「情報セキュリティ教育2025春期」確認テスト　解答・解説

2025年3月28日
TCS-HD情報セキュリティ室

教材の該当ページ
（17頁参照）

設問1　顧客ルールについて、**適切**なものを選択しなさい。

1. 顧客先で勤務しているが自社のセキュリティ規程やガイドラインを遵守しているので問題ない。

解説：顧客には顧客のルールが定められています。自社のセキュリティ規程やガイドラインもそうですが、顧客のルールも遵守する必要があります。
定期的に顧客ルールの確認を行い、ルールの遵守に勤めてください。
よって、**不適切**　です。

該当する規程・ガイドライン
「情04-12 社給端末利用ガイドライン」
> 第4章　作業端末(PC)に関する指針 > 1.利用指針

2. 業務効率化の為、先輩から教えてもらったツールを顧客から貸与されたPCにインストールした。

解説：ツールやシステム等の業務利用は認められたもの以外は使用しないでください。
使用する場合はPJリーダーや、顧客へ確認をしてください。

よって、**不適切**です。

該当する規程・ガイドライン
「情04-12 社給端末利用ガイドライン」
> 第4章　作業端末(PC)に関する指針 > 1.利用指針

3. 顧客ルールが変更されていないか、定期的に確認をしている。

解説：ルールは取り扱っている情報やシステムによって変更される場合があります。
過去にルールを確認していたとしても、ルールが変わり、今まで認められていたものも認められなくなることもあります。ルールは定期的に確認してください。
よって、**適切**です。

該当する規程・ガイドライン
「情04-12 社給端末利用ガイドライン」
> 第4章　作業端末(PC)に関する指針 > 1.利用指針

正解：3

設問2　飲酒に関する注意事項について、**不適切**なものを選択しなさい。

（18頁参照）

1. 居酒屋で社給スマホを取り出し、来ていたチャットに返信した。

解説：居酒屋は公共の場です。公共の場では業務を行わないようにしましょう。
また飲酒している場合は、注意力が低下するなどして置き忘れてしまうかもしれません。
居酒屋で社給スマホを取り出し、置き忘れる事故も発生しています。
カバンなどにしまって置き、さらにそのカバンを置き忘れないように注意しましょう。
よって**不適切**です。

該当する規程・ガイドライン
「情02 機密情報管理規定」
＞第一章　第5条（機密漏えいの禁止）＞一般禁止規定

2. 業務後飲み会の予定があったので、PCを持ち帰らず、鍵付きキャビネットにしまってから退勤した。

解説：飲酒をすると、注意力が低下し、カバンを置き忘れてしまったり、酔っ払いを狙った窃盗に遭う可能性もあります。飲酒する際には原則として情報資産を持たないようにしてください。
よって**適切**です。

該当する規程・ガイドライン
「情02 機密情報管理規定」
＞第一章　第5条（機密漏えいの禁止）＞一般禁止規定

3. 居酒屋から退店する際に、飲み会参加者同士で忘れ物がないかチェックをした。

解説：飲酒による紛失を防ぐために飲食店などから帰るときに忘れ物がないか確認したり、
帰りの電車内では荷物を網棚や足元に置かず、カバンをたすき掛けするなど、
普段より慎重な行動を行ってください。
よって**適切**です。

該当する規程・ガイドライン
「情02 機密情報管理規定」
＞第一章　第5条（機密漏えいの禁止）＞一般禁止規定

正解：1

設問3　社給スマホに関する文章のうち、**不適切なものをすべて**選択しなさい。　（28頁参照）

1. 開発画面情報を顧客未許可の社給スマホで撮影して、社内メンバーにメールで問い合わせた。

解説：社給スマホで撮影することは、機密情報を持ち出すリスクがあります。
このような機密情報の持出しは原則、禁止としています。
また万が一持ち出す場合でも、まず顧客の許可を取ってください。
さらに自分の上長の許可を取り、顧客が認める保存先(社給スマホや開発PCなど)に格納してください。
よって、**不適切**　です。

該当する規程・ガイドライン
「情04-11 社内環境利用ガイドライン」
＞第2章　オフィス環境について＞1. 物理セキュリティ対策　情報資産の管理
「情04-12 社給端末利用ガイドライン」
＞第4章　作業端末(PC)に関する指針＞1. 利用指針＞1. 3セキュリティ対策　情報の保存
「情04-08開発ネットワークガイドライン」
＞第2章 利用者の指針＞3. 顧客ネットワークに接続したネットワーク区画の利用＞機密情報の移動

2. 在宅勤務中、業務用PCの調子が悪いため、顧客未許可の社給スマホでWeb会議に参加した。

解説：顧客との合意事項を優先して遵守して安全を確保しなければいけません。
顧客の許可を得ていない端末を顧客ネットワークに接続すると、顧客ルール違反と判断されることがあります。顧客貸出し機器以外はすべて、顧客の許可を得なければいけません。
よって、**不適切**です。

