令和６年度 情報セキュリティ監査セルフチェックシート 解説資料

令和６年度（令和６年 11 月１日～令和７年１月８日）に実施させていただいた、表題のセルフチェックシートについて、全教職員を対象とした設問項目につき、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・ご認識いただけますと幸いです。緑枠で各設問と選択肢を記し、続けて枠外に解説を記載しています。

1-1　パスワードガイドラインの遵守

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、使用する文字列等に関するルールを設けています。
あなたのパスワードは、下記のルールを満たしていますか。

(1) 8 文字以上の長さを持つ。
(2) 以下の①～③から各 1 文字以上を含む。
　① 英字(a～z、A～Z)
　② 数字(0～9)
　③ 記号(* ? ~ ^ [ ] { } / @ ! # % _ + - , . =)
(3) 以下の文字列は容易に推察できる為にパスワードとして設定してはならない。
　① 利用者のアカウント情報から容易に推測できる文字列(氏名、ユーザ ID 等)
　② 上記を並べ替えたもの、上記に数字や記号を追加したもの
　③ 辞書の見出し語(単語として意味を持つ文字)
　④ 一般的に用いられる氏名等の固有名詞
　※「国立大学法人山梨大学情報システム利用者パスワードガイドライン」より要約
　https://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

○はい
○いいえ

[解説]　正答：「はい」

単純・容易に推測可能・他サービス間で同じ物を使い回しているパスワード等の利用は、ID を不正に第三者に利用される不正アクセス被害を受けるリスクの増大に繋がります。ご自身や大学の信用の失墜や他者の迷惑になるだけでなく、情報漏洩にも繋がり得るため、パスワードは下記の本学ガイドラインに従い十分に複雑な物にしてください。

※国立大学法人山梨大学情報システム利用者パスワードガイドライン
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
(https://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)

1-2　パスワードの変更 **　条件：1-1 で「いいえ」を選択**
1-1 で「いいえ」を選択した方は、下記 URL よりパスワードを変更してください。 https://obtt.yamanashi.ac.jp/
○パスワードを変更しました

[解説]
　同上

1-3　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、どの種類の宛先の利用が適していますか。
○TO ○CC ○BCC

[解説]　正答：BCC
　BCC とは Blind Carbon Copy の略で、BCC に指定したアドレスは、当該メールの受信者には見えません。メールアドレスも立派な個人情報であり、複数の宛先にメールを送付する場合、送信者にとって支障はなくても、メールの受信者間でメールアドレスがお互いに知られる事は不適切なケースが考えられます。
　複数の宛先アドレスを全て BCC に指定することで、受信者間で意図せずアドレスが知られてしまう事を避けることが出来ます。

※利用すべき例…当該情報を受信している事を他者に知られる事が不利益になる通知メール(督促等)
　　相互に繋がりのない複数の学外の宛先アドレスに対するメール

1-4　E メールでの機密情報等の送信

機密情報等を 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。

※[用語] 機密情報等
　第三者に知られる事で組織運営上問題を引き起こし得る、外部に流出させるべきでない情報。
　例：学生や教職員の個人情報、関係者外秘の教育研究データ

○はい
○いいえ

1-5　E メールでの機密情報等の送信を行う際の対応
**　条件：1-4 で「はい」を選択**

1-4 で「はい」を選択した方は、E メールで機密情報等を送信する際、メール自体の暗号化や、添付ファイルの暗号化(パスワードの付与)を行っていますか。

※[用語] 暗号化
　データを意図しない第三者から解読・改ざんできない状態に変換する処理。
　・メール自体の暗号化…送受信するメール自体を暗号化する事を指す。
　　主に Outlook 等のメールソフトでオプションとして提供される。
　　例えば Outlook では「新規メール ＞ オプション ＞ 南京錠のマーク ＞ 暗号化」で利用できる。
　・添付ファイルの暗号化…メールに添付するファイルを暗号化する事を指す。
　　パスワード付き ZIP ファイル(7zip や Lhaplus 等の利用)やパスワード付き Excel ファイル等。

