ラクパス

情報セキュリティマネジメント試験合格講座

- 情報セキュリティマネジメント試験　平成 28 年度　秋期　過去問題
  上記のリンクから、問題冊子、解答例、採点講評を入手できます。

- 情報セキュリティマネジメント試験　平成 28 年度　秋期　過去問題　解答・解説

平成 28 年度　秋期　午前問題の解説

〔問 01〕エ
PIN（Personal Identification Number）は、個人が持つ会員番号などに対する暗証番号なので、本人以外には知られないようにする必要があります。

〔問 02〕イ
保険に加入するという対応は、他者である保険会社とリスクを共有することになります。保険に入ったからといって、リスクが除去されたり増加したり、回避できるわけではありません。

〔問 03〕ウ
JPCERT/CC は、特定の政府機関や企業から独立した組織であり、国内のコンピュータセキュリティインシデントに関する報告の受付、対応の支援、発生状況の把握、手口の分析、再発防止策の検討や助言を行っています。

〔問 04〕ウ
JVN は、JPCERT/CC と IPA（情報処理推進機構）が共同運営する脆弱性対策情報ポータルサイトです。日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュリティ対策に資することを目的としています。

〔問 05〕ア
可用性（Availability）は、故障などで停止せずに、必要なときにアクセスおよび使用ができる特性と定義されています。ストレージ（記憶装置）を二重化し、耐障害性を向上させることは、可用性の向上に繋がります。本人確認、暗号化、不正アクセスの防止は、可用性ではなく、機密性を向上させます。

〔問 06〕ア
ベースラインアプローチは、既存の標準や基準をもとに自組織の対策基準であるベースラインを策定してチェックしていくリスク分析の方法です。比較的、簡単に実施できますがが、選択する標準や基準によっては求める対策のレベルが高すぎたり、低すぎたりする場合があります。

〔問 07〕ウ
資料Aによって利用者IDと利用者を突き合わせて、資料Bで組織の現在の所属者の名簿に載っているか否かを調べれば、退職者に発行されていた利用者 ID を発見できます。

〔問 08〕イ
リスク評価(Risk Evaluation)は、リスクが、受容可能か許容可能かを決定するために、リスクの特質を理解し、リスクレベルを決定するプロセスリスク分析の結果をリスク基準と比較するプロセスです。リスク評価は、対策を講じることによって、リスクを修正するプロセスであるリスク対応に関する意思決定を手助けします。

〔問 09〕エ
残留リスク(Residual Risk)は、リスクを修正するプロセスであるリスク対応(Risk Treatment)の後に残るリスクです。

〔問 10〕エ
JIS Q 27002:2014 では、組織の全ての従業員、および関係する場合には契約相手は、職務に関連する組織の方針および手順についての、適切な、意識向上のための教育および訓練を受け、また、定めに従ってその更新を受けることが望ましいとされています。

〔問 11〕エ
組織における内部不正防止ガイドラインでは、内部不正防止の観点から「他の役職員が不在で相互監視ができない環境における単独作業を制限することが望ましい」とされています。

〔問 12〕エ
C&C（Command and Control）サーバは、侵入して乗っ取ったコンピュータに対して、他のコンピュータへの攻撃などの不正な操作をするよう、外部から命令を出したり応答を受け取ったりする役割を持っています。

〔問 13〕エ
MDM（Mobile Device Management）は、会社や団体が、自組織の従業員に貸与するスマートフォンに対して、セキュリティポリシに従った一元的な設定をしたり、業務アプリケーションを配信したりすることで、スマートフォンの利用状況などを一元管理する携帯端末管理の仕組みです。

〔問 14〕
rootkit は、サーバにバックドアを作り、サーバ内で侵入の痕跡を隠蔽するなどの機能をもつ不正なプログラムやツールのパッケージです。TKIP（Temporal Key Integrity Protocol）は、暗号解読へのセキュリティを強化した無線 LAN のデータ暗号化プロトコルです。

