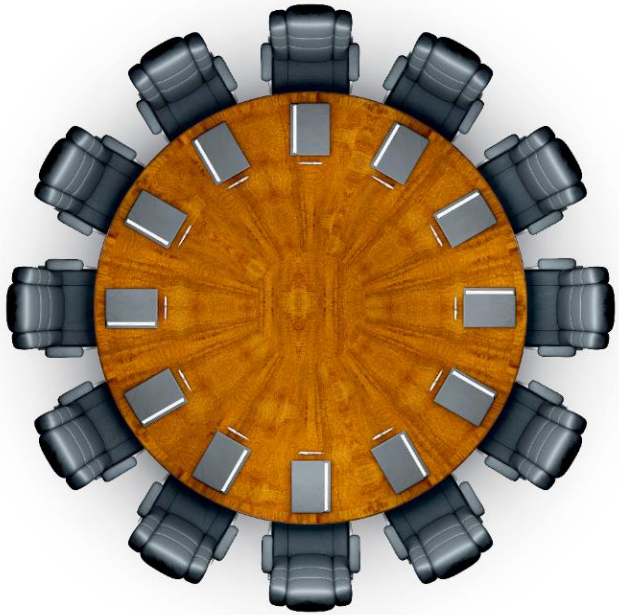

「情報セキュリティ研修教材（システム管理者向け）理解度テスト」

理解度テスト

問 パスワード管理について正しいものを選びなさい

1	同じ文字の繰り返しや短すぎる文字列ではなく、推測されにくい文字列で設定する ➢ 生年月日や辞書に記載されているような一般的な英単語は使用しません
2	パスワードは忘れないように、生年月日や同一の数値を並べて設定する
3	パスワードは一度設定したら、二度と変更してはいけない
4	多段階認証は、煩雑であるため使用しない

正解　1

他人に自分のユーザアカウントを不正に利用されないようにするには、安全なパスワードの設定と管理が必要です。パスワードが漏れる又は盗み出された場合、アカウントの乗っ取りやデータの改ざん、情報漏洩等の様々なリスクがあります。
そのため、他人に推測されづらいパスワードを設定することが重要です。

間違えた方は、8ページに戻り、復習しましょう

問 アップデートの通知が届いたときに実施すべき事項で正しいものを選択しなさい

1	システムの脆弱性を解決するために、迅速にアップデートを実施する
2	何をしたらいいのかわからないため、何もしないで放置する
3	システム部門へ確認し、具体的な指示に従ってアップデートを実施する
4	システム部門がないため、アップデートしてから考える

正解　3

医療機関は複数のシステムが相互に連携しており、アップデート処理によっては、
他システムが正常に稼働しなくなる恐れがあります。
そのため、業務用パソコンやスマートフォンなどでアップデートの通知が届いた場合
は以下の対応を実施します。

■ 院内の情報システム部門または担当者に確認する
■ 事前に情報システム部門より、対応方法の連絡がある場合は指示に従う

間違えた方は10ページに戻り、復習しましょう

問 USB等の記憶媒体の使用で気を付けることのうち、正しいものを選択しなさい

1	USB等の記憶媒体は、情報漏えいのリスクが高いため、使用してはいけません
2	USB等の記憶媒体は、ウイルス感染や情報漏えいのリスクがあるため、個人保有の記憶媒体は使用せずに、医療機関で管理する必要がある
3	USB等の記憶媒体は、便利なツールであり、制限なく利用することが望ましい
4	USB等の記憶媒体は、保存するファイルを暗号化させしておけば、ウイルスチェック機能やパスワード機能や生体認証等の対策を取ることは不要である

正解　2

紛失防止のための取組だけでなく、外部媒体への保存は暗号化の実施、外部媒体自体にウイルスチェック機能やパスワード機能、生体認証等の対策を付与することが重要です

間違えた方は11ページに戻り、復習しましょう

問 業務上でメール送信するときに留意すべき事項について正しいものを選択しなさい

1	急いでメール送信する必要があるため、特に留意すべき事項はない
2	仮にメールの宛先を間違っても、送信先から連絡が来るため気にしない
3	特に重要なメールについては、事前に上司に確認するとともに、メールに添付するファイルはパスワードを設定し、安易に読み取られないようにする
4	毎回Bccで全てメール送信を実施する

正解　3

メールの誤送信は最も多い情報セキュリティインシデントとして挙げられます。小事で済むことが多いですが、宛先や添付メールの内容によっては、情報漏洩という重大なインシデントに発展する可能性がありますので、対策を講じていく必要があります。

