令和２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２年度（令和２年 12 月～令和３年２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。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、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従って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。

学内のアドレス間でのメール送受信は暗号化されるため安全ですが、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、基本的にメール本文に重要・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、ブラインドカーボンコピー（Blind Carbon Copy）の略で、BCC に指定したアドレスは、受信した人からは確認ができません。
複数の宛先へメールを送信する場合、送信者のあなたは誰のアドレスにどんな内容を送っても支障はなくても、メールの受け手の間ではアドレスやメールの内容が、他者に知られてしまうのは不適切といったケースが考えられます。
送付先を全て BCC に指定し、TO には自分のアドレスのみを指定することで、受け手の間でアドレス（やメールの内容）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（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「パスワードをかけたファイル」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。メールとは別の方法（携帯電話、SMS 等）で伝える、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。一方、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、皆さん自身がメールや WEB サイトのリンクを安易にクリックしたり、添付ファイルをすぐ開封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してください。

特に最近、宅配業者の不在連絡や、インターネットバンキングを騙ったメッセージが届き、興味本位でクリック（タップ）する方が増えていますが、こういった行為によってマルウェアに感染する可能性があるため、決してクリック（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「/」の直前にある文字列が、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）の場合でも、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 PC を使用中、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 PC で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。

また業務に関係のあるなしによらず、閲覧したページで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、追加サービス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 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ことはもちろん、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、使用頻度が低くても、PC を使う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 管理担当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：1-1-15]

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。

■ 1-1-16 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
質問 1-1-15 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：1-1-16]

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。

■ 1-1-17 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：1-1-17]

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 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：1-1-17、1-1-18]

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。

■ 1-1-19 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 1-1-18 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、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、パスワードを窃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]

Office 365 や CNS 等、いくつかの山梨大学が提供するサービスについては、インターネット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 とパスワードを入力しますが、フリーWi-Fi を使用すると、それらの情報が傍受され、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 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。

■ 1-1-23 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。

■ 1-1-24,25 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）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。

■ 1-1-26 私用モバイル端末の OS 更新
質問 1-1-24 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：1-1-24、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ことと同じです。

■ 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、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
質問 1-1-24 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：1-1-28]

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数十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。

■ 1-1-30 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ご認識いただければと思います。

■ 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
質問 1-1-24 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：1-1-32]

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。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]にも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、実運用に載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、具体化に向けて引き続き検討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：1-1-37]
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。検討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：1-1-38]
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。

■ 1-1-39 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) 大学 HP などに掲載されている各種ファイルについて、プロパティに作成者のアカウント名などが残っていることが多いため、それらに対する注意喚起をした方が良いと思います。

ご助言ありがとうございます。適宜、学内へのアナウンスを実行していきたいと思います。

2) 必要なファイルが自分のパソコンにのみ入っているので色々な人が自分のパソコンに触れるのが嫌です。中には個人情報のファイルなどもあり、見られたくないのですが、どうしても仕事上で皆が使うファイルなので嫌々でも我慢しています。これはセキュリティ問題にはならないでしょうか。このパソコンを使えばメールも見れてしまうので、共通のパソコンのようで困ります。

組織内の全員が同じアカウントでログインできる共有 PC で、一部の人にのみ共有されるべきファイルが管理されている、ということでしょうか。その場合は本学の情報セキュリティポリシーに違反していますので是正が必要です。個別に対応させていただきますのでご連絡ください。

3) 大学病院業務カルテ用端末の OS アップデートを常にして欲しい。出来ないなら、学内ページ以外に繋がらない様にするべきと考えます。御存知の通り、数年前に、病院端末を暗号化し身代金要求する事件がありました。バックアップも含めて、当院も、少なくとも病院端末は、セキュリティ対策した方が良いです。

昨年も同様のご意見が寄せられました。病院端末については医療情報課の管轄となります。医療情報課からの回答を、再掲させていただきます。

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。

---

4) ファイル共有につきまして、学内で使用されている情報を見たり使用したりすることがそれにあたるのであれば利用していますが、自分でインストールすることはないのでどのように回答してよいのかわかりません。ファイル共有ができている？もうすでにインストールされている？パソコンについてあまり理解していないので検討違いな答えをしていたらすみません。

ファイル共有については、それ専用のソフトウェア（アプリ）をインストールして使用することを指しています。本学の「大学運営 DB」「事務ファイルサーバ（ネットワークドライブ）」「BISON」等は該当しませんので、後者のみ使用の場合は「ファイル共有ソフトは使用していない」と回答いただければと思います。

5) パスワード変更の方法について記載、もしくはリンクを貼っておいていただきたい。確認すべき

書類についてのリンクをこの後の画面にはっておいていただきたい。いずれも確認がすぐにできなかったり、このアンケートに答えながらの回答が困難なため。

ご意見ありがとうございます。今後の監査実施に向けて、改良の参考にさせていただきます。

6) 専門的な内容が分かりにくいが、大学の情報を扱う上では理解しないといけないと感じているが、難しい内容です。もう少し簡単にならないかと思います

具体的に、どの設問が難しいのか、情報システム課へご連絡いただければ幸いです。

7) パスワードのガイドラインは「指針」であると理解している。則っていない場合に「変更しなければ先に進めない」と「強制」するのは、調査の域を超えており、いかがなものかと思う。

パスワードガイドラインは、確かにガイドラインではあります。一方実際問題として、このガイドラインを充たさないパスワードを設定していたことにより、本学のサービスが悪用され、学外の機関へ迷惑をかけるといった事案が未だに続いています。
総合情報戦略機構としては、このような本学の評価を下げたり、学外へ迷惑をかけるような自体の発生を早期に根絶したく、今回のような方法をとらせていただいています。
ご理解いただければ幸いです。

8) 可能な範囲でもう少しコンパクトにして頂けると助かります。
9) 質問が多すぎます。せいぜい 10 個まで

質問については、できるだけ削り、本学のサービス利用者であれば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、総合情報戦略会議にて確認し、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。

10) 再確認ができて、良かった。

前向きなご感想、ありがとうございます。引き続き、ルールを守ってサービスの利用をお願いいたします。

11) １～２週間前に回答した覚えがあるのですが未回答になっていました。
12) 既に回答しているつもりでした、すみません。
13) 一度回答したのに未回答であるとして再度回答依頼が来た

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多数ありました。
誠に恐れ入りますが、回答時はこの点を再度ご確認いただければ幸いです。

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