〔問 15〕イ
SIEM は、様々なシステムの動作ログを一元的に蓄積、管理し、セキュリティ上の脅威となる事象をいち早く検知、分析する仕組みです。ネットワークへの侵入を試みるパケットを検知し通知する侵入検知システムは、IDS（Intrusion Detection System）です。

〔問 16〕エ
SPF は、電子メールの送信者偽称を防ぐ送信ドメイン認証技術です。内部ネットワークへの不正侵入を検知するのは IDS（Intrusion Detection System）です。

〔問 17〕イ
HTTP over TLS（HTTPS）は、暗号化通信機能の加えた Web サーバで利用されるプロトコルです。Web ブラウザから Web メールのサーバまでの通信は暗号化されますが、その後のサーバ間の通信が暗号化されない場合もあるので、ファイルを暗号化してメールに添付するのが適切です。

〔問 18〕エ
ビヘイビア法は振る舞い(Behavior)を判断する検知方法です。ウイルスに感染していないことを保証する情報と検査対象から算出した情報を比較する方法はチェックサム、原本と検査対象を比較するのはコンペアと呼ばれる方法です。

〔問 19〕イ
NTP(Network Time Protocol)は、TCP/IP 環境において、タイムサーバの時刻を基に複数のコンピュータの時刻を同期させるプロトコルです。FTP(File Transfer Protocol)はファイルの転送、SMTP(Simple Mail Transfer Protocol)はメールの転送、SNMP(Simple Network Management Protocol)は機器の監視です。

〔問 20〕ア
CAPTCHA は、人間には読み取ることが可能でも、プログラムでは読み取ることが難しいという差異を利用して、ゆがめたり一部を隠したりした画像から文字を判読して入力させることによって、プログラムによる自動入力を排除するための技術です。

〔問 21〕ア
完全性(Integrity)正確さおよび完全さの特性です。Web ページを改ざんされると、正確さおよび完全さが損なわれます。

〔問 22〕ア
クロスサイトスクリプティングは、攻撃者が用意したスクリプトを、閲覧者の Web ブラウザを介して脆弱な Web サイトに送り込み、閲覧者の Web ブラウザ上でスクリプトを実行させる攻撃手法です。

〔問 23〕ア
サイバーセキュリティ戦略の五つの基本原則は、(1)情報の自由な流通の確保、(2)法の支配、(3)開放性、(4)自立性、(5)多様な主体の連携です。「サイバー空間が一部の主体に占有されることがあってはならず、常に参加を求める者に開かれたものでなければならない」のは開放性に含まれます。

〔問 24〕イ
スクリプトキディ(Script Kiddy)は、自分ではプログラミングをせずに、他人の製作したスクリプト(簡易なプログラム)を使って攻撃しようとする者のことです。

〔問 25〕ア
緊急事態を装って組織内部の人間からパスワードや機密情報を入手する不正な行為は、ソーシャルエンジニアリングに分類されます。

〔問 26〕ウ
パスワードリスト攻撃は、どこかの Web サイトから流出した利用者 ID とパスワードのリストを用いて、他の Web サイトに対してログインを試行する攻撃手法です。想定され得るパスワードとそのハッシュ値との対のリストを用いて、入手したハッシュ値からパスワードを効率的に解析しようとするのは、レインボーテーブル攻撃と呼ばれています。

〔問 27〕エ
ランサムウェア（Ransom Ware）は、感染した PC のファイルを暗号化し、ファイルの復号と引換えに金銭を要求するマルウェアです。Ransom は「身代金」という意味です。

〔問 28〕ウ
ディジタル署名の署名者のメールアドレスのドメインが EC サイトのものであり、署名者のディジタル証明書の発行元が信頼できる組織のものであることが確認できれば、なりすましメールでなく、EC サイトから届いたものであると判断できます。

