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 29 年度　春期　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 29 年度　春期　過去問題　解答・解説

平成 29 年度　春期　午前問題の解説

〔問 01〕ア
トップマネジメントは、人々を指揮し支援したり、組織の戦略的な方向性と両立させたりしなければなりません。「他のプロセスと分ける」のではなく、統合させます。「方針に従う」のではなく、対応計画よりも大きな方針を策定します。

〔問 02〕ウ
セキュリティ対策は、自社だけでなく、サプライチェーンのビジネスパートナの実施状況を確認すべきです。

〔問 03〕ア
CSIRT（Computer Security Incident Response Team）マテリアルは、組織的なインシデント対応体制である組織内 CSIRT の構築を支援する目的で JPCERT/CC が作成している公開資料です。

〔問 04〕エ
ディザスタリカバリ（Disaster Recovery）は、災害（Disaster）からの回復（Recovery）するための措置です。RPO（目標復旧時点）は、直前なのか 24 時間前なのか 1 週間前でいいのかという状態を戻したい日時のことです。「災害発生時からどのくらいの時間以内にシステムを再稼働しなければならないかを示す指標」は RTO（Recovery Time Objective）です。

〔問 05〕イ
リスクマネジメントは、組織が置かれている環境やリスクの特徴と整合するように、組織に合わせて作られることが望ましい原則です。静的（固定的）なものではなく、動的であり、継続的に変化を察知して対応します。

〔問 06〕イ
リスクマネジメントのプロセスは、リスクを特定し、特定されたリスクを分析して把握した上で評価して、そのリスクへの対応を決定します。

〔問 07〕イ
リスクレベル（Level of Risk）は、「結果とその起こりやすさの組合せとして表現される、リスクの大きさ」です。結果（Consequence）は「目的に影響を与える事象の結末」、起こりやすさ（Likelihood）は「何かが起こる可能性」です。

〔問 08〕ウ
あらかじめ定めた連絡経路に従って迅速に連絡するのは正しい対応です。委託先である B 社に任せたり、経験豊富とはいえ担当者個人の判断を優先させたりすることは適切ではありません。

〔問 09〕イ
暗号の危殆化（Compromise）は、昔は解読できなかった暗号アルゴリズムが、解読されやすい状態になり、安全性が低下してしまうことです。

〔問 10〕ウ
タイムスタンプは、ファイルがある時刻以前に存在していたことや、その日時以降に改ざんされていないことを証明する仕組みです。

〔問 11〕ウ
情報セキュリティマネジメントシステムについて組織で働く人は、(1) 情報セキュリティ方針、(2) 自らの貢献、(3) 要求事項に適合しないで違反していることの意味について、認識を持っていなければなりません。

〔問 12〕ウ
JVN（Japan Vulnerability Notes）は、JPCERT/CC と IPA（情報処理推進機構）が共同で管理してソフトウェアなどの脆弱性関連情報や対策情報を提供している脆弱性情報データベースです。

〔問 13〕ア
NIDS（Network Intrusion Detection System）は、管理下のネットワーク内への不正侵入の試みを検知し、管理者に通知するネットワーク型侵入検知システムです。

〔問 14〕ア
「アクセスログの定期的な確認と解析」は、漏えいの可能性を早期に発見するために有効です。ウイルス対策ソフトは予防、バックアップは復旧、暗号化は漏えい防止の有効な対策です。

〔問 15〕エ
ディジタルフォレンジックスは、インシデントの究明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。

〔問 16〕ア
辞書攻撃は「推測されにくいパスワード」と「試行回数に制限」、盗聴を行うスニッフィングは「暗号化」、ブルートフォース(総当たり)攻撃には「試行回数に制限」が有効です。

〔問 17〕ウ
DMZ(DeMilitarized Zone)は、内部ネットワークと外部セグメントの両方から通信できます。ただし、DMZ から内部ネットワークに通信することはできず、外部セグメントへの通信だけが許可されています。

〔問 18〕ウ
パスワードと秘密の質問は「記憶」、静脈と指紋は「身体」、証明書とトークンは「所有」による認証です。2 要素認証は二つの要素の組み合わせにしなければなりません。