○はい
○いいえ

[解説]　正答：「1-4 いいえ」 もしくは 「1-4 はい→1-5 はい」

　十分な対策を講じる事が出来ない場合、機密情報等を E メールで送付することは避けるべきです。理由として、E メールは現実の郵便と同様に、送信から受信までの流れの中で、複数のメール転送サーバ(郵便物を中継する郵便局に相当)を中継して送受信され得るため、通信経路上で中身を盗聴されるリスクが存在するほか、宛先を誤って送信してしまう人為的なミスのリスク等が挙げられます。

　機密情報等を E メールで送付する必要がある場合は、1-5 の設問のとおり、「メール自体の暗号化」もしくは「添付ファイルの暗号化」を行ってください。

1-6　添付ファイルのパスワードの伝達方法
**　条件：1-5 で「はい」を選択**

パスワード付きの添付ファイルを E メールで送信する際、そのパスワードをどのように伝えていますか。

○添付ファイルを送るメールの本文に記載
○添付ファイルを送るメールとは別のメールに記載
○メールとは別の方法(電話・SMS・FAX・事前共有等)

[解説]　正答：「メールとは別の方法(電話・SMS・FAX・事前共有等)」

　パスワード付きの添付ファイルを E メールで送信する際は、パスワードを必ず「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 E 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添付ファイルを復号して中身を見ることが出来てしまい、パスワードを掛けた意味が全くありません。なお、ファイルを添付した E 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の対策にはならず、推奨されません(両方のメールが同一の経路と手順を辿る可能性が高いため)。

　複雑なパスワードを郵送・電話等で事前に関係者間で共有し、パスワードのやりとりを一切 E メールで行わない等の方法が推奨されます。

1-7　メールの安全性の確認

届いたメールに添付ファイルや URL(リンク)の記載があった場合、どのように扱いますか。

※[用語] 拡張子
　ファイルの種類を表す文字列。ファイル名に続けて「.(ピリオド)」以降に記載される。
　ファイルの拡張子はパソコン上の設定で常に表示させる事が可能である。
　(例：.xlsx ＝ エクセルファイル/.txt ＝ テキストファイル)

○送り主・ファイル拡張子・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)
○すぐに開く
○その他([記述欄])

[解説]　正答：「送り主・ファイル拡張子・URL の正当性を確認してから開く」

　受信したメール中に URL(リンク)や添付ファイルがあった場合、下記赤枠の手順を参考に、安全性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を図るサイバー攻撃は、各種防御システム(例：ファイアウォール)により防がれていますが、メールを使いマルウェアを実行させる攻撃や、有害なサイトにアクセスを誘導して情報を盗み取る攻撃等は、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・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等を装ったメッセージや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が多く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、決してクリックしないようにしてください。

URL(リンク)や添付ファイルの安全性を見分ける手順を下記赤枠の通り示しますが、もしご自身で判断が難しいメールを受信した場合は、情報システム課までご相談ください。

URL(リンク)の安全性の見分け方

メール本文に記載されたリンクにマウスカーソルをかざすことで、実際にジャンプする先の URL が表示されます。表示された URL の「http(s)://」から 1 番最初の「/」に挟まれた文字列を確認し、この文字列が企業や組織の正しい文字列(ドメイン)かどうかを、公式サイトの検索等を行い確認します。
(例：文部科学省 ～.mext.go.jp、佐川急便 ～.sagawa-exp.co.jp)文字列が不正な場合は、殆どの場合アクセスしてはいけない不正なサイトです。

例：情報システム課員を名乗り「この URL に ID と PW を入力してください」という旨のメール
メール中の URL ＝ 「https:// passwordchange.yamonashi.ac.jp /」
Google 検索で調べた山梨大学の公式サイトの URL ＝ 「https:// www.yamanashi.ac.jp /」
→yamonashi.ac.jp と yamanashi.ac.jp が一致していないため「不正なサイト」と判断