〔問 29〕ウ
PKI（Public Key Infrastructure、公開鍵基盤）の認証局（Certification Authority）は、失効したディジタル証明書の一覧である CRL（Certificate Revocation List）を更新しています。

〔問 30〕ウ
コモンクライテリア（CC、Common Criteria）は、情報技術セキュリティの観点から、情報技術に関連した製品およびシステムが適切に設計され、その設計が正しく実装されていることを評価するための国際標準規格で、1999 年に ISO/IEC 15408 として制定されました。

〔問 31〕エ
プロバイダ責任制限法では、他人の権利が侵害されていることを知らなかったり、知ることができなかったりした場合は、プロバイダに損害賠償責任はないと規定されています。

〔問 32〕ウ
預金残高や送金データを操作するなど、銀行のシステムに虚偽の情報を与え、不正な振込や送金をさせる行為は、刑法の電子計算機使用詐欺罪が適用されます。

〔問 33〕ウ
個人番号を源泉徴収票などの法定調書に記載して行政機関等に提出することは、個人番号を利用できる事務に該当します。

〔問 34〕ウ
取引関係にあるなどの一定の場合を除き、あらかじめ送信に同意した者だけに対して送信するオプトイン方式をとることは、特定電子メール法に違反していません。

〔問 35〕エ
不正アクセス禁止法は、実際には不正アクセスを行っていないとしても、不正アクセスを行う目的で他人の利用者 ID、パスワードを取得したり保管したりする行為そのものを禁じています。

〔問 36〕ウ
準委任契約は、当事者の一方が、特定の行為をすることを委託する契約です。請負契約のように目的物を完成させる義務は負いませんが、報告義務や善良な管理者としての注意が求められる善管注意義務を負って作業を受託することになります。

〔問 37〕エ
ISMS（Information Security Management System、情報セキュリティ管理システム）の運用では、監査プログラムは関連するプロセスの重要性および前回までの監査の結果を考慮に入れなければなりません。

〔問 38〕ウ
ディジタルフォレンジックス（Digital Forensics）は、インシデントの調査やシステム監査にも利用できる、証拠を収集し保全する技法です。コンティンジェンシープラン（Contingency Plan）は緊急時対応計画です。

〔問 39〕ア
事業継続計画（BCP、Business Continuity Plan）は、災害やシステム障害など予期せぬ事態が発生した場合でも、重要な業務の継続を可能とするために事前に策定される行動計画です。緊急連絡先リストを常に最新版に更新しているのは適切な状況です。

〔問 40〕ウ
情報セキュリティ監査の判断の尺度には、原則として「情報セキュリティ管理基準」を用いるのは適切な判断です。監査人には独立性が求められ、他の専門家の支援を受けることが適切な場合もあります。

〔問 41〕ア
確実性や効率性の観点で、既存システムから新システムへの切替え手順や切替えに伴う問題点を確認することは、システムの移行テストを実施する主要な目的のひとつです。

〔問 42〕ウ
インシデントは、サービスに対する計画外の中断、サービスの品質の低下、または顧客へのサービスにまだ影響していない事象のことです。プログラムの異常終了は、インシデントに該当します。

〔問 43〕ア
磁気テープへのフルバックアップに加え、毎日、磁気テープへの差分バックアップを行うことは、前日の状態までには復旧できるようにする適切な対応策になります。この他の選択肢の手段では、前日の状態までは復旧できない場合があります。

〔問 44〕イ
ステークホルダ（Stakeholder）は、「意思決定若しくは活動に影響を与え、影響されることがある、または影響されると認知しているあらゆる人または組織のこと」と定義されています。ステークホルダは個人とは限らず、会社や学校のような組織の場合もあります。影響には、自らの利益になる場合と不利益になる場合があります。

〔問 45〕ア
クライアントサーバシステムにおいて、Web ブラウザによってクライアント処理を行えば、専用のアプリケーションを用意する必要がなく、クライアント環境の保守の軽減になります。

