

付録

平成28年度春期
情報セキュリティ
マネジメント

平成 28 年度春 情報セキュリティマネジメント試験 解答解説 午前

[問 1] 解答 ウ

CSIRT (Computer Security Incident Response Team, シーサート) は, 企業内や政府機関などに設置される組織で, 情報セキュリティインシデントに関する報告を受け, 対応を行います。したがって, ウが正解です。

アは ICANN (The Internet Corporation for Assigned Names and Numbers), イは IETF (The Internet Engineering Task Force), エは共通思想集団の説明となります。

[問 2] 解答 ウ

クリアデスクとは, 情報セキュリティ対策での行動指針の一つで, 自席の机の上に情報資産を放置しないことです。夜間などは施錠できる安全な場所に保管することが推奨されています。したがって, ウが正解です。

アはフォルダ管理, イはクリアスクリーン, エはセキュリティワイヤの説明となります。

[問 3] 解答 イ

情報セキュリティの整備, 運用状況などについて, 独立かつ専門的な立場の人が検証, 評価し, 保証又は助言を与えるものは, 情報セキュリティ監査です。したがって, イが正解となります。

ア 実際に運用している人自身が, その有効性について評価・分析を行う手法です。

ウ 組織の情報セキュリティ対策自己診断テストで, IPA セキュリティセンターが公開 (<http://www.ipa.go.jp/security/benchmark/>) しています。

エ 犯罪捜査や法的紛争などのために, コンピュータなどのデジタル記録を収集・分析し, 法的な証拠とするものです。

[問 4] 解答 イ

モバイル機器を紛失したとき, 情報漏えいを防止するためには, モバイル機器内の情報をリモートから消去できる機能 (リモートワイプ機能) を持ったツールが有効です。したがって, イが正解となります。

アは SNS 経由での情報漏えい, ウはモバイル通信時の情報漏えい, エはショルダーハッキングなどでの情報漏えいの対策として有効です。

[問 5] 解答 ア

JIS Q 27001 の「6.1.3 情報セキュリティリスク対応」には, 「残留している情報セキュリティの受容について, リスク所有者の承認を得る」とあります。したがって, アが正解です。

イ 受容するリスクもモニタリングやレビューを行う必要があります。

ウ、エ リスクを受容するかどうかは、リスク分析後で、リスク対応の前に決定します。

[問 6] 解答 イ

JIS Q 27001 の「5.2 方針」には、情報セキュリティ方針は、「組織内に伝達する。」「必要に応じて、利害関係者が入手可能である。」という事項を満たさなければならないとあります。したがって、イが正解です。

ア 情報セキュリティ方針は機密情報ではありません。

ウ 情報セキュリティ方針はトップマネジメントがリーダーシップをとって確立します。

エ 制定後に見直して改訂していく ISMS のプロセスを確立する必要があります。

[問 7] 解答 ア

IPA が作成した「組織における内部不正ガイドライン」では、「4-4. 技術・運用管理 (12) ネットワーク利用のための安全管理」で、「組織のネットワーク利用では、PC 等の情報機器から重要情報が漏えいしないように、ファイル共有ソフト及びソーシャル・ネットワーク・サービス (SNS)、外部のオンラインストレージ等の使用を制限して安全なネットワーク環境を整えなければならない。」と記載されています。したがって、アが正解です。

イ 私用のメールアドレスなどの利用は制限すべきです。

ウ ウイルス対策ソフトは、常に有効にしておく必要があります。

エ 組織が使用を許可していないソフトウェアはインストールしてはいけません。

[問 8] 解答 ウ

JIS Q 27002 の「9.2.3 特権的アクセス権の管理」に、「各々のシステム又はプロセス (例えば、オペレーションシステム、データベース管理システム、各アプリケーション) に関連した特権的アクセス権」とあるように、特権的アクセス権とは、システムを管理特権で操作するために必要な権限です。システム管理者が、業務システムのプログラムのバージョンアップを行うには特権的アクセス権が必要ですので、ウが正解です。

ア、イは通常のアクセス権、エはゲスト用のアクセス権を利用した行為です。

[問 9] 解答 ア

“不正のトライアングル”理論によると、不正行為は、機会、動機、正当化という 3 要素の不正リスクがすべて揃ったときに起きると言われています。したがって、アが正解です。

イは情報セキュリティの 3 要素、ウは 3C 分析の 3 つの視点です。エは AAA (Authentication, Authorization, Accounting) であり、3 つの異なるセキュリティ機能の枠組みです。

[問 10] 解答 エ

IPA の「組織における内部不正ガイドライン」では、「4-5. 証拠確保 (17) 情報システムにおけるログ・証跡の記録と保存」で、「内部不正の早期発見及び (27) の事後対策の影響範囲の観点から、重要情報へのアクセス履歴及び利用者の操作履歴等のログ・証跡を記録し、定めた期間に安全に保存することが望ましい。」と記載されています。したがって、エが正解です。

ア 定めた期間の保管が適切です。

イ, ウ 内部不正を助長することになりますので適切ではありません。

[問 11] 解答 エ

BYOD (Bring Your Own Device) とは、従業員が私物の情報端末を持ち込んで業務に利用することです。セキュリティ設定の不備などにより情報セキュリティリスクは増大しますので、エが正解です。

ア, イは情報端末の持ち出しによるリスク, ウは情報端末の持ち込みによるリスクとなります。

[問 12] 解答 ウ

IDS (Intrusion Detection System : 侵入検知システム) とは、サーバやネットワーク上で不正侵入を検知するシステムです。セキュリティポリシーを侵害するような挙動を管理者へ通知しますので、ウが正解です。

アは、JVN (Japan Vulnerability Notes) が提供する「MyJVN バージョンチェッカ」などが該当します。イはファジング, エは情報セキュリティ対策ベンチマークの説明となります。

[問 13] 解答 イ

Web サーバに送信された HTTP データを検査して、SQL インジェクションなどの攻撃を遮断するためのファイアウォールを WAF (Web Application Firewall) といいます。したがって、イが正解です。