間違えた方は9ページに戻り、復習しましょう

問 マルウェアの主な感染経路について正しいものを選択しなさい

1	感染経路は全く不明のため、わからない
2	パソコンやスマートフォン等の機器の接触で感染する
3	同じ部屋の機器等から空気感染する
4	メール（添付ファイル）による感染やWebサイトの閲覧、アプリケーション、ツールのインストールや記憶媒体（USBメモリやCD,DVDなど）を介した感染が多い

正解　4

マルウェアはネットワークやコンピュータ、記憶媒体などから感染します。

間違えた方は13ページに戻り、復習しましょう

問 マルウェアに感染しないために職員が気を付けることについて正しいものを選択しなさい

1	感染経路は全く不明であり、感染予防できないため、特に気を付けることはない
2	パソコンやスマートフォン等の機器の接触で感染するため、機器を近づけない
3	見知らぬ添付ファイル付きの電子メールは注意する（受信メールの信頼性を確認する、添付ファイルを開かない、安易にクリニックしない等）
4	適度に部屋の換気をする

正解　3

身に覚えがない部署や差出人のアドレス、おかしなURL等、違和感を感じたら添付ファイルやリンク先を安易にクリックせずに、周りやシステム管理部門に相談することが大切です。

間違えた方は14ページに戻り、復習しましょう

問　無線LANを貸与するときに、セキュリティの面から気を付けることについて正しいものを選択しなさい

1	減るものではないので、特に気を付けることはない
2	無線LANは気軽に外部からの接続を行うとウイルスやマルウェアが入り込む可能性があるため、訪問者用のアクセスポイントを設定し院内ネットワークと分離する
3	貸与時間に応じて報酬を請求する
4	院内のネットワークに接続するIDやパスワードを教えて貸与する

正解　2

外部の方が持ち込んだノートPCやタブレットをインターネットに接続したいと要望された場合、院内ネットワークの無線LANを知らせれば接続できますが、訪問者の端末からウイルスやマルウェアが入り込む可能性もあるため留意が必要です。

間違えた方は16ページに戻り、復習しましょう

問　なりすましを防止するために必要なことについて正しいものを選択しなさい

1	緊急性がある場合は、相手を確認しないで自分のIDやパスワードを伝えても問題ない
2	送信されてきたメールに添付されているファイルやURL等のリンク先は、念のためクリックして確認する
3	なりすまし、非常に高度のため、現場の職員が対応できることはない
4	折り返し連絡をし、本人確認を行ったうえで回答したり、電話番号などから相手が特定できない問い合わせには答えない

正解　4

攻撃者は、電話やメールを用いて職員などを装い、心理的に答えざるを得ない状況を作り聞き出そうとするため、即時に対応せず本人確認を行う等の対応をすることが重要です。

間違えた方は18ページに戻り、復習しましょう

問　職員による個人情報の持出等の不正を防止するための取組として誤りを選択しなさい

1	アクセス権限について分類して一人の職員でデータの閲覧から出力等を実施できないようにする
2	機密情報へのアクセスについては、アクセス予定時間を申請して承認を取る運用にする
3	担当者間、部門間等で相互に運用状況の点検を実施し、相互牽制を働かせる
4	上司や同僚を疑って仕事をするのは良くないため、人を信じて仕事を進める

正解　4

動機・機会・正当性の3つの要素がそろったときに不正が発生するリスクが高くなります。

間違えた方は21ページに戻り、復習しましょう

問　情報セキュリティ対策としての組織的対策として誤っているものを選択しなさい

1. 情報システム部門及び担当者、専門スタッフの配置
2. セキュリティ対策としての規定やマニュアル等の整備
3. セキュリティにかかる予算の確保
4. 麻薬や劇薬の保管管理の徹底

正解　4

医療安全対策としては、麻薬や劇薬の管理は非常に重要になりますが、情報セキュリティ対策ではありません。

間違えた方は28～29ページに戻り、復習しましょう

問　情報セキュリティ対策としての物理的対策として誤っているものを選択しなさい

1　セキュアなネットワークの設計

2　特定区域の入退室管理、施錠管理

3　端末等の盗難防止策の実施

4　患者の転倒、転落防止策の実施

正解　4

医療安全対策としては、患者の転倒・転落防止策の実施は非常に重要になりますが、
情報セキュリティ対策ではありません。

間違えた方は28～29ページに戻り、復習しましょう

問 セキュリティの視点から業務で異常を感じた時の対応として誤っているものを選択しなさい

1	院内の情報部門やセキュリティ担当者に連絡をする
2	システムベンダー等に問い合わせを実施する
3	上司や同僚に相談する
4	日々の業務が大変なため、何もしない