〔問 19〕ウ
ディジタル署名は、メッセージがその送信者からのものであることと改竄されていないことが確認できます。ディジタル署名には盗聴防止などの機能はありません。

〔問 20〕ウ
ハッシュ値(メッセージダイジェスト)は、メッセージからハッシュ関数によって生成されますが、ハッシュ値からメッセージを復元することは基本的にできません。

〔問 21〕ア
ソーシャルエンジニアリング (Social Engineering)は、技術的な手段ではなく、人間の心理的な隙や行動のミスを利用して、パスワードなどの重要な情報を盗み出す行為です。

〔問 22〕エ
ディジタル署名は送信者の秘密鍵でハッシュ値(メッセージダイジェスト)を暗号化し、受信者が送信者の公開鍵を使って復号して、メッセージがその送信者からのものであることと改竄されていないことを検証できる仕組みです。

〔問 23〕イ
ディレクトリトラバーサル攻撃は、サーバ内の想定外のファイル名を直接入力することによって、本来は許されないファイルを不正に閲覧する攻撃手法です。

〔問 24〕イ
エンティティは、実体や主体とも呼ばれ、情報を使用する組織および人、情報を扱う設備、ソフトウェアおよび物理的媒体などを意味する用語です。真正性(Authenticity)は、「エンティティは、それが主張するとおりのものであるという特性」と定義されています。信頼性(Reliability)は、意図する行動と結果とが一貫しているという特性です。

〔問 25〕エ
CRL(Certificate Revocation List、証明書失効リスト)は、何らかの理由で有効期間中に失効したディジタル証明書の一覧を示す証明書失効リストです。CA(Certification Authority)は認証局、CP(Certificate Policy)は証明書の利用方針、CPS(Certification Practice Statement)は運用規定です。

〔問 26〕イ
PCI DSS(Payment Card Industry Data Security Standard)は、クレジットカードなどのカード会員データのセキュリティ強化を目的として制定され、技術面および運用面の要件を定めた基準です。

〔問 27〕ア
不正のトライアングルは、不正行為が行われる三つの要素を示した理論です。三つの要素は、(1)業務量やノルマなどのプレッシャーや処遇への不満などの「動機」、(2)物理的な環境や組織のルールに盲点があるなどの「機会」、(3)不正行為を自己弁護できるような理由があるなどの「正当化」です。

〔問 28〕ア
IPsec（Security Architecture for Internet Protocol）は、OSI 基本参照モデルのネットワーク層で動作し、認証ヘッダ（AH、Authentication Header）と暗号ペイロード（ESP、Encapsulated Security Payload）の二つのプロトコルを含む暗号化のプロトコルです。

〔問 29〕イ
WAF（Web Application Firewall）におけるホワイトリストは、許可する通信データパターンを定義したもので、それ以外の通信は遮断します。ホワイトリスとは逆に、ブラックリストは、問題のある通信データパターンを定義したものであり、該当する通信を遮断または無害化します。

〔問 30〕ア
ポートスキャナ（Port Scanner）は、接続可能なポートがあるか、不要なサービスが稼働していないかなど確認するために、Web サーバで稼働しているサービスを列挙して走査（スキャン）することです。

〔問 31〕イ
電子署名法（電子署名および認証業務に関する法律）は、本人による一定の要件を満たす電子署名、が手書きの署名や押印と同等に通用する法的基盤です。

〔問 32〕ウ
インターネットショッピングで商品を購入するときは、事業者からの承諾の通知が消費者のメールサーバに到達した時点で売買の合意があったとされ、売買契約が成立します。

〔問 33〕エ
不正競争防止法で保護される「営業秘密」とは、(1) 秘密として管理されている、(2) 公然と知られていない、(3) 事業活動に有用な技術または営業上の情報という三つの要素を持つものです。

〔問 34〕ア
著作権法による保護の対象となるものは、著作物とそれを創作した著作者の権利であり、ソースプログラムそのものも保護の対象になります。ただし、プログラム言語やプロトコル（規約）、アルゴリズム（解法）や考え方は、著作権法の対象ではありません。