ア SSL (Secure Sockets Layer) を使って通信を暗号化し、VPN (Virtual Private Network) を構築する機能です。

ウ 複数のコンピュータを結合し、ひとまとまりのシステムにする機能です。

エ 複数台のサーバを並列に稼働させて、負荷分散させる機能です。

[問 14] 解答 イ

PC におけるマルウェア対策では、ウイルス対策ソフトの導入だけでなく、OS 及びアプリケーションの修正パッチを適切に適用することも大切です。したがって、イが正解とな

ります。

ア 定義ファイルが新しくなっていると、以前の定義ファイルでは検出できなかったウイルスが検出される可能性があります。そのため、全てのファイルを対象とします。

ウ、エ このような場合のウイルス感染対策には、ポートの遮断や動的グローバル IP アドレスの付与などは意味がありません。

[問 15] 解答 ウ

内部不正を防止する対策としては、一人のシステム管理者に権限が集中しないように権限を分散し、相互に監視できるようにすることが有効です。したがって、ウが正解です。

ア 複数の管理者 ID を利用する必要があります。

イ 必要時にのみ、特権が付与された管理者 ID を使う必要があります。

エ 操作ログには、本人にアクセス権限は付与しません。

[問 16] 解答 ウ

デジタルフォレンジックスでは、法的な証拠性を確保するために、ログなどのハッシュ値を取得します。改ざんを検出し、原本と複製の同一性を証明することができますので、ウが正解です。

ア パスワードをハッシュ化してファイルに保存するときのハッシュ値の利用目的です。

イ ハッシュ値から元のデータは復元できません。

エ 盗聴の有無は、ハッシュ値では判別できません。

[問 17] 解答 ウ

磁気ディスクを廃棄する場合には、ディスク内の情報を完全に消去する必要があります。ランダムなビット列で、磁気ディスクの全領域を上書きすることで、ディスク内のデータを読み出せないようにすることが可能です。したがって、ウが正解となります。

アの圧縮や、イのマスタブートレコードの消去、エのファイル名の変更などは、データの消去には役に立ちません。

[問 18] 解答 ア

2 要素認証とは、認証に用いる情報の種類である認証の 3 要素、「記憶」、「所持」、「生体」のうち 2 要素を用いて行う認証です。IC カード認証は所持の認証、指紋認証は生体の認証ですので、この二つの組合せは 2 要素認証となり、アが正解です。

イは二つとも所持の認証、ウは二つとも生体認証、エは二つとも記憶の認証です。

[問 19] 解答 ウ

APT (Advanced Persistent Threat) は、サイバー攻撃の一種で、標的型攻撃のうち高

度で執拗な攻撃を指します。持続的標的型攻撃などと訳されることもあります。特定の目的を持ち、標的の組織に執拗に攻撃を繰り返しますので、ウが正解です。

ア、イ 高度な攻撃ではありませんので誤りです。

エ APT は不特定多数への攻撃ではありませんので誤りです。

[問 20] 解答 ウ

HDD (Hard Disk Drive : ハードディスクドライブ) は、補助記憶装置の一種です。HDD 自体を暗号化するためには、HDD パスワードを設定して暗号化し、HDD だけを抜き取られても情報を読み出せないようにしておく必要があります。したがって、ウが正解です。

ア、イ、エでは、HDD を抜き取られたときに情報が漏えいするリスクがあります。

[問 21] 解答 エ

クロスサイトスクリプティングとは、不正なスクリプトを実行させる攻撃です。罠を仕掛けた Web ページを利用者が閲覧し、リンクをクリックしたときに不正スクリプトが実行されますので、エが正解です。

アは SQL インジェクション、イは DoS 攻撃 (Denial of Service attack)、ウはバッファオーバーフローに該当するものとなります。

[問 22] 解答 イ

クリックジャッキング攻撃とは、Web ページのリンクやボタンなどを隠蔽・偽装してクリックを誘う攻撃です。透明化した標的サイト B を配置して Web サイト A の操作に見せかける攻撃はクリックジャッキング攻撃に該当しますので、イが正解です。

アは HTTP レスポンス分割攻撃、ウはタブナビング攻撃、エはブラウザハイジャックに該当します。

[問 23] 解答 ウ

送信者 A が作成した文書ファイルのデジタル署名は、文書ファイルのハッシュ値に対して、送信者 A の署名生成鍵 Y を用いて暗号化したものです。受信者 B は、デジタル署名を署名検証鍵 X で復号し、文書ファイルのハッシュ値と照合することで、文書ファイルが改ざんされていないことと、デジタル署名が署名生成鍵 Y によって生成されたことの両方が確認できます。したがって、ウが正解です。

アの改ざんの部位や、イのウイルスに感染していないこと、ウの改ざんがどちらで行われたかなどは、デジタル署名では判定できません。

[問 24] 解答 イ

認証局 (CA : Certificate Authority) は、公開鍵に対するデジタル証明書を発行する

機関です。したがって、イが正解となります。

ア 秘密鍵を共有するのは、共通鍵暗号方式です。

ウ デジタル署名は CA が発行したデジタル証明書に付与され、CA が確かに生成していることを確認できます。

エ パスワードは、公開鍵暗号では利用しません。

[問 25] 解答 ウ

ドライブバイダウンロード攻撃とは、Web サイトなどを通じて、利用者が気づかぬうちにソフトウェアをダウンロードさせる攻撃です。利用者の PC に不正プログラムが転送されますので、ウが正解です。

アは USB メモリで感染するウイルス、イはランサムウェア、エはウォードライビングの説明となります。

[問 26] 解答 エ

パスワードリスト攻撃とは、別のサイトやシステムなどで流出した利用者 ID とパスワードのリストを使用して、他のサイトへのアクセスを試みる攻撃です。他サイトの利用者 ID とパスワードの一覧表を用いてログインを試行しますので、エが正解です。