添付ファイルの安全性の見分け方(拡張子の表示方法)

添付ファイルを一度保存し、エクスプローラからそのファイルの拡張子や種類を確認します。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、殆どの場合クリックしてはいけない不正なファイルです。

安全性が自明でない場合、普段利用する Microsoft Office のファイル(xls/xlsx・doc/dox 等)の場合でも、ApexOne 等のマルウェア対策ソフトを使いスキャンを行ってください。

ファイルの拡張子は下記の手順で常時表示させることができます。

[Windows の場合]
エクスプローラ ＞「表示」タブ ＞「□ファイル拡張子」にチェック
[MAC の場合]
Finder ＞「設定」＞「詳細」＞「□全てのファイル名拡張子を表示」にチェック

1-8　業務中の Web サイト閲覧
業務中に、業務用パソコンで業務に関係のない Web サイトにアクセスしたり、好奇心や興味本位でリンク・広告(バナー)・ボタン等をクリックすることがありますか。 ※[用語] 業務用パソコン 大学の予算等で購入され、本学の業務に使用されるパソコンをいう。 (例：情報システム課から配布される事務用パソコンや各部局等の予算で購入したパソコン)
○興味のあるものはクリックすることがある(例：車・家電・芸能ニュース等) ○業務上無関係な情報はクリックしない

[解説]　正答：「業務上無関係な情報はクリックしない」

業務用パソコンで、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。また、業務との関係の有無に関わらず、Web サイト上にある広告(バナー)をクリックした事で、外部からマルウェアが自動でダウンロードされてしまうケースや、一見マルウェアが感染したかのように見せる画面を表示すると共に「サポート窓口」と称した電話番号を表示し、修復のための金銭を要求されるケース等が確認されています。広告(バナー)にはアクセスしないようにご注意ください。

1-9　ファイル共有(P2P)ソフトウェアの仕様
業務用パソコンや個人所有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。 ※[用語] ファイル共有ソフト インターネットを経由してファイルを送受信・共有する為のソフトウェア (例：Winny/Share/μtorrent/BitTorrent)
○利用している ○利用していない

[解説]　正答：「利用していない」

本学では、他のパソコンと直接ファイルを送受信できるファイル共有(P2P)ソフトの利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非常に高いためです。

教育研究目的の場合、研究室内の閉じたネットワークで利用する等、同ソフトウェアの利用に係る問題が起きない環境に限り、利用を許可しています。安全を確保できない場合はパソコン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、保有する機密情報等が外部へと漏洩する事件等があった場合、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いたします。

1-10　業務用パソコンでのマルウェア対策機能
業務用パソコンでマルウェア対策機能を利用していますか。 ここでいうマルウェア対策機能とは、マルウェア対策ソフトウェア(例：ApexOne)の導入や、OS 標準のマルウェア対策機能(例：Windows Defender)を指します。 ※[用語] マルウェア 　悪意ある動作を行うソフトウェア(例：ウイルス)。
○している(情報システム課配布の事務用パソコンはこちら) ○していない ○確認方法がわからない

1-11　業務用パソコンでのマルウェア対策機能-未対策の理由 **　条件：1-10 で「していない」を選択**
1-10 で「していない」を選択した方は、その理由をお答えください。
※記述欄

[解説]　正答：「1-10 している(情報システム課配布の事務用パソコンはこちら)」

本学では、学内で利用するパソコンについて、マルウェア対策ソフトウェアの使用を規程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、マルウェア対策ソフトウェアのインストールと、マルウェア対策機能の有効化をお願いします。

業務に用いるパソコンであれば、大学が公開する ApexOne の利用が可能ですので、ご利用ください。インストール手順については、総合情報戦略機構の Web サイト(下記 URL)をご覧ください。

https://sojo.yamanashi.ac.jp/services/software/virusbuster/

なお、業務でパソコンを利用していない場合や、インターネット不使用(病院用端末等)の場合は、マルウェア対策ソフトウェアを使用していなくても問題ありません。

1-12　個人所有パソコンの業務利用有無
個人所有パソコンを業務で利用していますか。 (例：テレワーク･業務用メールの確認･大学に持ち込み業務で利用)
○はい ○いいえ/持っていない