〔問 35〕
労働基準法 36 条では、時間外労働に関する労使協定を定めています。時間外労働を命じる場合には、労働組合などと書面による協定（36 協定）を結び、労働基準監督署に届け出る必要があります。裁量労働制でも年俸制でも、定められた労働時間を超えた労働には時間外手当が支給されなければなりません。

〔問 36〕ア
特権 ID の貸出しおよび返却の管理簿と、特権 ID のログを照合することは、特権 ID の不正使用を「発見」するコントロールとして有効です。通常の操作では一般利用者 ID を使用させたり、使用するごとに特権 ID を貸出したり、使用範囲を狭めたりすることは不正使用を「予防」するコントロールです。

〔問 37〕エ
例外ケースや異常ケースを想定したテストが行われていることを確認するのはシステムテストの監査として適切です。開発者側を交えずに利用者側の責任者や担当者だけの承認だけでは不充分です。実際に業務が行われている環境でテストを行うことは業務に影響があるので適切ではありません。

〔問 38〕ウ
システム監査人が、監査報告書の原案について被監査部門と意見交換を行うことは、監査報告書に記載する指摘事項および改善勧告について、事実誤認がないことを確認できるので適切です。

〔問 39〕ウ
システム障害の種類や発生箇所、影響度合いに関係なく、共通の連絡・報告ルートが定められているのは適切ではなく、監査人が監査報告書で報告すべき指摘事項に該当します。

〔問 40〕イ
「決められた業務手順どおりにシステムが稼働すること」は、利用者が優先して確認すべき事項です。その他の選択肢は、情報システム部門の運用者が確認すべき事項になります。

〔問 41〕ウ
運用レベル合意書（OLA、Operational Level Agreement）は、サービス提供者と内部グループとの間で取り交わした合意文書であり、サービスおよびサービス目標を定義した文書です。サービスレベル合意書（SLA、Service Level Agreement）は、サービス提供者と顧客との間で取り交わした合意文書であり、サービスおよびサービス目標を定義した文書です。

〔問 42〕イ
問題管理プロセスは、インシデントの未知の根本原因を特定し、恒久的な解決策を提案したり、インシデントの発生を事前予防的に防止したりするプロセスです。合意したサービス目標および時間枠内に達成することを確実にするのは「サービスレベル管理プロセス」です。

〔問 43〕ウ
「A→B→E→H」は「30＋5＋40＋30＝105」、「A→C→F→H」は「30＋30＋25＋30＝115」、「A→D→G→H」は「30＋20＋30＋30＝110」、「A→D→G→H」は「30＋20＋Cの完了を待つ 10＋30＋30＝120」なので、完了までは最短で 120 日が必要となります。

〔問 44〕イ
ホットスタンバイ方式では、現用系が故障すると、動作状態にある待機系に自動で迅速に切り替えるので、故障が発生したことを利用者に感じさせないような切替えが実現できます。現用系マシンが故障すると予備機を立ち上げるのはコールドスタンバイ方式です。

〔問 45〕ウ
マイニング（Mining）は「鉱石を掘り出す」という意味です。データマイニングは、大量のデータから統計学的手法などを用いて新たな知識（傾向やパターン）を見つけ出すプロセスです。

〔問 46〕ア
「404 Not Found」は URL で指定したページが見つからなかったときのエラーコードです。時間が掛かり過ぎるときは「408 Request Timeout」、ログインが拒否され認証できなかったときは「401 Unauthorized」です。

〔問 47〕エ
経営戦略は情報戦略の上位に相当する概念で、経営計画を実現するために情報化投資計画があります。情報戦略の立案時には、長期の経営計画との整合性をとる必要があります。

〔問 48〕ア
業務プロセスを抜本的に再設計することを「BPR(Business Process Re-engineering)」と呼んでいます。新たな視点から高い目標を設定し、将来的に必要となる最上位の業務機能と業務組織のモデルを、すべての業務において再検討します。

〔問 49〕イ
機能要件はシステムが必ず満たすべき要件であり、非機能要件は使用性や保守性など機能要件以外の特性です。選択肢では「障害発生時は半日以内に回復できること」が非機能要件に該当します。他の選択肢は機能要件に該当します。