アは辞書攻撃、イ、ウはブルートフォース攻撃の手口に該当します。

[問 27] 解答 イ

バックドアとは、利用者に気づかれずにシステム内に秘密裏に仕込まれた遠隔操作のための窓口です。秘密裏に作成した利用者アカウントはバックドアに該当しますので、イが正解です。

ア、ウ、エは有効なアカウントとして利用できず、バックドアとしては機能しません。

[問 28] 解答 イ

暗号アルゴリズムの AES (Advanced Encryption Standard) は、米国の新暗号規格として規格化された共通鍵暗号方式です。暗号化には PC とサーバで共有された共通鍵を用いますので、イが正解です。

ア、ウ、エは、公開鍵暗号方式で利用する鍵となります。

[問 29] 解答 ア

ポートスキャンとは、利用可能なポートを探す行為です。ポート（番号）が分かると、それを利用しているサービスが分かりますので、攻撃できそうなサービスがあるかどうかを調査できます。したがって、アが正解です。

イ ID チェッカーなどが利用されます。

ウ スパイウェアなどが利用されます。

エ rootkit などが利用されます。

[問 30] 解答 エ

A さんが B さんの公開鍵で暗号化した電子メールは、B さんの公開鍵のキーペアである B さんの秘密鍵でのみ復号できます。そのため、秘密鍵を持っている B さんだけが、自身の秘密鍵で電子メールを復号できますので、エが正解です。

[問 31] 解答 エ

OECD プライバシーガイドラインの 8 原則には「データ内容の原則」があり、データ内容の正確性、完全性、最新性を確保することが定められています。したがって、エが正解です。

アは「収集制限の原則」、イは「公開の原則」、ウは「目的明確化の原則」の説明となります。

[問 32] 解答 ア

個人情報保護法で定義されている個人情報は、生存する個人の情報であって、特定の個人を識別できる情報を含むものです。メールアドレスは、構成する文字列やドメイン名によって特定の個人を識別できる場合は、個人情報となります。したがって、アが正解です。

イ 特定の個人を識別できる情報が含まれていれば個人情報です。

ウ 既に公表されているものでも、個人情報に該当します。

エ 法人の情報は個人情報とはなりません。

[問 33] 解答 ア

“電子計算機損壊等業務妨害”とは、人の業務に使用する電子計算機を損壊するなどの方法によって、電子計算機に使用目的に沿うべき動作をさせず、または使用目的に反する動作をさせて、人の業務を妨害することです。Web ページの改ざんは業務妨害に該当しますので、アが正解です。

イは不正競争防止法（ドメイン名の不正取得）違反、ウは著作権侵害、エは詐欺罪に該当します。

[問 34] 解答 エ

特定電子メール送信適正化法で規制される特定電子メールとは、営業や広告宣伝の手段として送信するメールで、あらかじめ特定電子メールを受信することを許可した人以外へのメール送信は禁じられています。したがって、送信することの許諾を得ていない不特定多数の人に送った広告メールは特定電子メール送信適正化法で禁止されており、迷惑メー

ルに該当しますので、エが正解です。

ア ウイルスに感染していることを知らずに行った場合には罪にはなりません。

イ、ウ 特定の相手に送るメールは特定電子メールとはならないため、特定電子メール送信適正化法では規制されません。

[問 35] 解答 ウ

不正競争防止法によって保護される対象として規定されるものに営業秘密があります。営業秘密とは、秘密として管理されている事業活動に有用な技術上又は営業上の情報であって、公然と知られていないものですので、ウが正解です。

アは特許法で保護される発明、イ、エは著作権法で保護される著作物です。

[問 36] 解答 イ

請負契約とは、請負人が仕事の完成を約束する契約です。この場合は、労働者の作業場所が契約先の事務所であっても、請負人の雇用主は自らの指揮命令の下に労働者を業務に従事させる必要があります。したがって、イが正解です。

ア、エは労働者派遣契約の下で行われる必要があります。また、請負契約、労働者派遣契約のどちらでも、ウのような雇用関係の変更はありません。

[問 37] 解答 イ

スプレッドシートの利用に係るコントロール（統制）に関しては、金融商品取引法で企業に要求される内部統制のうち、スプレッドシート統制として定められています。具体的な基準は、経済産業省が「システム管理基準 追補版(財務報告に係る IT 統制ガイダンス)」として公開しています。

<http://www.meti.go.jp/policy/netsecurity/docs/regulations/ITGovernanceGuideline.pdf>

この基準では、スプレッドシートに対するアクセス制御や検証、変更管理について定義されています。スプレッドシートに組み込まれたロジックを、随時、変更し上書き保存することは、不正が見逃されるリスクにつながるので不適切であり、指摘事項に該当します。したがって、イが正解です。

アの正確性確認やウのアクセスコントロール、エのバックアップは適切な対処ですので、指摘事項には該当しません。

[問 38] 解答 ア

“情報セキュリティ管理基準”の管理策基準「4.3 雇用の終了又は変更」には、「雇用終了以降の一定期間継続する、秘密保持契約及び雇用条件に規定された責任」の記述があります。雇用の終了をもって守秘義務が解消されるわけではありませんので、アは指摘事項に該当します。

イ、ウ、エは情報セキュリティ管理基準に基づいた適切な雇用契約ですので、指摘事項には該当しません。

[問 39] 解答 ア

経済産業省が公表している“情報セキュリティ監査基準 実施基準ガイドライン”の「I. 情報セキュリティ監査実施上の前提事項」には、『「情報セキュリティ管理基準」は、情報資産を保護するため』という記述があります。また、情報資産とは、財務情報、人事情報、顧客情報、技術情報などの目に見えない資産であり、コンピュータ内のデータだけでなく紙や人の記憶なども含まれますので、コンピュータを導入していない部署でも監査を実施する必要があります。したがって、アのように、監査の対象は「情報資産」、コンピュータを導入していない部署における監査実施の要否は「必要」となります。

[問 40] 解答 ア

SLA (Service Level Agreement : サービス品質保証／サービスレベル合意書) とは、サービス提供者が顧客に対して、どの程度の品質を保証するかを示したものです。サービス及びサービス目標を特定した合意事項ですので、アが正解です。