1-13　個人所有パソコンでのマルウェア対策機能 条件：1-12 で「はい」を選択
個人所有パソコンでマルウェア対策機能を利用していますか。 ここでいうマルウェア対策機能とは、マルウェア対策ソフトウェア(例：ApexOne)の導入や、OS 標準のマルウェア対策機能(例：Windows Defender)を指します。
○している ○していない ○確認方法がわからない

1-14　個人所有パソコンでのマルウェア対策機能-未対策の理由 条件：1-13 で「していない」を選択
1-13 で「していない」を選択した方は、その理由をお答えください。
※記述欄

[解説]　正答：「1-12 はい→1-13 している」 もしくは 「1-12 いいえ/持っていない」

本学では、個人所有パソコンの業務利用を制限していませんが、学内で利用するパソコン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。

大学の業務を個人所有パソコンで一切しない場合はこの限りではありませんが、個人所有パソコンでの十分な対策を怠り、本学に影響するセキュリティ上の自己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ります。

1-15　個人所有モバイル端末の業務利用有無

個人所有モバイル端末(例：スマホ･タブレット)を業務で利用していますか。
(例：業務用メールの確認･Teams の確認･大学に持ち込み業務で利用)

○はい
○いいえ/持っていない

1-16　個人所有モバイル端末でのマルウェア対策機能
**　条件：1-15 で「はい」を選択**

個人所有モバイル端末でマルウェア対策機能を利用していますか。
ここでいうマルウェア対策機能とは、マルウェア対策アプリ(例：Enterprise Mobile Security)の導入や、OS 標準のマルウェア対策機能を指します。
なお、iPhone や iPad 等の iOS/iPadOS を搭載した端末は、標準状態で上記機能を有するものとします。

○している(iPhone や iPad はこちら)
○していない
○確認方法がわからない

1-17　個人所有モバイル端末でのマルウェア対策機能-未対策の理由
**　条件：1-16 で「していない」を選択**

1-15 で「していない」を選択した方は、その理由をお答えください。

※記述欄

[解説]　正答：「1-15 はい→1-16 している」 もしくは 「1-15 いいえ/持っていない」

個人所有モバイル端末を業務で利用する場合、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」)。マルウェア対策アプリについては、端末を購入した販売店やインターネット検索等により、適切な物を選び利用するようにしてください。

1-18　OS やマルウェア対策機能の更新
業務用パソコン･個人所有パソコン･個人所有モバイル端末で、OS の更新プログラム(例：Windows Update･iOS のアップデート)やマルウェア対策ソフトウェアを常に最新の状態に保つために更新していますか(自動更新の設定を含む)。
○している ○していない ○確認方法がわからない

[解説]　正答：「している」

パソコンやモバイル端末起動後はインターネットに接続し、OS の更新プログラムの適用や、マルウェア対策ソフトウェアの更新を行ってから利用するようにするか、自動更新を有効にして利用してください。

OS のマルウェア対策機能やマルウェア対策ソフトウェアを有効化･導入していても、最新の状態でなければ新たに発見されたマルウェアに対処することが出来ず感染してしまいます。

本学では「情報機器取扱ガイドライン」で、利用端末の OS やアプリ等を定期的に最新の状態に更新することや、マルウェア対策ソフトウェアのパターンファイルを最新の状態に保っておく事を義務付けています。

1-19　OS やマルウェア対策機能の更新-未実施の理由 条件：1-18 で「していない」を選択
1-18 で「していない」を選択した方は、その理由をお答えください。
※記述欄

[解説]

利用している業務用パソコンや、業務で用いる個人所有パソコン･個人所有モバイル端末がない場合は問題ありません。更新の方法は、ご利用の端末に応じてインターネット検索等で確認し、各自行ってください。