〔問 50〕ウ
BCP(Business Continuity Plan)は、大規模な災害などによって、企業活動を支える重要な情報システムに障害が発生したような場合でも、企業活動の継続を可能にするために、あらかじめ策定する事業継続計画です。

平成 29 年度 春期 午後問題の解説

問 1

〔設問 1〕
(1) a オ
(2) コ
(3) イ

「画面に見慣れないメッセージが表示され」ていて、メッセージの内容は「画面にはファイルを復元するための金銭を要求するメッセージと、支払の手順が表示されていた」という記述から、ランサムウェアと呼ばれる種類のマルウェアに感染した可能性が高いと考えられます。

ランサムウェアが動作すると、端末がロックされたり、ファイルが暗号化されたりするなど、操作・使用ができなくなるなど、可用性が損なわれます。そして、可用性を取り戻すことと引き換えに、利用者や管理者に対して、犯人が金銭を要求するような脅迫を行います。

選択肢の中で、攻撃者の身元を特定しにくくするために使える技術は、仮想通貨の「Bitcoin(ビットコイン)」、インターネット上に公開されている代理サーバ「Tor」です。

〔設問 2〕
(1) b オ c ク
(2) ア

「支払った場合にはデータを確実に復元できるが、支払わなかった場合にはデータを復元できない可能性が高い」という前提なので、「攻撃者から要求されている金額」を支払えば、その分は損失になり、さらに犯人に屈して「犯罪を助長したという事実に起因する企業価値の損失」が想定されます。

前提の通りであれば、「攻撃者から要求されている金額」を支払わずに、自力で復元すると「自力でのデータ復元の試みに要する金額」が掛かります。

「支払った場合にはデータを確実に復元できるが、支払わなかった場合にはデータを復元できない可能性が高い」という前提を置かずに対応について検討すれば、支払に応じるべきではない理由は「金銭を支払うことによって、自社への更なる攻撃につながり得るから」であり、犯罪行為を行う攻撃者に「金銭を支払っても、ファイルを復号できる保証がないから」です。

〔設問 3〕
(1) ウ、エ
(2) イ
(3) イ

「データの取扱いおよびバックアップに関するルールの内容が不十分であったこと」直接の原因になるのは、「Q 営業所で NAS のデータのバックアップが実施されなかったこと」と「何を NAS に保存するか、PC に保存するかが」決められていないので、統一されていないことです。

「今回の種類のマルウェアに感染することによってファイルが暗号化されてしまうという被害に備えたバックアップ」として効果があるのは、定期的に複製すること、安全に保管することです。ネットワークから記憶媒体（ハードディスク）を切り離すのは、安全に保管することになります。

「バックアップ対象のデータの可用性確保のための対策を検討」すれば、「バックアップした媒体からデータが正しく復元できるかテストする」ことと「バックアップした媒体を二つ作成し、一つは営業所に、もう一つは別の安全な場所に保管する」ことが挙げられます。完全な破棄や暗号化を施すことは「可用性確保のため」ではありません。

問 2

〔設問 1〕
(1) a ア
(2) ク
(3) b イ
(4) c カ

選択肢の中で、クラウドサービスを利用するメリットは「IT 資源を迅速かつ柔軟に利用できる」ことが挙げられます。

「情報システム部と一緒に Y 社 SaaS における情報セキュリティ対策を確認」すべきなのは、Y 社 SaaS で管理されていたデータに関すること、Y 社 SaaS におけるデータ暗号化機能、Y 社の「入退出管理、管理者特権」の管理状況です。

「I. P システムの概要」では、P システムへは常に社内ポータルにログインしてからアクセスするので、に社内ポータルとなる「X 社のグローバル IP アドレス」からのアクセスだけを受け付ける設定にすればよいことになります。

コストパフォーマンスも考慮すると自社でシステムを運用しようとする「P システムのコールドスタンバイ」は大がかり過ぎて無駄で、他社のサービスに移行することを考えると「見込客データのバックアップ」について検討することが最善です。