イはサービス料金などの明示事項、ウは内部グループの合意、エは IT サービスの要件に関する内容です。

[問 41] 解答 エ

事業継続計画で用いられる用語のうち、インシデントの発生後、復旧までにかかる時間のことを RTO (Recovery Time Objective : 目標復旧時間) といいます。したがって、エが正解です。

アは平均故障間隔、イは平均復旧時間 (平均修理時間) で、稼働率の計算に用いられます。ウは目標復旧地点 (Recovery Point Objective) で、インシデントで損害・紛失したデータをどの時点まで復旧させる必要があるのかを示す指標です。

[問 42] 解答 ア

過去 5 年間のシステム障害を種類別に積み重ねて棒グラフで示し、年ごとの種類別件数と総件数の推移をまとめて表すためには、積上げ棒グラフを利用するのが適当です。したがって、アが正解となります。

イの二重円グラフは、二つの推移の比較に、ウのポートフォリオ図は全体の割合の確認に、エのレーダチャートは分野ごとの偏りなどを表すのに適しています。

[問 43] 解答 エ

コンピュータシステムに対して指示してから、最初の処理結果が出始めるまでの時間を

レスポンスタイム（エ）、最後を受け取るまでの時間をターンアラウンドタイム（ウ）といいます。したがって、エが正解です。

アのアクセスタイム（アクセス時間）は CPU が記憶装置にデータの書き込みを行うのに必要な時間、イのサイクルタイムは、繰り返し処理で一連のサイクルを実施するのにかかる時間です。

[問 44] 解答 イ

大量のデータを整理・統合して蓄積しておき、意思決定支援などに利用するものをデータウェアハウスといいます。したがって、イが正解です。

アはデータを管理すること、ウはデータの種類や名称などを管理するもの、エは異なるデータ間での関連づけを行うことです。

[問 45] 解答 ア

ルータは、ネットワーク層で中継を行う装置で、LAN 同士、LAN と WAN 間など、様々なネットワークを相互接続します。したがって、アが正解です。

イはリピータ、ウ、エはブリッジ（スイッチングハブ、レイヤ 2 スイッチ）に関する記述です。

[問 46] 解答 エ

社内ネットワークからインターネットへのアクセスを中継するサーバで、Web コンテンツをキャッシュする機能をもつものをプロキシサーバといいます。したがって、エが正解です。

ア 非武装地帯（DeMilitarized Zone）で、ファイアウォールによって内部ネットワークとインターネットの両方から隔離し、外部からの接続を直接受け付けるネットワークです。

イ IP アドレスとポート番号を用いて、IP アドレス変換を行うものです。

ウ ネットワーク上で通過させるべきではない通信を遮断するための装置です。

[問 47] 解答 イ

インターネット経由でサービスプロバイダが提供するアプリケーションの必要な機能（サービス）を利用する仕組みを、SaaS（Software as a Service）といいます。したがって、イが正解です。

ア 統合基幹業務システム（Enterprise Resource Planning）で、企業の資源を統合的に管理するものです。

ウ サプライチェーンマネジメント（Supply Chain Management）で、業界の流れを統合的に見直し、プロセス全体の効率化を図るものです。

エ 拡張可能な事業報告言語（eXtensible Business Reporting Language）で、XML をベ

ースにしたビジネスレポートなどを電子文書化するときに使う規格です。

[問 48] 解答 イ

情報システムを調達するときには、まず発注元はベンダに情報提供を依頼する RFI (Request For Information) を示します (a)。続いて、その情報をもとに、発注元がベンダに提案書を依頼する RFP (Request For Proposal) を示します (b)。その後、RFP などを参考に、供給者の選定を行います (c)。最後に、選定した調達先と、役割や責任分担などを決め、契約の締結を行います (d)。したがって、b に入るものは RFP ですので、イが正解です。

[問 49] 解答 イ

事業継続計画の策定においては、緊急時の資源配分が大切です。そのため、リスクに優先度をつけ、許容できる損失を超えるものから優先的に対処することが必要となります。したがって、イが正解です。

ア、ウのように全てのリスクに対応することや、エのように優先度に差をつけずに検討することは、限られた資源で事業継続を行うという観点から、適切ではありません。

[問 50] 解答 ウ

企業経営の透明性を確保するために、企業活動を監督・監視する仕組みのことをコーポレートガバナンスといいます。したがって、ウが正解です。

ア 企業の活動分野のうち、競合他社を圧倒的に上回るレベルの能力のことです。

イ 企業戦略の一つで、企業文化の特性や独自性を統一されたデザインやメッセージで発信することです。

エ ある変革を実行に移すとき、そのステークホルダ（利害関係者）を洗い出し、対策を考えることです。

[問 1] 標的型攻撃メールの脅威と対策

【解答】

[設問 1] (1) a: キ, b: ク (2) ウ (3) ア, エ (4) カ

[設問 2] (1) カ (2) エ (3) イ (4) ア (5) エ

【解説】

標的型攻撃メールの脅威と対策に関する問題です。インシデントの発生から、対応の問題、課題と対策と、標的型攻撃メール対応の典型的な流れが問題となっています。

[設問 1]

〔受信したメール〕についての問題です。標的型攻撃メールの特徴や、その見分け方などが問われています。

(1)

標的型攻撃メールの特徴を問われています。標的型攻撃メールとは、**特定**の組織や個人を対象として、受信者の PC にマルウェアを送りつけ、情報を搾取することなどを目的とするメールであり、**不特定多数**の組織や個人を対象として送られるウイルスメールとは異なるものです。したがって、空欄 a は**キ**、空欄 b は**ク**が正解です。

(2)

受信者が疑いをもたないように、メールの差出人を公的機関などに詐称したり、メールの件名や内容を受信者の業務に関連したものに偽装したりする手法のことを、**ソーシャルエンジニアリング**といいます。したがって、空欄 c は**ウ**が正解です。

(3)