OS 等にセキュリティ上の脆弱な部分が発見されると、当該部分を修正する更新プログラム等が公開されるため、更新プログラムの通知を端末で受けたら、速やかに適用してください。

また、「インターネットに接続しない」場合でも、USB メモリ等の外部記録媒体を利用する事が有れば、ドレらの媒体を経由してマルウェアに感染する可能性が有るため、最新版のマルウェア対策ソフトウェアが導入された端末を用いて当該外部記録媒体のスキャンを行い、安全を確認した上で、インターネットに接続しない端末へ接続するようにしてください。この手順を怠った事で、インターネットに接続しない端末にマルウェアが感染した事例が実際に発生しています(例：Stuxnet)。

1-20　学外での無線ネットワークの利用

学外から本学のシステムにアクセスする際に、利用する事がある無線ネットワークを全てお答えください。

□学外からは利用しない
□eduroam（大学で提供）
□フリーWi-Fi（飲食店・ホテル・商業施設等で提供）
□家庭のネットワーク回線（個人で用意）
□モバイルルータ・携帯電話回線（個人で用意）

1-21　フリーWi-Fi やホテルが提供する Wi-Fi の危険性

フリーWi-Fi やホテルが提供する Wi-Fi は、通信の内容が暗号化されていない事がある等、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が禁止されていることを知っていますか。
(例：Web サイトで入力した ID やパスワードが窃取される)

○はい
○いいえ

[解説]　正答：「1-20 フリーWi-Fi(飲食店・ホテル・商業施設等で提供）以外→1-21 はい」

フリーWi-Fi はセキュリティ上非常に脆弱で、業務や機密情報等を扱う際に利用するべきではありません。フリーWi-Fi と同一の SSID(接続先の Wi-Fi アクセスポイントの名称)を騙る、悪意ある 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て、利用者の個人情報を盗み取る手口等も存在しています(Evil Twin)。このことから、本学ではフリーWi-Fi を業務で使用する事を禁止しています(「情報機器取扱ガイドライン」7 条 7.1 項)。

1-22　SNS やブログ等への機密情報等公開

あなたは業務や研究で大きな成果が上がり、周囲の関係者から評価される等の喜ばしい事がありました。それを SNS(例：X/Facebook/Instagram)やブログ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く

○すぐに掲載する
○掲載による影響が誰に及ぶかわからないために慎重に判断する
○掲載しない

[解説]　正答：「掲載しない」

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掲載することにより、意図しない影響が他者に及ぶ可能性や、機密情報等が漏洩する可能性が有る為、原則公開しないでください。ただし、学内組織の広報活動として、関係者の了承のもと情報公開する場合は除きます。

1-23　多要素認証の利用状況
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、これを利用していますか(https://board.yamanashi.ac.jp/?b=102&k=2023061576384)。 実際の実施状況と回答が異なる場合、確認のために個別にご連絡させていただくことが有ります。 ※[用語] 多要素認証 2 つ以上の認証要素を組合わせて認証を行う手法(例：ID とパスワード&アプリ認証)
○利用している ○検討中 ○利用するつもりはない

1-24　多要素認証を利用しない理由 **条件：1-23 で「利用するつもりはない」を選択**
1-23 で「利用するつもりはない」を選択した方は、その理由をお答えください。
※記述欄

[解説]

Microsoft の研究者が公開した情報によると、多要素認証を利用する事で、アカウントに対する攻撃のうち「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登用されるリスクを大幅に軽減することが出来るため、積極的な導入のご検討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ため、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。

1-25　外部記録媒体取扱手順-確認状況

業務で外部記録媒体(例：USB メモリ)を利用する際の取扱い等を定めた、「外部記録媒体取扱手順」に従い外部記録媒体を管理していますか。(https://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)