該当する規程・ガイドライン
「情報04-08開発ネットワークガイドライン」
＞第2章　利用者の指針＞3. 顧客ネットワークに接続したネットワーク区画の利用＞ネットワーク区画のセキュリティ確保

3. お客様も業務用スマホでWeb会議に参加しているので、許可を得ていないが自社の社給スマホでWeb会議に参加した。

解説：たとえ顧客社員が業務用スマホを利用してWeb会議に参加していたとしても、必ず顧客の許可を得てから端末を顧客ネットワークに接続しなければいけません。
よって、**不適切**です。

該当する規程・ガイドライン
「情報04-08開発ネットワークガイドライン」
＞第2章　利用者の指針＞3. 顧客ネットワークに接続したネットワーク区画の利用＞ネットワーク区画のセキュリティ確保

正解：1、2、3

設問4　在宅勤務に関する文章のうち、**不適切**なものを選択しなさい。　（29頁参照）

1. 社給PCと社給スマホをUSBケーブルで接続し、社給スマホは自宅の無線LANに接続して業務を行った。

解説：在宅勤務を行う際のネットワークは、社給スマホのテザリングや会社が許可したモバイルルーターを利用できます。また社給スマホを自宅の無線LANに接続し、パケットを抑制することが許可されています。
よって、**適切**です。

該当する規程・ガイドライン
「情04-08 開発ネットワークガイドライン」＞第2章 利用者の指針＞4. テレワーク

2. 在宅勤務を行うためPCを持ち帰る際、バッグを持っているのが大変だったので網棚に置いた。

解説：在宅勤務を行う際に、PCを持ち運ぶことが多くあります。業務情報を運搬する場合は、速やかに目的地まで移動し、盗難や紛失などの事故に遭わないよう十分な注意が必要です。
運搬する際は、肌身離さず持ち運ぶことが望ましいです。
よって、**不適切**です。

該当する規程・ガイドライン
「情04-12 社給端末利用ガイドライン」＞第2章 作業場所について＞2. 2 送付・運搬対策

3. 顧客の許可を得た上で顧客貸与PCを自宅ネットワークに直接接続してWeb会議に参加していた。

解説：顧客の貸与物は、すべて顧客ルールが適用されます。TCSグループでは社給PCを直接自宅ネットワークに接続することは禁止されておりますが、顧客が顧客PCを自宅ネットワークにつなげることを許可されているケースがあります。顧客貸与物に関するルールは、入場時に必ず確認してください。
よって、**適切**です。

該当する規程・ガイドライン
「情04-08 開発ネットワークガイドライン」＞第2章 利用者の指針＞4. テレワーク

正解：2

設問5　コンピュータウイルスに関する文章のうち、**不適切**なものを選択しなさい。　（43頁参照）

1．ウイルス感染したことを自社の情報セキュリティ担当者に報告し、指示を仰いだ。

解説：ウイルス感染、またはウイルス感染が疑われる場合、まず最初にネットワークから切り離してください。（有線LANを利用している時はLAN線を抜く、無線LANを利用している時は、接続設定を「切断」してください。）
あわせて、周囲の人へも事象を伝え、感染が拡散していないか確認します。
そして、自社のシステム管理者またはセキュリティ担当者に状況（PCの挙動や症状、気づいた日時など）を報告してください。感染かどうかわからない場合でも、必ず報告してください。
よって**適切**です。

該当する規程・ガイドライン

「情04-08開発ネットワークガイドライン」
＞第6章 外部からの攻撃対策指針＞1．ウイルス感染、拡散防止＞ウイルス感染、拡散防止
「情04-11 社内環境利用ガイドライン」
＞第4章　ネットワーク設計・構築指針＞3．外部ネットワークからの攻撃対策 ウイルス感染、拡散防止
「情04-12 社給端末利用ガイドライン」
＞第5章　作業端末（スマホ）に関する指針＞1．利用指針＞1．4事故対応　ウイルス感染の疑い

2．ウイルス感染に気が付いたため、周りに言わずにすぐ自分のPCのみ手動でウイルス検索を実施した。

解説：選択肢1と同様に、最初にネットワークから切り離し、周囲に事象を伝え、自社のシステム管理者またはセキュリティ担当者に状況を報告してください。そのうえで、手動でウイルス検索を行います。
決して自分だけの問題ではなく、周りに伝えて感染拡大を防がなければいけません。
よって**不適切**です。