図 1 の G 君が受信したメールの内容を見ていきます。

まず、件名に「**Re:Re:**」が付加されています。これは、メールを返信するときに付加される文字列なので、**2** 回付加されていることで複数回メールのやり取りを行っていることがわかります。つまり、メールを複数回やり取りすることで、返信するに値する相手であると思わせ、問合せ者に対する疑いを低減しています。また、図 2 の G 君へのヒアリングにも、「製品の問合せが **3** 回あり」とあり、複数回のやり取りが裏付けられます。

次に、メール本文 **6** 行目に「導入する方向で検討を進めております。」とあります。この文面から、取引先になる可能性の高い優良顧客であることを示唆し、G 君に対してきちんと対応することを迫っています。さらに、メール本文下から **2** 行目に「本日 **15** 時までに回

答を」と期限を指定しています。件名に「【至急】」と書かれている点も緊急性を表現し、すぐに添付ファイルを開いて確認しなければならない動機付けになっています。

したがって、ア、エが正解です。

イ Y 社従業員しか知り得ない情報は記載されていません。

ウ 正当な URL を装ったリンクは記載されていません。

(4)

(i)～(iv)の内容を見ていきます。

(i)

差出人のメールアドレスは「F@zz-freemail.co.jp」となっており、Y 社の社内メールアドレスに詐称はされていません。(i)は誤りです。

(ii)

署名のメールアドレスは「F@x-sha.co.jp」であり、差出人のメールアドレスと異なります。

(iii)

拡張子が「.exe」の実行形式ファイルが添付されています。

したがって、(ii)、(iii)が該当し、カが正解です。

[設問 2]

〔情報セキュリティ意識向上に向けて〕について、問題点や適切な対応について問われています。

(1)

今回の初動対応における問題点について問われています。(i)～(iv)の内容を確認し、今回の問題点を挙げていきます。

(i)

図3 管理規程の第2章に「従業員は、各自の判断で復旧対応や解決を試みるのではなく、必ず情報セキュリティリーダーの指示又は勧告に従うこと」とあるので、直ちに復旧対応を行う必要はありません。したがって、(i)は問題点ではありません。

(ii)

図2 G 君へのヒアリング結果の1行目に「X 社は過去に取引がある会社であった。」とあることから、取引記録を確認していることがわかります。したがって、(ii)は誤りです。

(iii)

図3 管理規程の第2章に「インシデントを発見した際には、速やかに情報セキュリティリーダーに報告し」とあります。しかし、G 君へのヒアリング結果によると、図2の下から7

行目に「誰にも相談せず、報告もしなかった。」、下から 4 行目には「報告したくないと思っていた。」とあり、報告しなかったことがわかります。したがって、これは問題点です。

(iv)

図 3 管理規程の第 2 章に「インシデントであるかどうか判断がつかない疑わしい事象も、自己判断せず同様に報告すること」とあります。しかし、G 君へのヒアリング結果によると、図 2 の下から 7 行目に「マルウェア感染はあり得ないだろうと考え」、下から 4 行目に「マルウェア感染と確信できない限りは」とあり、自己判断で疑わしい事象を報告しなかったことがわかります。したがって、これも問題点となります。

以上から、(iii)、(iv)が該当するので、**カ**が正解です。

(2)

図 3 管理規程の第 2 章に「従業員は、インシデントを発見した際には、**速やかに**情報セキュリティリーダーに報告し、その指示に従うこと」とあります。したがって、**エ**が正解です。

(3)

図 3 管理規程の第 2 章に「なお、インシデントであるかどうか**判断がつかない疑わしい事象も**、自己判断せず同様に報告すること。」とあります。したがって、**イ**が正解です。

(4)

規程やルールを策定しただけで順守されないという現状があったため、それを改善し実際に順守させるために行うことについて問われています。(i)～(iv)について、順守させるために有効な対策であるか考えていきます。

(i)

図 2 G 君へのヒアリング結果によると、下から 3 行目に「管理規程については、新入社員研修の際に一度見たことがある程度で、重要な規程とは思っていなかった。」とあります。そのため、重要な規程であるということと、その内容を従業員へ周知させることは重要です。

(ii)

図 2 G 君へのヒアリング結果によると、下から 6 行目に「マルウェア感染が起きたことを上司に報告した際に、上司から大変厳しく叱責されたと H 君本人から聞いていたので、マルウェア感染と確信できない限りは、報告したくないと思っていた。」とあります。このように情報の伝達がされない組織は問題であるので、情報共有や報告が包み隠さず行われるような組織文化の醸成が必要です。

(iii)

情報セキュリティにおけるクラッキング手法などは、情報セキュリティの専門家が、セキュリティ対応を考えるために学ぶものです。一般の従業員に教育すべきものではありません。

(iv)

マルウェア感染時の復旧対応は、情報セキュリティリーダーの指示のもとに行います。そのため、あらかじめ一般の従業員が知っておく必要はなく、また、自己判断を助長することになるため危険でもあります。したがって、適切ではありません。

以上から、適切なものは(i), (ii)となり、アが正解です。

(5)

標的型攻撃メールは、設問 1(2)にあるように「ソーシャルエンジニアリング」を利用しています。そのため、アの標語の掲示や、イの DVD 上映会、ウの事例教育などを行っていたとしても、標的型攻撃メールを業務に関連するメールであると認識してしまう可能性が高く、一人一人が適切に対応できるかは未知数です。また、実際に対応できるかどうかは、これらの対策では測定できません。

実際に攻撃を受けた場合の対応を定量的に測定し評価するためには、模擬の標的型攻撃メールを従業員に送付して対応を確認する方法があります。従業員に向けた標的型攻撃メールを、期間を空けて何回か送付し、その対応を確認します。従業員からのインシデントであると認識した報告の件数、通知時間の測定や、添付ファイルの開封率の変化を調査することで、定量的に評価できるようになります。したがって、エが正解です。

