけ避けましょう。
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「パスワードをかけた圧縮（zip）ファイル」にして「添付ファイル」で送信するようにしてください。
またそのパスワードを相手に伝える場合、ファイルを添付したメール本文にそのパスワードを書いてしまっては、ファイルにパスワードを付けた意味がなくなってしまいます。
最低限、添付ファイルとは別メールで送信する、また可能ならメールとは別の方法（携帯電話、SMS 等）で伝えるようにしましょう。

■ 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
・情報システム課に確認する

・メールを削除する

お詫び：
この設問については、届いたメールの文中に、WEB サイトへのリンクが記入されていたり、ファイルが添付されていたりした場合に、それらが「問題を起こさないことを確認できない場合の対処」を尋ねる主旨でしたが、質問文にその意図が反映されていませんでした。
この点お詫びしますとともに、次年度の質問文はより適切なものに修正させていただきます。

■ 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、そのリンクが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、よく確認してから開くようにしてください。
ネットワークを伝って山梨大学内に外部から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が、メールを使って山梨大学の内部から有害なサイトにアクセスさせたり、不正な実行ファイル（マルウェア）を送り込んだりして、情報を漏洩させようとする攻撃は、皆さん自身が安易にリンクをクリックしたり、添付ファイルをクリックしたりしないようにすることでしか防ぐことができません。
実際、このような攻撃によるマルウェア感染や外部への通信が、複数確認されています。高い意識をもって対応くださるよう、お願いします。

特に最近、佐川急便の不在連絡や、三菱 UFJ 銀行ネットバンキングを騙ったメッセージが届き、正しいものかどうか確認するためクリック（タップ）する方が増えていますが、こういった行為でマルウェアがダウンロードされる可能性があるため、クリック（タップ）しないようにしてください。

これらが正規のメッセージがどうかは、比較的簡単に見分けることができます。

以下、不正なリンクや有害な添付ファイルの見分け方を示しますが、受信したメールについて、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。（またはメール本文に埋め込まれたリンクにマウスポインタをかざすと、そのリンクが実際にはどの URL を指しているのかを見分けることができます。表面上の記載と、実際のリンク先が異なっていることが多いので、よく注意してください。）

その URL のうち、「http(s)://」から次の「/」までの間にある文字列が、送信元が示す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）になっているか確認します。

これらが不正な場合は、ほぼすべて有害なサイトですので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》

禁止：添付ファイルをすぐにクリックしないでください。

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 となっている場合は、ほぼすべて有害なファイルと考えてください（クリックしてはいけません）。

また、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）だった場合でも、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。

ファイルの拡張子は、エクスプローラを開いて「表示」タブを選択し、（右の方にある）「□ファイル拡張子」にチェックを入れることで表示させることができます。

■ 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]

業務で PC 使用中、業務に関係のないホームページ（WEB ページ）にアクセスしないようにしてください。業務で PC を使ってそういったページを閲覧することは適切ではありません。

またそういったページや、業務上の必要があって閲覧したページでも、開かれたバナー広告へアク

セスしたことで、不適切なソフトウェアがインストールされてしまい、追加ソフトウェアの購入を促すメッセージが再三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そうになったりといったケースが見つかっています。バナー広告には原則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、一時世間を騒がせた Winny に代表される、他の PC とのファイル交換を行うための P2P ソフトウェアの使用を禁止しています。これは、著作権を侵害する恐れがあるためなのはもちろんのこと、あなたが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は、学外とのファイル共有ができない閉じたネットワークで使用する等、問題を起こさない環境下で使用してください。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するようお願いします。

■ 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」にウィルス対策ソフトを使用していますか。

期待される回答：
・はい

[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
質問 1-1-12 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：1-1-13]