正解　4

日々の業務でなにかしら異常を感じたら、まずはシステム部門やセキュリティ担当者に連絡して指示を受けましょう。迅速な初動対応が重要です。

間違えた方は5ページに戻り、復習しましょう

問　サイバー攻撃を受けた医療機関で発生した損害について誤っているものを選択しなさい

1　システムの稼働が停止し、患者へ診療行為ができなくなった

2　システム内の患者の情報が暗号化されてしまい、過去の記録等を閲覧できなくなった

3　サイバー攻撃で医療機関が損害を受けることはほとんどない

4　患者の診療にかかる記録（個人情報）が外部へ流出してしまった

正解　3

日本においても海外においても、サイバー攻撃により医療機関が個人情報の漏えいや診療停止等の深刻な損害をうけています。
間違えた方は22～24ページに戻り、復習しましょう

問 情報セキュリティ対策としての技術的対策として誤っているものを選択しなさい

1. ウイルス対策ソフトの導入
2. 更新プログラムの適用
3. ファイヤーウォールの導入
4. 外部ベンダーに全て任せる

正解　4

外部ベンダーのセキュリティ体制やセキュリティ確保に向けた取組等については、リスクと一緒に説明を受けて、対応策を検討する必要があります。

間違えた方は26～29ページに戻り、復習しましょう

問 情報セキュリティ対策としての人的対策として正しいものを選択しなさい

1. 特定区域への入退室管理
2. システムへのアクセスログの記録や分析
3. セキュリティにかかる教育訓練
4. セキュリティにかかる規定やマニュアルの整備

正解　3

特定区域の入退室管理は物理的対策、システムのアクセルログの記録や分析は技術的対策、セキュリティにかかる規定やマニュアルの整備は組織的対策になります。

間違えた方は28～29ページに戻り、復習しましょう

問　サイバー攻撃等によるシステム障害の復旧処理時に留意すべき事項として誤っているものを選択しなさい

1	迅速に復旧させるためにバックアップを取らずにシステムを初期化する
2	被害拡大の防止のためにネットワークの遮断や使用しているIDやパスワードの無効化等の対策を実施する
3	職員や外部委託先等にシステム復旧までシステムの利用ができないことを伝達する
4	証拠保全のためにシステム上に残された記録のバックアップを取る

正解　1

不正アクセスや不正プログラム等の情報システムからの情報漏えいの可能性がある場合は、証拠保全のためにシステム上の記録を消さないようにする必要があります。
間違えた方は32ページに戻り、復習しましょう

問　サイバー攻撃により、医療サービス提供体制に支障が発生する場合に必要な手続として正しいものを選択しなさい

1	何もしない
2	厚生労働省医政局研究開発振興課医療技術情報推進室へ報告する
3	原因調査を実施して再発防止策を検討する
4	再発防止策の取組を実践する

正解　2

厚生労働省医政局研究開発振興課医療技術情報推進室へ報告する必要があります。
原因調査や再発防止策の取組については、報告後の手続になります。

間違えたからは33ページに戻り復習しましょう

問　サイバー攻撃により、個人情報の漏えい、滅失又は毀損等の恐れがある場合の対応として正しいものを選択しなさい

1	何もしない
2	個人情報保護委員会へ報告する
3	報告すると話が大きくなるため、システム担当者のみで留める
4	後で問題にならないように自分たちで復旧する方法を検討する

正解　2

個人情報保護委員会へ報告する必要があります。

間違えた方は33ページに戻り復習しましょう

問　セキュリティ事故発生後の再発防止の取組として誤っているものを選択しなさい

1	再発防止に向けて関係部門の責任者等へ日常業務への反映を指示する
2	再発防止のために設備投資が必要な場合は、必要コストや効果について経営層に説明する
3	職員や外部委託先に指示を実施するとともに、取組状況のモニタリングを定期的に実施する
4	再発防止の取組を実施することは困難であるため、特に実施する取組はない

正解　4

再発防止の取組については、日々の業務へ反映するとともに、定期的なモニタリングが重要です。

間違えた方は34ページに戻り復習しましょう

問　情報セキュリティガイドラインとして誤っているものを選択しなさい

1. 医療情報システムの安全管理に関するガイドライン
2. 医療情報を取り扱う情報システムサービスの提供事業者における安全管理ガイドライン
3. 医療・介護関係事業者における個人情報の適切な取り扱いのためのガイダンス
4. 医療法人会計基準

正解　4

医療法人会計基準とは、医療法人が準拠すべき「一般に公正妥当と認められる会計の慣行」を具体化するものの一つとして取りまとめたものであり、セキュリティに関する基準ではありません。

間違えた方は6ページに戻り復習しましょう