[問 2] 業務委託におけるアクセス制御

【解答】

[設問 1] (1) オ (2) エ (3) a: オ, b: イ (4) ウ (5) エ (6) イ

[設問 2] (1) エ (2) d: ア, e: ウ, f: ア (3) ウ (4) ア

【解説】

業務委託におけるアクセス制御に関する問題です。アクセス権限やロールに対して、複雑な事象を丁寧に読み解く必要があります。他の問と比較して難易度が高めの問題です。

[設問 1]

〔受注管理業務の委託〕についての問題です。業務の入力作業を B 社に追加で委託するにあたって、新しい操作権限案（表 2）を考え、それについて検討していきます。

(1)

本文中の下線①の「J システムで利用方針に違反」について、承認権限を追加することで違反してしまう利用方針を考えます。〔J システム及び T システムの操作権限〕の 4 つの方針について、表 2 の操作権限で違反が起こるかどうかを考えます。

〔方針 1〕〔方針 2〕については、今回の変更はロールとロールに付与される操作権限のみですので、利用者 ID の付与には影響はありません。したがって、特に違反とはなりません。

〔方針 3〕については、J システムでは今までは A 社販売担当者が入力、A 社販売責任者が承認というように権限が分かれていたので、ある利用者が入力した情報は、別の利用者が承認するという利用方針は満たされていました。しかし、A 社販売担当者ロールに承認権限を追加すると、A 社販売担当者が入力と承認の両方を行うことができることになり、利用方針に違反します。

〔方針 4〕については、A 社販売責任者に対しての権限には変更はなく、問題ありません。

したがって、違反が考えられる利用方針は〔方針 3〕のみとなり、**オ**が正解です。

(2)

〔方針 3〕の利用方針違反が高めるリスクについて問われています。A 社販売担当者が入力と承認の両方を行うことができるようになると、一人で注文を入力し、承認を行うことが可能となってしまいます。すると、不正に入力された注文をチェックする人がいなくなり、承認されてしまうことがありえます。したがって、**エ**が正解です。

アの承認されないことや、ウの差し戻されることで滞留が発生するのは、方針 3 の利用方針違反とは関係ありません。また、注文情報の窃取は、閲覧権限があればできることで、承認権限とは関係ありません。

(3)

空欄 a, b の穴埋め問題です。文章の流れに沿って、選択肢から 2 つの案を選び出していきます。

空欄 a, b では、“A 社販売担当者”ロールに承認権限を追加した上で、利用方針にも合致するものを考えます。空欄 a の条件は「要求 2」を満たさないものであり、これも満たすのが空欄 b です。

利用方針「方針 3」の入力と承認の利用者を分けるための方法としては、オの「他の利用者 ID によって入力された注文だけを承認できる権限」を追加する方法が有効です。しかし、この方法だと、A 社の販売担当者同士でも別人なら承認が可能となり、「要求 2」の A 社の担当者が入力した場合の要件を満たしません。

また、“A 社販売担当者”ロールで承認できる注文を、「B 社 J システム担当者”ロール又は“B 社管理者”ロールを使って入力された注文だけ」に限ると、「方針 3」の入力と承認が別の利用者という条件を満たせると同時に、「要求 2」の A 社販売担当者の入力は A 社販売責任者のみの承認という要件を満たせます。

したがって、空欄 a がオ、空欄 b がイとなります。

(4)

空欄 a のオの方法では「要求 2」を満たせない理由が問われています。(3)で説明したとおり、他の利用者 ID によって入力された注文だけを承認できるという制限だけでは、“A 社販売担当者”ロールの利用者が複数人いるときに、2 人で協力して入力し承認することが可能となります。つまり、1 人が入力し、別の 1 人が承認することができるため、「要求 2」の A 社販売責任者の承認が必要なくなります。したがって、ウが正解です。

ア,エのような、B 社に関する権限に関しては問題ありません。イの承認依頼については、権限の話とは関係ありません。

(5)

下線③の「来年度から毎年 2, 3 回, 2 週間ほどの海外出張に出る予定なので、誰かに代行してもらう必要が出てくる」場合に代行者をどうするかを考えます。

利用方針の「方針 3」より、入力と承認は別の人が行う必要がありますが、アのように、“A 社販売責任者”ロールを A 社の担当者に割り当ててしまうと、この方針が満たせなくなります。

同様に、イでも A 社の担当者に入力と承認の両方が割り当てられますので、「方針 3」が満たせません。

ウについては、N 課長の利用者 ID やパスワードを別の人が運用することは、「方針 2」の、一つの利用者 ID を 1 人の利用者だけが利用する方針に違反します。

エのように、N 課長の上長なら A 社販売担当者ではありませんので、入力と承認の権限が重なることはありません。そのため、上長の利用者 ID に“A 社販売責任者ロール”を設定して代行を行うことに問題はあります。

したがって、利用方針に合致するものはエとなります。

(6)

本文中の下線④での、B 社の担当者の一部が応援できるように、必要な操作権限を与える方法を考えます。B 社 T システム担当者は、通常は T システムを担当していますが、問合せ数が少ない時間帯に、応援として J システムの利用も行うことになりました。そのためには、B 社応援担当者について新しいロールを定義し、そのロールは“B 社 T システム担当者”と“B 社 J システム担当者”の両方の権限を併せ持つ必要があります。したがって、イの新しいロールの定義が正解となります。

ア、エのような都度切り替えて行う運用については、[J システム及び T システムの操作権限]に、利用者 ID に対するロール設定は「翌営業日の朝 5 時に自動的にシステムに反映」とあり、必要に応じた即時の対応はできないので誤りです。ウの“B 社管理者”のロールでは T システムへの入力ができなくなり、業務に支障が出ます。

[設問 2]

〔B 社担当者の追加及び変更〕についての問題です。B 社担当者の追加や変更を行う場合に必要な手続きや運用について問われています。

(1)