該当する規程・ガイドライン

「情04-11 社内環境利用ガイドライン」
＞第4章　ネットワーク設計・構築指針＞3．外部ネットワークからの攻撃対策 ウイルス感染、拡散防止
「情04-12 社給端末利用ガイドライン」
＞第5章　作業端末（スマホ）に関する指針＞1．利用指針＞1．4事故対応　ウイルス感染の疑い
「情04-08開発ネットワークガイドライン」
＞第6章 外部からの攻撃対策指針＞1．ウイルス感染、拡散防止＞ウイルス感染、拡散防止

3．感染したPCについて、初動対策完了後、初期化インストールしてから、自社ネットワークに接続した。

解説：ウイルス感染したPCを再利用する場合、PCの初期化インストールを行い、初期状態に戻したのち、ネットワークに接続することが必要です。
よって**適切**です。

該当する規程・ガイドライン

「情04-11 社内環境利用ガイドライン」
＞第4章　ネットワーク設計・構築指針＞3．外部ネットワークからの攻撃対策 ウイルス感染、拡散防止
「情04-12 社給端末利用ガイドライン」
＞第5章　作業端末（スマホ）に関する指針＞1．利用指針＞1．4事故対応　ウイルス感染の疑い
「情04-08開発ネットワークガイドライン」
＞第6章 外部からの攻撃対策指針＞1．ウイルス感染、拡散防止＞ウイルス感染、拡散防止

正解：2

設問6　メールの誤送信対策の行動として**不適切**なものを選択しなさい。　（43項参照）

1. メール誤送信対策機能から自動返信された内容は宛先、件名、本文、添付ファイル名、添付ファイルの内容を必ず指差し確認をしてから、メールの送信を行っている。

解説：メール誤送信対策機能を活用することによって、メールの送信前に必ず宛先、本文、添付物の再確認が実施されます。特に急いでいる時や、複数のメールの対応をおこなっている時は、誤送信対策機能に表示された内容をよく確認してから送信を行ってください。
確認することによって、宛先、本文、添付物の誤りを訂正出来るため、誤送信の防止として有効です。
よって、**適切**です。

該当する規程・ガイドライン
「情04-10 コミュニケーションツール利用ガイドライン」＞第2章　利用指針＞2. コミュニケーションツールの利用における注意事項

2. 身に覚えがないメールが届いた時、上長、部門長、メンバーに報告のみ行ってメールの開封はしていない。

解説：送信元に心当たりがない場合には、開封と同時にウイルスが感染・発症する可能性が考えられるため、メールの開封を行わないでください。確証や自信がないのであれば上長、部門長、周りの人に相談をしてください。
よって、**適切**です。

該当する規程・ガイドライン
「情04-10 コミュニケーションツール利用ガイドライン」＞第2章　利用指針＞2. コミュニケーションツールの利用における注意事項＞2. 2　メール＞（3）ファイルの授受

3. メールの宛先間違いに気づいたが、誤って送った相手からメールを消した連絡があったので、そのまま業務を続けた。

解説：メールの誤送信は、第三者に情報が渡った時点で、情報資産の漏洩となり情報セキュリティー事故に該当します。誤って送信してしてしまった相手が適切な対応を実施していたとしても、事故報告を行う必要があります。
よって、**不適切**です。

該当する規程・ガイドライン
「情02-01 情報セキュリティ事故報告ガイドライン」＞第3章　事象と報告対象＞2. 報告基準

正解：3

設問7　SNSを利用する際の行動として**適切**なものを選択しなさい。　（44項参照）

1. 職場の先輩が公開前の製品情報を教えてくれたので、SNSアカウントで製品情報を投稿した。

解説：企業の未公開製品情報は通常、機密情報として扱われ、外部に漏らすことは契約違反や法的問題を引き起こす可能性があるため、情報漏えい事故にあたります。また、情報漏えいを起こした事により、信頼関係が失われる可能性があります。
機密情報の取り扱いに十分注意し、公開前の情報を外部に漏らさないようにすることが重要です。
よって、**不適切**です。

該当する規程・ガイドライン
なし。

2. プロジェクトの打ち上げ終了後、メンバーと記念撮影をしてSNSに画像つきで投稿した。

解説：個人の特定に繋がる顔写真や、場所の特定に繋がる情報を不特定多数が閲覧するSNSに公開する行動はセキュリティリスクやプライバシーリスクの増加に繋がります。個人、企業アカウントで情報の発信などを行う場合は、フィルターや加工を利用して個人や場所の特定に繋がる危険性がある情報公開は極力、避けることが重要です。
よって、**不適切**です。

該当する規程・ガイドライン
なし。

3. 著名人のスキャンダルや災害情報などを見かけても、投稿内容を確認してから発信するか判断している。

解説：情報の真偽を確認することが重要です。発信するまえに確認することで、誤った情報を拡散することを防ぎ、信頼性のある情報を共有することができます。真偽を確認せずに発信してしまい、個人のプライバシーの侵害、誤った災害情報を拡散してしまい社会に大きな影響を与えてしまう可能性があります。真偽を確認しないまま、安易な発信をすることは控えましょう。
よって、**適切**です。