〔問 46〕イ
E－R 図は、対象とする世界を実体と関連の二つの概念で表現する図です。管理の対象を実体であるエンティティ（Entity）およびエンティティ間の関連を表現できるリレーションシップ（Relationship）として表します。

〔問 47〕ウ
DHCP（Dynamic Host Configuration Protocol）は、TCP/IP 環境でネットワークを構築するとき、クライアント数が多くなると IP アドレスの管理が煩雑となる。クライアントからの要求によって動的に IP アドレスを割り当てることで、IP アドレスの管理が効率化できるプロトコルです。動的に IP アドレスを割り当てるので、あらかじめ DHCP サーバのアドレスを設定しておく必要はありません。

〔問 48〕イ
BPO（Business Process Outsourcing）は、自社の管理部門やコールセンタなど特定部門の業務プロセス全般を、業務システムの運用などと一体として外部の専門業者に委託することです。

〔問 49〕ウ
経営や事業の目的、目標を達成するために必要なシステムに関係する経営上のニーズ、システム化またはシステム改善を必要とする業務上の課題などは、共通フレームにおける企画プロセスで明確にしておくべき事項です。

〔問 50〕イ
マトリックス組織は、二人以上の上司から指揮命令を受け、プロジェクトの目的別管理と職能部門の職能的責任との調和を図ろうとする組織構造です。業務遂行に必要な機能と利益責任を部門ごとにもつのは事業部制組織、機能分化された部門をもつのは職能別組織、期間と目標を定めて活動するのはプロジェクト組織です。

平成 28 年度 秋期 午後問題の解説

問 1

〔設問 1〕
(1) a オ
(2)オ

公開されていた秘密情報のファイルは、Q 社従業員がインターネット検索を行っていたときに発見されているので、誰でも閲覧できる状態であったことになります。誰でも閲覧可能ということは X サービスの設定で、ファイル共有先としてインターネット上に公開される「パブリック」に指定されていて、かつ、共有権限に利用者のアカウントがなくてもインターネットからのファイル閲覧ができる「閲覧権限」が付与されていたことになります。

情報セキュリティ責任者である T 部長が、直ちに X サービスに登録している全てのファイルを削除し、X サービスの利用を中止するように指示した理由は、この時点では、なぜ公開される設定になっていたのかが不明だったからです。選択肢の中では「ファイルが公開された原因が不明であり、J 社が X サービスに登録している他のファイルや、今後登録するファイルにも被害が及ぶおそれがあったから」です。

「原因は不明だが、X サービスに登録されている全てのファイルが公開されたことが明らかであり、J 社としても早急に被害の拡大を防止する必要があったから」は、「全てのファイルが公開された」という部分が誤りです。

〔設問 2〕 キ

プロキシサーバは、内部ネットワークのクライアントが外部サーバと通信する場合、中継役となりクライアントの代わりに外部サーバに接続する機能を持ちます。プロキシサーバを調査した理由は、自社から外部の X サーバへの接続を調査するためなので、選択肢では「製造部の PC 以外の J 社 PC の中に、X サービスに接続したものがあるかを確認するため」です。

〔設問 3〕(1) b エ
(2)ケ

X サービスのファイル共有設定を間違える理由となるのは、「ファイルの共有設定に関係する用語の意味を正しくは理解していない従業員が」いることです。S 主任が、利用方法についての十分な教育と間違った共有設定がなされても第三者にファイルを読まれる可能性を下げる対策の必要性を反省していることからも明らかです。

万一間違った共有設定がなされても第三者にファイルを読まれる可能性を下げるには、アクセスされても内容を読めないように暗号化しておくことや、必要のないときにはファイルを共有の状態にしないことが考えられます。

選択肢の対策では、「登録するファイルを暗号化する」と「ファイル登録後、B 社だけに連絡し、B 社のダウンロードが完了次第直ちに削除する」が該当します。電子署名やハッシュ値の利用では、改ざんの発見にはつながりますが、第三者にファイルを読まれる可能性を下げる対策にはなりません。