病院用端末を除く、業務用パソコンを使用していない場合や、インターネット不使用の場合は問題ありません。

一方、使用頻度が低い場合でも使うことがある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。また、Mac の場合でもウィルス対策ソフトは存在しますし、インストールが必要です。業務用の PC であれば、大学が公開しているウィルスバスターをインストールすることが可能ですので、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 30 件以上寄せられましたが、総合情報戦略機構の WEB ページ：https://sojo.yamanashi.ac.jp/services/software/virusbuster/
に手順が公開されていますので、こちらをご覧ください。

また、業務に使用しているパソコンにウィルス対策ソフトが入っているかどうかは、ご自身でも認識しておいてください。上長に聞く、PC 管理部署に聞く等して確認しておくことを推奨します。

■ 1-1-14 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」にウィルス対策ソフトを使用していますか。

期待される回答：

・はい

[解説：1-1-14]

本学では、自宅の PC を業務に使用することを制限していません。そのため自宅の PC を仕事に使用したり、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 メモリを使用した場合、その USB メモリを介してウィルスに感染することを避ける必要があります。

このような理由から、自宅にお持ちの 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。

大学の業務を自宅の PC では一切行わない、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、たとえ自宅 PC であっても十分な対策を怠って、山梨大学に影響するセキュリティ上の問題、事故を発生させた場合は、就業規則に則った罰則が適用されることがある点にご注意ください。

■ 1-1-15 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
質問 1-1-14 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：1-1-15]

自宅にパソコン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。

その他の場合も含め本学では、[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。

■ 1-1-16 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：1-1-16]

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。

■ 1-1-17 不正ソフトウェア対策機能の更新（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：1-1-16、1-1-17]

せっかく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あっても、それらのソフトウェアが最新でなければ、新しいタイプのウィルス、不正ソフト（マルウェア）が出現するとそれに対処できません。

このため、PC 起動後はできればすぐに Internet 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。Internet 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。

■ 1-1-18 不正ソフトウェア対策機能の更新（アップデート）を実施しない理由
質問 1-1-17 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：1-1-18]

利用する業務用パソコンや自宅のパソコンが一切ない場合は問題ありません。

一方、利用する業務用パソコンや自宅のパソコンをインターネットに接続しない場合でも、USB メモリやポータブル HDD 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。

ウィルス対策ソフトが入っていない PC は無防備な状態です。

USB メモリや HDD 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の状態になっている 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、インターネット無接続の PC にウィルスを感染させたという例がありました。

■ 1-1-19 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」

■ 1-1-20 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：1-1-19、1-1-20]

Office 365 や CNS、いくつかの山梨大学が提供するサービスについては、Internet に接続できれば外出先から利用することが可能です。

このとき、ID やパスワードが伝送されますが、フリーWi-Fi を使用すると、それらの情報が簡単に傍受され、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。

■ 1-1-21 SNS/ブログ等への、秘密情報公開の禁止(必須)

あなたは、Twitter 等の SNS やブログに業務上知りえた秘密を掲載してはいけないことを知っていますか。

■ 1-1-22 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。

期待される回答：

その掲載によって誰にどのような影響が及ぶかわからないので、学内で得た情報は絶対に掲載しない

[解説：1-1-21、1-1-22]

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じてはいませんが、あなたが「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、原則公開はしないようにしてください。

但し、大学や学内組織の広報のために、関係者の了解のもとに情報を公開する場合は除きます。

■ 1-1-23 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）業務用メールアカウントのチェックなど、業務に個人のモバイル端末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。

■ 1-1-24 私用モバイル端末の OS 更新

質問 1-1-23 のケースでモバイル端末を利用している場合、「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：1-1-23、1-1-24]

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。

■ 1-1-25 私用モバイル端末の OS 更新を実施しない理由

質問 1-1-24 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：1-1-25]

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、OS 毎にネット検索等で確認し、各自行うようにしてください。

OS にも完全なものはなく、特にセキュリティ上の脆弱性が発見されると、対策を講じた更新版が公開されます。更新版リリースの通知を受けたら、速やかに適用し、セキュリティ脆弱性を突いた攻撃を防げる状態にしておいてください。