空欄 c の穴埋め問題です。利用部署が、業務委託先要員への閲覧権限付与を希望する場合の申請方法について問われています。〔B 社担当者の追加及び変更〕(3)に、「利用部署の希望によって閲覧権限を付与する場合は、利用部署の長が、その情報のオーナー部署の長に申請して承認を得る」とあります。また、業務委託先要員の監督責任は利用部署にありますので、業務委託先の管理者から利用者の情報を入手し、確認する必要があります。そのため、利用部署が、業務委託先要員への閲覧権限付与を希望する場合は、利用部署の長が、業務委託先の管理者から提出された利用者の情報に基づいて、情報のオーナー部署の長に申請する必要があります。したがって、エが正解です。

アのように、業務委託先と情報のオーナー部署が直接やりとりすることはありません。また、業務を依頼するのは利用部署ですので、イやウのように、業務委託先から申請を行うこともありません。

(2)

空欄 d～f の穴埋め問題です。

空欄 d

D システムの閲覧権限を見直して、必要最小限にすることは、B 社 J システム担当者からの情報漏えいを防ぐことになり、これは内部不正のリスクを低減することに当たります。したがって空欄 d は、アの内部不正となります。

空欄 e

閲覧権限の付与に関しては、[B 社担当者の追加及び変更] (4)の空欄 c より、利用部署の長が情報のオーナー部署の長に申請する必要があります。つまり、利用部署の長である N 課長が行うことは、情報のオーナー部署の長に対しての申請です。したがって空欄 e は、ウの情報のオーナー部署の長となります。

空欄 f

B 社の担当者変更に関しては、[B 社担当者の追加及び変更] (4)の空欄 c より、利用者の情報を業務委託先の管理者から受け取る必要があります。業務委託先は B 社ですので、情報提供は B 社の管理者が行います。したがって空欄 f は、アの B 社の管理者となります。

(3)

本文中の下線⑤の「来月中に 1 人が退任し 1 人が新規に着任する」ことに対応するために必要な利用者 ID 管理の手続を考えます。[J システム及び T システムの操作権限] の利用方針のうち [方針 1] [方針 2] を満たすためには、退任者と新任者それぞれに利用者 ID が必要となります。また、引き継ぎ期間は同時に T システムと D システムを利用しますので、この業務に支障が出ないように、なおかつ必要最小限の権限となるようにすることも必要です。そのため、引き継ぎ開始に当たり、新任者の利用者 ID を発行し、引き継ぎ期間後、直ちに退任者の利用者 ID を無効化することが有効です。したがって、ウが正解となります。

ア 退任者の利用者 ID は、必要がなくなったら直ちに無効化する必要があります。

イ 利用者 ID の引き継ぎは、利用方針 [方針 2] に反します。

エ 引継ぎ開始時に退任予定者の利用者 ID を無効化すると、引継ぎ業務に支障が出てしまいます。

(4)

本文中の下線⑥について、担当者変更のために受領する情報としては不要なものを考えます。(3)の利用者 ID 管理の手続を行うためには、無効化する退任者の利用者 ID と、新任者の着任予定日、退任者の退任予定日は必要となります。しかし、新任者の閲覧希望情報については、閲覧する情報は業務を引き継ぐだけなので退任者と変わらず、またどの情報

を閲覧させるのかを決めるのは利用部署の長（今回は N 課長）ですので，申請を受け取る必要はありません。したがって不要なものは，**ア**の新任者の閲覧希望情報となります。

[問 3] 情報セキュリティ自己点検

【解答】

[設問 1] イ

[設問 2] イ, オ

[設問 3] (1) イ (2) エ (3) ア (4) イ (5) イ

[設問 4] (1) カ (2) ア

【解説】

情報セキュリティ自己点検に関する問題です。海外営業部において、監査部が CSA (Control Self Assessment : 統制自己評価) 方式による情報セキュリティ監査を実施します。標的型攻撃メールや ISMS などについての基礎知識と、問題文の正確な理解が必要な問題です。

[設問 1]

本文中の下線①の「結果が正しいか客観的に判断できないチェック項目」について問われています。表 2 のチェック項目の No.11「不審な電子メールの添付ファイル」については、「不審」かどうかは本人の判断によります。標的型攻撃メールの場合には、不審だと判断されないようなメールを巧妙に送ってきます。したがって、客観的に判断できないチェック項目は、イの 11 となります。

No.10 のパスワードを書いていないことや、No.12 の連絡先を知っていること、No.13 の施錠保管しているというチェック項目は、実際に知っているか行っているかどうかだけです。客観的な判断が可能です。

[設問 2]

本文中の下線②「監査部が各部門を直接監査する方式と CSA 方式の利点、欠点を比較評価」について、CSA 方式の利点を問われています。CSA 方式は、自己評価を行う方式ですので、業務を行っている本人が評価します。そのため、イのとおり、業務内容は十分理解しており、その理解に基づいて評価することができます。また、評価を自分たちで行うことで、何をすべきなのかを学習することができます。そのため、オのとおり、評価実施者に対する意識付けや教育として役立ちます。したがって、イ, オが正解です。

アの準拠性の担保やエの独立的な立場については、監査部が各部門を直接評価する方式の利点です。ウの証跡については、どちらの場合でも監査には必要となります。

[設問 3]

〔CSA の実施〕についての問題です。表 3 の CSA シートについて空欄 a~d の穴埋めを行い、改善計画を考えます。R 社海外営業部の現状を正確に読みとることがポイントです。

(1)

表 3 中の空欄 a, No.4 の評価項目に対する穴埋め問題です。全員が教育を受けているかどうかについては、本文中に「R 社では、情報セキュリティ推進部が実施する情報セキュリティ教育があり、海外営業部では、新たに配属された部員だけが受講することになっている。」とあります。そのため、配属時の教育の後に発見された新たなセキュリティ脅威については、情報セキュリティ教育を受けていないことになります。したがって評価は“NG”で、評価根拠は“新たなセキュリティ脅威に関する教育を受けていない部員がいる”となり、イが正解です。

(2)