〔設問 4〕
(1) c イ
d オ
(2) e・ f イ・エ(順不同)
(3) ウ
(4) キ

表 2 の「X サービスを業務で利用することの問題点とその理由」を整理すると、事故が発生した原因を後から調べることができないのは、操作の履歴情報が提供されていないからです。

従業員が自由にファイル共有を設定できる状態は、ファイル共有設定を間違える「誤操作」や、故意に情報を流出させようとする「意図的な公開」を防げません。メールアドレスとパスワードだけで利用できる状態では、誰でも利用できることになり、なりすましのリスクがあり、2 要素認証にもなっていません。

現在の X サービス利用規則の内容では、事故発生時の原因特定が困難とされる理由は「図 1 X サービス利用規則」によって、J 社製造部が X サービスを利用するメールアドレスを共有することになっているからです。

情報セキュリティ委員会が行うべき組織的対策は、「社外の IT サービスの導入について、全て情報セキュリティ委員会の承認を必要とすることを情報セキュリティ関連規程に定める」ことと「情報システムの利用アカウントの共有を禁止する旨を情報セキュリティ関連規程に定める」です。

情報システム課が行うべき技術的対策は、「新たに選定する法人向けのオンラインストレージサービスに登録する全てのファイルを、定期的にバックアップする」ことです。ファイル共有設定のミスと秘密保持契約は関係なく、Web サイトの閲覧を制限は現状でも行っています。共有のメールアドレスを変更したり、に電子署名を付与しても状況は変わりません。

問 2

〔設問 1〕 a ア
b エ
c イ
d エ

インシデント発生とその初動対応の経緯を示した図 2 によると、K 課長は、関係者を招集して状況説明を行っています。空欄 a に入る選択肢のうち初動対応として情報機器に保存されていた情報の内容および量を確認しているのは「F さんが紛失した情報の内容および量の特定」だけです。空欄 b は、初動対応の規定にある「情報セキュリティ対策の実施状況を確認」に該当する選択肢の「情報セキュリティ対策の実施状況の確認」が入ります。

図 2 の初動対応で W 主任が「上記で特定したシステムにおいて F さんのアクセス権の無効化」を行った記述があるので、紛失した NPC に情報システムのアカウント情報が含まれていたことがわかります。W 主任は「F さんが外出先からアクセスできる」システムを特定し、「社外から不審なアクセスがないかどうかの幅広い確認」をする必要があります。

〔設問 2〕
(1) ア
(2) ク
(3) e イ

(4) f イ
(5) g イ

持出しの承認の後でも、NPC に顧客情報を追加で保存する方法は、(1)1 か月間の NPC 期間持出しの承認を得るとその期間中に NPC を会社に持ち帰ったときに追加で保存する、(2)
NPC の持出しとは別に会社貸与の USB メモリに保存して持ち出して NPC に保存する、(3)外出先から L システムにアクセスして NPC にダウンロードして保存するという 3 つの方法が可能です。顧客情報は別のシステムであり、Z 社が貸与する USB メモリしか接続できないので、顧客から借りた USB メモリからコピーはできないはずです。

NPC 紛失時に NPC の中の情報を盗まれるリスクを低減する手順を表 1 で探すと、NPC のための情報セキュリティ対策で挙がっているルール(h)にあるハードディスク全体の暗号化が該当します。

秘密鍵の漏えいの有無を調査するためには「アクセスを試みた形跡」が L システムの「本日 00:00 から 15:30」のログ中にないか確認します。F さんがまた L システムにアクセスできる状態にするためには、F さんの従来のクライアント証明書を失効させてから、新しい鍵ペアを生成しクライアント証明書を発行し直した後で、アクセス権を有効にします。