RPO（Recovery Point Objective）は復旧させる時点、RTO（Recovery Time Objective）復旧に掛かる時間の目標値ですが、SaaS を利用する側なので、直接の検討対象にはなりません。

〔設問 2〕
(1) d ア
e エ
f イ
(2) キ

空欄 d には、対策基準を満たして、10 月 1 日から実施できることが条件になります。この条件を満たしているのは「営業所の所長または主任が、都度、販売企画課にメールで連絡する」だけです。人事システムの改修は 10 月 1 日からの実施には「難しい」という記述があります。

空欄 e には、申請と承認を切り分けて、相互牽制が働く手順である「販売企画課担当者用アカウントには申請権限だけを設定し、販売企画課管理者用アカウントには承認権限だけを設定して、後者の付与は E 主任のままとする」が入ります。空欄 f には、一度は同意した配信を解除する手続きである「オプトアウト」が入ります。

販売員用アカウント以外のアカウントにも送信停止の権限を設定する必要である理由は、販売員が送信停止処理よりも販売活動を優先するおそれがあるから、見込客が本社宛てに電話などで申し出た場合や、見込客を担当する販売員が不在の場合でも、電話を受けた営業所で停止処理ができるようにする必要があるからです。

問 3

〔設問 1〕
(1) a カ
b オ
c ケ
(2) ア
(3) 2 カ
3 オ
4 イ
5 ア

共有エリアの複合機で、個人情報を含む文書を印刷して放置しているという問題の改善策を探る空欄 a には、複合機に従業員証を認識させる(案 1)と、通販事業部エリアでしか印刷させない(案 4)が入ります。

大量に保有している紙媒体の管理が問題となる空欄 b には、スキャナで電子化する(案 6)と機密情報を明確に分けて施錠できるキャビネットに保管する(案 7)が適切です。

通販事業部エリアへの入室時に、通販事業部の複数の従業員同士が一緒に入室してしま共連れの問題は、標語の掲示で啓蒙を行う(案 10)と、情報セキュリティリーダが個別に注意する(案 12)が有効です。

他の人と同時に入室してしまって入室記録がない「共連れ」だと思われるログを抽出するための条件は「1 日の入室ログ件数と退室ログ件数が異なる従業員のログ」です。

対策は諦めて現状のままにする 2 は「リスク保有」、入室したときの記録がないと退室できないような仕組みであるアンチパスバックを有効にする 3 は「リスク発生可能性の低減」です。

個人情報が漏えいした場合に備えて保険に加入しておく 4 は保険会社との「リスク共有」、リスクをゼロするために事業をやめてしまう 5 は「リスク回避」に相当します。

〔設問 2〕
d キ

鍵店に行けば簡単に合い鍵が作れるという空欄 d1 は「シリンダ錠」、設定を変えるだけで利用者を制限できるが情報が他人に漏れたら解錠されてしまう空欄 d2 は「プッシュボタン式の暗証番号錠」が入ります。

複製が困難なのは ID 情報を埋め込んだタグによる近距離無線通信である空欄 d3 は「RFID 認証式の錠」、解錠に必要なものを貸し出すことができない空欄 d4 はバイオメトリクス認証の「指静脈認証錠」です。

〔設問 3〕
e エ
f ウ
g ア
h カ

コールセンタ要員以外のものが侵入してくる空欄 e と空欄 f は「ネックストラップ式の入館証をコールセンタ要員に貸与し、着用させる」、「出入口に警備員を配置し、入館証チェックや持ち物チェックを行う」が適切です。

コールセンタ要員は記憶媒体を持ち込んで情報を窃取する空欄 f と空欄 g は「コールセンタ内での記憶媒体の使用を禁止する」、「入り口の外にロッカーを設置し、私物をそこに預け、業務上必要な物だけを透明なバッグに入れて執務室に出入りするようにする」が適切です。

コールセンタ要員がノートPCを盗んでしまう空欄f、空欄g、空欄hは、警備員によるチェック、私物の持ち込み制限、「ノートPCをセキュリティケーブルで机に固定する」が適切です。

以上