■ 1-1-26 私用モバイル端末での不正ソフトウェア対策

質問 1-1-23 のケースでモバイル端末を利用している場合、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：1-1-26]

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ことと同じです。

■ 1-1-27 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 1-1-26 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： 1-1-27]

所持していない場合は問題ありません。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、適切なものを選ぶようにしてください。

iPhone なので不要という認識を持たれている方については、Apple Store からインストールするアプリに関しては、不正なアプリをインストールするリスクは低減できるものの、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、マルウェアに感染したりするリスクは抑えられません。

このため iPhone であってもウィルス対策ソフトをインストールするようにしてください。

なおウィルス対策ソフトのインストール方法がわからないという回答が 50 件程度見られましたが、製品を購入すれば手順も提供されます。その手順に従うようにしてください。

■ 1-1-28 私用モバイル端末での不正ソフトウェア対策機能、最新化（更新）

質問 1-1-26 で「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：1-1-28]

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ことと同じです。

■ 1-1-29 私用モバイル端末での不正ソフトウェア対策について、最新化していない理由

質問 1-1-28 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：1-1-29]

モバイル端末のセキュリティ対策アプリについて、自動的に更新を確認する、自動的に更新する、といった機能を持っていますので、それらを適宜有効にし、更新がなされるようにしてください。面倒だから、特に理由はない、といった理由で更新を行わず、それが原因で重大な事故等につながった場合、服務規程に沿って処罰されることがあり得る点を認識いただければと思います。

■ 1-1-30 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

質問 1-1-23 のケースでモバイル端末を利用している場合、「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：1-1-30]

本学では『情報機器取扱ガイドライン』5 条 5.3 項、「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」設定とすることで、これを満たすことができます。

しかしながら、正規のソフトウェアであっても、供給元不明アプリのインストールを許可する設定に変更しないとインストールができない場合があります。その場合は、一時的に許可する設定にして、インストールが終わったら不許可に戻す、といった対応をお願いします。

一方、iPhone や iPad 等では、アプリは一般に Apple Store からインストールすることや、Apple 社による審査をパスしなければ、供給元はアプリを Apple Store に公開できないこと等から、アプリを Apple Store からしかインストールしないようにしてください（この場合は、規定の条件を満たしていると判断いただいて構いません）。

但し、iPhone/iPad といえども、Apple Store を経由せずに提供される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った場合は責任を問われる可能性がありますので、この点を十分に認識の上、本当に信頼してよいアプリかどうかを慎重に判断してください。

■ 1-1-31 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 1-1-30 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：1-1-31]
上記[解説：1-1-30]にも記載している通りです。

■ 1-1-32 「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：1-1-32]
本学では、取り扱う様々な情報について格付けを行い、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、実運用に載せるようお願いします。

■ 1-1-33 「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」については今後改良していく予定です。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：1-1-33]
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、具体化に向けて検討を進めたいと考えています。

■ 1-1-34 「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：1-1-34]
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。

■ 1-1-35 「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」については今後改良していく予定です。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。検討を進めたいと考えています。

■ 1-1-36 重要データのバックアップ(必須)
あなたはそのデータ（情報、資料等）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：1-1-36]
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、適切な方法で取得をしてください。
またバックアップはなるべく、情報の格納先である PC とは別の媒体に取得するようにお願いします。同一 PC 内の別の場所に取っていても、PC が故障してしまうと回収ができなくなるためです。

■ 1-1-37 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：1-1-37]
▽ご意見・ご要望
1) 個人情報と機密情報と、用語の使途が食い違っている。