一時的にでも自社の管理を離れたことによって情報が盗まれたり、マルウェアが入れられたりした可能性があるので、証拠保全をした上で調査し、F さんには今の NPC を使い続けるのではなく、新しい NPC を手配することになります。ハードディスクを複製してもマルウェア対策にはならず、データ消去や初期化、破壊をすると調査ができないので誤りです。

問 3

〔設問 1〕
(1) イ
(2) a ア
(3) カ

情報セキュリティインシデントの発生時には、第一に被害拡大の防止、第二に証拠保全に努めなければならないと「利用規定」に記されているので、これを踏まえて選択肢を検討します。

「電源を強制切断」と「再起動」は証拠保全ができないので誤りです。対策をする以前に、すぐに「ログインパスワードを変更」することは新たなパスワードの漏えいに繋がる可能性があり、初動対応としては適切ではありません。

B 課長が E さんに指示すべき初動対応は、被害を拡大させないように敢えて「E-PC の HDD 内のフォルダとファイルに対して何も操作をしない」ことと「E-PC を LAN から切り離す」です。

B 課長は、不審なアクセスが認められた E-PC を使う E さんの行動を確認する手段のひとつとして「勤怠管理システム」と外部ネットワークである「インターネット」へのアクセスログを調査を行います。しかし、E さんの勤務時間とアクセスログを突き合わせたところ、大量の通信が記録されていた時刻には E さんは「退勤していた」ことがわかり、今回の不審なアクセスは、E さん自身によるものではないと推定されます。

まず、情報システム部は「E-PC の HDD を別の HDD にフルコピー」して、証拠保全を行います。次に、最新のパターンファイルを搭載した別の PC で「フルスキャンを実施」したり「ログなどを時系列に沿って整理および分析」したりすることで、原因を探ります。原因を特定する前に E さんに HDD を預けたり、OS を再インストールしたり、プロキシサーバを経由しない通信を許可したりするのは適切ではありません。

〔設問 2〕
(1) b ウ
c ア
d カ
e ア
(2) ウ

D 課長が「7 月 4 日から昨日までのログ中の通信先を解析したところ」「悪意ある Web サイトと判断された URL または IP アドレスに該当するものはなかった」と語っているので、E さんは怪しい Web サイトへはアクセスしていなかったと考えられます。

このことから、空欄 b と c は、閲覧するだけで不正プログラムに感染するように、企業の「正規」の公開 Web サイトが「改ざん」されたものだったと判断できます。

Web サイトが「改ざん」されたことによって、その Web サイトの所有者たる企業は「被害者」になります。しかし、Web サイト閲覧者からすると、不正プログラムによる被害をその Web サイトから受けたことになり、Web サイトの所有者は「加害者」にもなります。

そうした事態を避けるために、自社 Web サイトの脆弱性検査を定期的に実施して、問題があれば修正する。また、新たな脆弱性が発見された場合にも必要な対応をとる必要があります。

〔設問 3〕
(1) f カ
(2) エ
(3) g イ

B 課長は、内容が不明なデータが E-PC から社外に大量に送信されたことから、「情報漏えい」が起きたおそれもあると考え、E さんにヒアリングしました。こちらが送信しているので、DDoS 攻撃、辞書攻撃、総当たり攻撃は誤りで、改ざんや情報破壊も大量の送信とは直接は結びつきません。

マーケティング 1 課の E さんがマーケティング 2 課のプレゼントキャンペーンに関するファイルを共有フォルダで発見していて、マーケティング部内の共有パスワードもあることから、社内共有フォルダ N のアクセス権の設定単位は「部単位」だと判断できます。

改善すべき課題が他にもないか探すには、抜本的な調査が必要になります。脆弱性検査やアクセス権限、ウイルス対策ソフトやアップデート、インストールの状況といった限定的な調査や評価（アセスメント）では不十分です。マーケティング部内で取り扱っている全ての情報資産とその取扱い状況を可視化した上で、リスクアセスメントを実施するのが適切になります。

以上