表 3 中の空欄 b, No.11 の評価項目に対する穴埋め問題です。リモート接続のためのパスワードの変更については、本文中に「貸与 PC のうち、ノート PC だけが、リモート接続サービスによる社内ネットワークへの接続を許可されている」とあり、また「海外営業部の部員は、出張がなく、全員がデスクトップ PC だけを使っている」とあります。そのため、リモート接続サービスの接続が許可されている PC はないことになります。したがって評価は“NA”で、評価根拠は“部内ではリモート接続は誰も行わない”となり、エが正解です。

(3)

表 3 中の空欄 c, No.19 の評価項目に対する穴埋め問題です。ファイルサーバ上の顧客情報のアクセス権が最小権限の原則に基づいて設定されているかどうかについては、表 1 の簡易チェックリスト No.1 に「業務上の必要がある人だけにアクセス権を付与している。」とあり、最小権限で設定されているかどうかを簡易チェックしています。そのため、自己判断で全部員に確認していることになります。したがって評価は“OK”で、評価根拠は“簡易チェックで、アクセス権の付与状況について確認している”となり、アが正解です。

(4)

表 3 中の空欄 d, No.26 の評価項目を答える穴埋め問題です。No.26 の評価根拠には、「部外者が従業員に気付かれずに入ることは難しい」、「出入口を施錠」とあるので、入退室に関することであることがわかります。また、評価結果が“(OK)”であることから、この入退室管理の方法が代替コントロールであることがわかります。そのため、本来行うべき情報セキュリティ対策としては、入退室管理システムなどで厳密に入退室管理を行うような方法であることが考えられます。したがって、評価項目は“入退室管理システムが導入され、関係者だけ入室可能になっている”となり、イが正解です。

(5)

本文中の下線③「改善計画を策定」について、その概要が問われています。改善が必要な内容としては、〔CSAの実施〕に「棚卸の際に不要と判断された利用者IDが5個あること」で、「棚卸の1か月以上前から、部員の退職又は異動で不要になっていた」とあります。つまり、退職又は異動の際に速やかに利用者IDが削除されていないことが問題であり、それを改善するには、システムからの削除を速やかに行う対策が必要です。したがって正解は、イの「部員の退職又は異動の際は、利用者IDの削除申請とCシステムからの削除を速やかに行うよう、管理職一人一人に周知する」となります。

[設問 4]

〔新たな指摘についての改善計画〕についての問題です。最小権限の原則を守り、社外への顧客情報の漏えいを防止できるようにするための対策を考えていきます。

(1)

本文中の空欄 e1～e3 に入る対策を考えていきます。

空欄 e1 は、新たな指摘に対応するための対策で、全部員に担当顧客を確認してから行う根本対策となります。Cシステムにおいて、最小権限の原則を守らせるためには、システムで制御することが最も効果的です。具体的には、〔対策 3〕の「担当する顧客の顧客情報だけにアクセスできるようにアクセス権を設定するという対策」が有効です。したがって、空欄 e1 は〔対策 3〕となります。

空欄 e2 は、暫定的な対策で、e1 の対策を行うために必要な2週間のリスクを低減するための対策となります。最小権限の原則を守らせるためにシステム以外で制御するには、規則を周知徹底させて運用的に行う方法があります。具体的には、〔対策 2〕の「営業部員に対し、担当顧客以外の顧客情報を閲覧しないように周知し、牽制するという対策」が有効です。したがって、空欄 e2 は〔対策 2〕となります。

空欄 e3 は、万が一顧客情報の漏えいが発生してしまったときのための対策となります。顧客情報の漏えいが発生した場合には、アクセスログなどをもとに、その漏えい元を特定することが肝心です。しかし、本文中に「Cシステムでは、アクセスログを3か月分保存している」とあり、3か月より前に発生した情報漏えいについては追跡できないことになります。そのため、〔対策 1〕の「アクセスログの保管期間を3年間に変更する」ことが有効です。したがって、空欄 e3 は〔対策 3〕となります。

これらの組合せで、正解は**カ**となります。

(2)

本文中の空欄 f1～f3 に対する対策を考えていきます。

空欄 f1 は、顧客情報の追加・修正・削除の権限についての対策で、厳密ですが業務が回

らない対策となります。部員が顧客情報を不適切に変更しないようにするには、管理職だけが追加・修正・削除を行うことが最も確実ですが、業務は非効率となります。具体的には、[対策 4] の「顧客情報の追加・修正・削除の権限は管理職だけに付与するという対策」が該当します。したがって、空欄 f1 は [対策 4] となります。

空欄 f2 は、f1 よりも効率的な対策ですが、ベンダに開発をお願いして半年掛かる対策です。顧客情報を追加・修正・削除したとき、それが不適切でないことを確認するには、上長が承認を行うことが確実です。具体的には、[対策 5] の「部員による顧客情報の追加・修正・削除は、システムのワークフロー機能を使って上長が承認することによって、データベースに反映されるようにするという対策」が有効です。したがって、空欄 f2 は [対策 5] となります。

空欄 f3 は、f2 の対策が有効になるまでの暫定的な対策となります。上長の承認がシステムのワークフロー機能で行えない場合には、それを手動で行う必要があります。具体的には、[対策 6] の「顧客情報の追加・修正・削除のログを上長が定期的に確認するという対策」が有効です。したがって、空欄 f3 は [対策 6] となります。

これらの組合せで、正解は **ア** となります。

徹底攻略 情報セキュリティマネジメント教科書【購入者限定特典】 平成28年度春期試験解説（ダウンロード版）

著 者 株式会社わくわくスタディワールド 瀬戸美月／齋藤健一

発行人 土田米一

編集人 高橋隆志

発行所 株式会社インプレス
〒101-0051 東京都千代田区神田神保町一丁目105番地
TEL 03-6837-4635（出版営業統括部）
ホームページ <http://book.impress.co.jp/>

本書は著作権法上の保護を受けています。本書の一部あるいは全部について（ソフトウェア及びプログラムを含む）、株式会社インプレスから文書による許諾を得ずに、いかなる方法においても無断で複写、複製することは禁じられています。

Copyright © 2016 Mizuki Seto/Kenichi Saito. All rights reserved.