該当する規程・ガイドライン
なし。

正解：3

設問8　生成AI利用時の注意事項として**適切**なものを選択しなさい。

（45頁参照）

1. 生成AIの回答は常に進化しているので、内容の確認をする必要はない。
解説：AIが生成した内容には誤った情報が含まれる可能性があります。
社内で精査することで、誤った情報を排除し、正確で信頼性の高い情報を活用することができます。
AIが生成した内容が既存の作品やアイデアに似ている場合、知的財産権の侵害となるリスクがあります。社内で精査することにで、これらのリスクを事前に発見し、適切な対策を講じることができます。
よって、**不適切**です。

該当する規程・ガイドライン
なし

2. 生成された画像や映像はオリジナルなので、著作権や肖像権を気にする必要はない。
解説：AIが生成したイラストが既存の作品やキャラクターに似ている場合、著作権や商標権の侵害となる可能性があります。これにより、法的なトラブルや賠償請求が発生するリスクがあります。
AIが生成するイラストは、既存のデータを基にしているため、完全にオリジナルなデザインを保証することはとても難しいです。
生成物を採用する前に、社内で十分に検討する事が重要です。
よって、**不適切**です。

該当する規程・ガイドライン
なし

3.生成された内容を使用する前に、生成内容を周りの人や有識者に相談している。
解説：内容が正確でない場合、誤った情報を広めてしまう可能性があります。誤った情報を広めてしまうと、組織の信頼性を失うことにも繋がります。生成された内容が正確であるかどうかを確認するために、周りの人や社内の有識者の意見を聞くことは重要です。これにより、誤った情報を使用するリスクを減らすことができます。
よって、適切です。

該当する規程・ガイドライン
なし

正解：3

設問9　マイナンバー制度に関して**不適切**なものを選択しなさい。　（55頁参照）

1. マイナンバーと個人番号は同じものである。

解説：マイナンバーは通称で、正式名称は個人番号といいます。
よって、**適切**です。

該当する規程・ガイドライン
「情09 特定個人情報取扱規程」＞第1章　総則＞第2条＞第3項

2. マイナンバーは定期的に変更される。

解説：マイナンバーは生涯にわたって利用する番号です。
よって、**不適切**です。

該当する規程・ガイドライン
「情09 特定個人情報取扱規程」＞第1章　総則＞第2条＞第3項

3. マイナンバーは「社会保障」「税」「災害対策」の分野で、それぞれの機関に存在する個人の情報が、同一人の情報であることの確認のために利用される。

解説：マイナンバー法（行政手続における特定の個人を識別するための番号の利用等に関する法律）により、個人番号の利用範囲については厳格に限定されており、それ以外の目的で利用することは禁止されています。
よって、**適切**です。

該当する規程・ガイドライン
「情09 特定個人情報取扱規程」＞第1章　総則＞第2条＞第6項

正解：2

設問10 情報セキュリティ事故発生時の対応として、**適切**なものを選択しなさい。 （66頁参照）

1. 出社時に入館証を紛失している事に気が付いた、急いで取りに帰り、無事自宅で見つかった。

解説：自宅にあるかもしれないという場合でも、事故を認識したらすぐに第一報をしてください。
一報が遅れ、事故が拡大する場合もあります。
探し始める前に第一報を行ってください。
よって、**不適切**です。

該当する規程・ガイドライン
「情02-01 情報セキュリティ事故対応・報告ガイドライン」
＞第4章　事故発生時の対応及び報告＞3. 報告の時間軸

2. 居酒屋で飲酒し、帰宅後に社給スマホがないことに気づいたが時間も遅いこともあり連絡が取れないと考え、翌日朝一番に報告した。

解説：第一報は事故が発生した時間に関わらず、認識した段階ですぐに行ってください。
事故報告が遅れると事故の拡大の他、隠ぺいを疑われる可能性もあります。
よって、**不適切**です。

該当する規程・ガイドライン
「情02-01 情報セキュリティ事故対応・報告ガイドライン」
＞第4章　事故発生時の対応及び報告＞3. 報告の時間軸

3. ヒヤリハットが発生してしまったため、チームで原因を分析し、対策を運用することにした。

解説：ヒヤリハットを分析し、対策を練ることで事故の予防策にもつながります。
事故にならなくてよかった、とやり過ごしてしまうといつか大きな事故や事件を引き起こす可能性があります。ヒヤリハットが発生したときの行動を振り返り、チームや部署内で情報共有を行い、
事故の予防策に活用してください。
よって、**適切**です。

該当する規程・ガイドライン
「情02-01 情報セキュリティ事故対応・報告ガイドライン」
＞第4章　事故発生時の対応及び報告＞4. 報告内容

正解：3