用語の使い方が不適切な設問については、今後適切なものに改めます。

2) 機密情報はメール本文に書かないが、個人情報は書いている。

ご自身の個人情報を記載する場合は、ご自身の責任の下、ご判断いただければと思いますが、他者の個人情報はメールの本文に記載しないようにしてください。

3) 「いいえ」と答えた場合には、回答しない項目は回答できなくする（見えなくする）等の機能があると、時間の節約になる。

以後改善していきたいと思います。

4) SNS への情報公開について、回答の選択肢が少なすぎる。

広報目的で関係者全員の合意が取れている場合は公開しても問題はありません。選択肢として不

足の感は否めませんので、この点を含む選択肢を加えるようにしたいと思います。

5) 質問の中に、回答を誘導するような質問があって回答する気が削がれる。

該当の質問は、回答の選択肢から正しい行動内容を理解していただくことを目的としています。いわゆる採点を目的としたテストではないため、ご了承ください。

6) 1-1-8「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。」という質問について、回答の選択肢が極端すぎる。

問題文が不適切だった点、お詫びいたします。この問いは、リンクや添付ファイルが「問題を起こさないことを確認できない場合の対処」を尋ねる主旨でした。次回修正の予定です。

7) 1-1-14「自宅のパソコン」にウィルス対策ソフトを使用していますか。」という質問で、自宅のパソコンがない場合に回答できない。

その場合はいいえで回答いただき、次の記述欄に自宅に所持していない旨を回答いただくことが可能ではあるのですが、今後選択肢を増やす方向で検討させていただきます。

その他適切な選択肢が設けられていない設問がある点については、ご指摘いただいた点を勘案し、次回検討させていただきます。

8) Windows ユーザーや Android ユーザー向けと見えるような設問が多くありますので、iOS、OSX ユーザーが回答しにくいところが多数あります。

設問内容について、再度吟味させていただきます。

9) 個人情報等をメールで送る場合の理由を尋ねたほうがよい。

設問の追加要否を検討させていただきます。

10) 簡単な方法がよい

具体案をお寄せいただければ幸いです。

11) 専門用語が多くて質問の意味がよくわからない。

恐れ入りますが、回答の際、具体的にどこがわからないのか情報システム課へお問合せください。

▽フィードバック希望

12) フィードバックをしてほしい。

前年度は実施できず申し訳ございませんでした。今回は、このような方法で実施させていただいております。

13) パスワード後送信や，パスワードの定期的な変更にはセキュリティ上の意味がないという意見がありますが，どのように思われますか。説得力のある議論のように読めましたが，間違っていますか。
https://qiita.com/spaces/items/39a822050b6e22d35123?fbclid=IwAR1hOmPFDT-eErZY35KPOUuxZshGZH1j-3HqLpHh5_wWhGwmBURI0LO86-o

ご意見ごもっともだと認識しております。このためパスワードの定期的な変更はお願いしておりません。またパスワードの後送信についても、不完全な対策であり、できるだけ別の手段で相手に伝えていただきたいと考えております。後者については[解説：1-1-3]もご覧ください。

14) もしもの時に必須なウィルス対策やバックアップ等の対策を随時新しいものをわかりやすく提示してほしい。

設問：1-1-36 と回答（選択肢）、解説：1-1-36 をご覧ください。

15) 質問が多すぎる。このアンケートの結果がどのように反映されたのか報告するべき。

質問については、できるだけ削り、最低限ご留意いただきたい事項に絞っています。
また本監査の結果は、総合情報戦略機構にて確認し、今後の施策や方針の検討材料とさせていただいております。

16) 先日生じたメールアドレス漏洩について「何が原因で生じたのか」を公開することも情報セキュリティへの関心を高めることに繋がると思いますので、詳細に解析した結果を掲示板等で公開してください。

令和元年 12 月に掲示板にてお知らせしました、メールアドレス＆パスワード漏洩チェックのお願いに対し、ご協力をいただきありがとうございました。

パスワード漏洩の原因については、この時利用したサイトでは、一般に知られている有名ソフトウェア/サービス会社で過去に起こった大規模情報漏洩事故が原因といった程度のことしかわからず、それ以外のケースでは原因を追跡できません。
自身ではどうにもならない原因については不可抗力です。
一方、自身の不注意でパスワードが漏洩したケースについては、本監査やこのフィードバックでポイントを提示させていただいております。
なお今後、アカウント情報の流出事故等の情報が入った場合は、適宜アナウンスをさせていただく予定です。