利用に際しては、下記のルール等が定められています。
・業務で利用する際…「外部記録媒体登録管理台帳」への記載・「登録用ステッカー等」の貼付
・学外へ持ち出す際…「外部記録媒体持出許可簿」により部局情報システム管理責任者から許可を得る
・外部機関等の外部記録媒体を使用する際…提供元及び使用者自身によるウイルスチェックの実施
※「外部記録媒体取扱手順」より要約
https://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

〇手順に従い運用中
〇運用開始に向け準備中
〇手順の存在を知らなかった
〇外部記録媒体を業務で利用していない

1-26　外部記録媒体取扱手順-ご意見　※任意

外部記録媒体取扱手順については、必要に応じ見直しをする予定です。より良い改訂に向けて、ご意見がありましたらお願いします。(自由記述)

※記述欄

[解説]　正答：「手順に従い運用中」「運用開始に向け準備中」「外部記録媒体を業務で利用していない」

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 等の取扱い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扱いを行っていただきますよう、お願いいたします。

また、同手順につき、ルールの把握に時間がかかる等のご意見をいただきました。対応を検討させていただきます。

1-27　重要なデータのバックアップ
業務で取り扱う重要なデータについて、バックアップをどのように取っていますか。
○バックアップを取っていない ○バックアップを取っている-同じパソコンの別のフォルダ ○バックアップを取っている-別の媒体(外付けハードディスクや NAS 等) ○バックアップを取っている-クラウドサービス(OneDrive 等) ○その他([記述欄])

[解説]

本学では、「情報システム運用・管理内規」の第 49 条により、業務で取り扱う情報に関し、情報の格付に応じて、適切な方法でバックアップを実施する事を規定しています。

バックアップの取得方法としては、下記赤枠に示す「3-2-1 ルール」が効果的です。この方法に従うことにより、パソコンが故障した際に元ファイルとバックアップファイル両方が喪失されてしまうリスクや、パソコン上のファイルを暗号化して閲覧不可能にしたうえで、情報を元に戻す為の身代金を要求する「ランサムウェア」による被害を封じ込めることが出来ます。

バックアップの 3-2-1 ルール

機密情報等の特に重要なデータをバックアップする際に推奨される手法です。

3-2-1 の各数字は、下記の 3 つのバックアップ取得手法を示しています。

・“3”　常に 3 つのバックアップ(コピー)を作成しておく

・“2”　それらを 2 つの異なる媒体に保管しておく

・“1”　そのうち 1 つはネットワークに接続されていないオフライン環境に保管する

例：パソコン上にある要配慮個人情報を含むエクセルファイル「Hairyo.xlsx」のバックアップ

“3”　コピーして 3 つのファイルを作成…Hairyo.xlsx(元)/Hairyo-copy1.xlsx/Hairyo-copy2.xlsx

“2”　Hairyo-copy2.xlsx のみ管理台帳で管理されている USB メモリに保管、他は PC に保管

“1”　USB メモリは通常時はパソコン(ネットワーク)と接続せず金庫で保管する

1-28　情報セキュリティ監査-ご意見　※任意
本調査はいただいたご意見をもとに、毎年度見直しを行っています。より良い調査の実施に際し、ご意見がありましたらお願いします。(自由記述)
※記述欄

[解説]

①アンケート/申請･調査システムの UI の改善提案に係るご意見

次年度以降他の手法での実施や設問の配置の工夫等により改善を重ねてまいります。

②内容が分かり易い旨のご意見

ご感想、ご意見有難うございます。令和 5 年度に多くいただいた「内容が難しい」「設問数が多い」旨のご要望に基づき、一部設問を統廃合し設問数を削減の上用語の注釈を付けさせていただきました。次年度以降も改善を重ねてまいります。

③ルールやセキュリティに関する纏まった資料が欲しい旨のご意見

本監査の設問及び本フィードバック資料の各設問の解説をご参照いただけますと幸いです。

別途情報セキュリティに関する学内のルール等につきご不明点等がございましたら、

情報システム課までお問い合わせください。

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、ご協力のほどよろしくお願いいたします。

以上