17) 病院ネットワークをクラッキングされ、病院業務端末にランサムウェアをインストールされ、患者データを人質に多額の身代金を要求されてしまう事が、5 年くらい前から海外で大問題になっている。本院にて病院端末で誰でもネット接続できる事は問題無いのか知りたい。また、今月でセキュリティアップデートが無くなる Windows7 を病院端末に使用して問題が無いのか、そもそも病院端末はセキュリティアップデートしているのか、知りたい。

ご意見ありがとうございます。病院端末については医療情報課の所管となります。このご意見について、医療情報課より回答がございましたので、転載します。

〇病院端末でネット接続できることについて

病院端末からのインターネット接続は、仮想サーバを使用して間接的に参照する環境となっております。
端末上でデータを直接送受信することはできないため、セキュリティは確保しております。

〇Windows7 について

病院端末は病院の業務を行うための機器であり、これらは通常のパソコンとは用途も利用環境も異なるため、常に最新アップデートするといった運用はできません。そのような運用を行うためには、アップデートの都度、各業務システムすべてについて動作検証を行い、場合によってはプログラム改修も行わなければならず、莫大な費用と時間がかかるためです。
また、病院端末を接続しているネットワークは閉鎖環境で使用しており、外部ネットワークからのセキュリティを確保しております。

---

18) 本当にセキュアな手段についての情報をアップデートし，伝達していただきたい。

できるだけ最新のセキュリティに関する情報と対策を「セキュリティニュース」として提供しています。総合情報戦略機構の WEB サイト、「セキュリティニュース」のページ：
https://sojo.yamanashi.ac.jp/secnews/
をご覧ください。

▽システム導入希望

19) バックアップを取ろうと思うとクラッシュします。意識しないでバックアップされる仕組みが必要かもしれません。

恐れ入りますが、対象機器の所有者、管理部署により相談先が異なってきます。まずは対象機器の所有部署、管理部署へご相談ください。

▽ルール策定希望

20) ファイル管理が個人ごとに無秩序な状態を何とかしてほしい。

ファイルに関しては、「第 7 条 2 号-34_情報格付け及び取扱制限基準」にて基準を定めており、これに沿ってファイル内の情報を格付けし、管理をしていただくようお願いしています。
ただ部署により格付けの方法や管理指針にも細かな違いがあると思われます。恐れ入りますが、まず所属部署内で管理をどのようにしていくかご相談・ご検討をお願いできますでしょうか。

▽その他

21) まだ入って間もないので、今までの様子やこれからについて分からない事が多いので、このようなパソコンでの回答や伝達方法については勉強不足な為、これから少しずつ学んでいきたいと考えております。

前向きなご意見ありがとうございます。不明な点がありましたら情報システム課へご相談いただければと思います。

22) 別の媒体（外付ハードディスクや DVD 等）にバックアップしている

バックアップについて、対策を実施いただきありがとうございます。

23) 今回のように、未実施の人に、アラートのメールを送ることは、よいことと思う。

ありがとうございます。次回も継続の予定です。

24) 情報セキュリティポリシーの内容をひととおり確認しようとしましたが、フリーズしてしまうことがあります。例　第６条２号サイバーセキュリティ対策等基本計画、第２０条情報セキュリティ組織体制に関する内規

ご使用のブラウザを変えてみる、ファイルをダウンロードしてから、Adobe Acrobat Reader や、Just PDF 等で開いてご覧ください。

25) 不要なアンケート調査は実施しないでいただきたい。業務時間と生産性の損失につながっている

恐れ入りますが、本セルフチェックは規定された「監査」の一環で実施されており、実施の義務がございます。期限まで１か月という長い実施期間を設けておりますことと、一時保存が可能であることとから、是非ご理解、ご協力を賜れればと存じます。

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、多数の方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