第 16 章　第2回試験（平成 28 年＝2016 年秋）午前問題と解説

本章について

2016 年秋，情報処理技術者試験センターは2回目の情報セキュリティマネジメント試験の開催後，試験問題（午前 50 問，午後 3 問）と解答，採点講評を公開しました．本章では午前問題の全問題文とオリジナル解説を掲載します．

出題割合はストラテジ系が 10 問，マネジメント系が 6 問，テクノロジ系が 34 問で第1回と全く同じ（出題要綱の通り）でした．合格率は（合格点が固定で人数制限のない試験ですので合格率を気にする必要は全くありませんが）第1回の 88.0%に対して第2回は 70.3%でした．下降傾向に見えますが，第1回が異常だったと考えて良いでしょう．

16.1 第2回午前試験＜テクノロジ系＞の問題と解説

問1　＜テクノロジ系＞　IC カードと PIN を用いた利用者認証における適切な運用はどれか．

ア　IC カードによって個々の利用者を識別できるので，管理負荷を軽減するために全利用者に共通の PIN を設定する．
イ　IC カード紛失時には，新たな IC カードを発行し，PIN を再設定した後で，紛失した IC カードの失効処理を行う．
ウ　PIN には，IC カードの表面に刻印してある数字情報を組み合わせたものを設定する．
エ　PIN は，IC カードには同封せず，別経路で利用者に知らせる．

正解：エ

PIN（1.1.12 参照）は個人識別番号であり「記憶による認証」の一種です．IC カードのような「所有物による認証」と組み合わせることで**2要素認証**（1.1.12　参照）となります．

PIN を IC カードに同封して送ると，盗難や事故により他者に渡った場合に，不正アクセスを引き起こすおそれがありますので，エが正解です．
アは他の利用者の IC カードを流用できてしまうので不適切です．
イは紛失した IC カードの失効処理を先に行うべきですので不適切です．
ウは IC カードから PIN が類推できてしまいますので不適切です．

問2 ＜テクノロジ系＞ リスクの顕在化に備えて地震保険に加入するという対応は，JIS Q 31000:2010 に示されているリスク対応のうち，どれに分類されるか．

ア ある機会を追求するために，そのリスクを取る又は増加させる．
イ 一つ以上の他者とそのリスクを共有する．
ウ リスク源を除去する．
エ リスクを生じさせる活動を開始又は継続しないと決定することによって，リスクを回避する．

正解：イ

JIS Q 31000:2010（1.2.1 参照）は，リスクマネジメントについての国際標準規格 ISO 31000 を JIS 化したものです．リスクの顕在化に備えて地震保険に加入することは**リスク共有**（10.2.5 参照）であり，イに該当します．
アは**リスク保有**（10.1.1 参照）に該当します．
ウとエは**リスク回避**（10.1.1 参照）に該当します．

問3 ＜テクノロジ系＞ JPCERT/CC の説明はどれか．

ア 工業標準化法に基づいて経済産業省に設置されている審議会であり，工業標準化全般に関する調査・審議を行っている．
イ 電子政府推奨暗号の安全性を評価・監視し，暗号技術の適切な実装法・運用法を調査・検討するプロジェクトであり，総務省及び経済産業省が共同で運営する暗号技術検討会などで構成される．
ウ 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る．
エ 内閣官房に設置され，我が国をサイバー攻撃から防衛するための司令塔機能を担う組織である．

正解：ウ

JPCERT/CC（1.2.9 参照）は特定の政府機関や企業からは独立した中立のセキュリティ機関です．
アは **JIS**（2.5.1 参照）です．
イは **CRYPTREC**（1.2.9 参照）です．
エは**内閣サイバーセキュリティセンター（NISC）**（1.2.9 参照）です．

問4 ＜テクノロジ系＞ JVN(Japan Vulnerability Notes)はどれか．

ア 情報システムに存在する脆弱性の深刻度を評価する手法．
イ 製品に存在する脆弱性に対して採番された識別子．

ウ　脆弱性対策情報などを提供するポータルサイト.
エ　組織内の情報セキュリティ問題を専門に扱うインシデント対応チーム.

正解:ウ

JVN(1.2.9 参照)は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する脆弱性対策情報ポータルサイトです.
アは **CVSS**(1.3.1 参照)です.
イは **CVE**(1.3.1 参照)です.
エは **CSIRT**(1.2.9 参照)です.

問5　＜テクノロジ系＞　ファイルサーバについて, 情報セキュリティにおける"可用性"を高めるための管理策として, 適切なものはどれか.

ア　ストレージを二重化し, 耐障害性を向上させる.
イ　ディジタル証明書を利用し, 利用者の本人確認を可能にする.
ウ　ファイルを暗号化し, 情報漏えいを防ぐ.
エ　フォルダにアクセス権を設定し, 部外者の不正アクセスを防止する.

正解:ア

可用性(1.1.1 参照)は **OECD セキュリティガイドライン**(**情報システムのセキュリティに関するガイドライン**: 1.1.1 参照)で述べられている情報セキュリティの3要素の1つで, 必要な時に必ず利用できること, またはその度合いです. 選択肢の中では耐障害性を向上させることが該当します.
イは **真正性**(1.1.1 参照)です.
ウ, エは **機密性**(1.1.1 参照)です.

問6　＜テクノロジ系＞　情報セキュリティ対策を検討する際の手法の一つであるベースラインアプローチの特徴はどれか.

ア　基準とする望ましい対策と組織の現状における対策とのギャップを分析する.
イ　現場担当者の経験や考え方によって検討結果が左右されやすい.
ウ　情報資産ごとにリスクを分析する.
エ　複数のアプローチを併用して分析作業の効率化や分析精度の向上を図る.

正解:ア

ベースラインアプローチ(1.2.4 参照)はリスク分析手法の一つで, ベースライン(自組織の対策基準)を策定し, 適用するものです. 採用した管理策への準拠状況を把握するために, 基準とする望ましい対策と組織の現状における対策とのギャップを分析します.

ウは「情報資産毎にリスクを評価しない」の誤りです.
イとエは, ベースラインアプローチの特徴ではありません.

問7 ＜テクノロジ系＞ 組織の所属者全員に利用者 ID が発行されるシステムがある. 利用者 ID の発行・削除は申請に基づき行われているが, 申請漏れや申請内容のシステムへの反映漏れがある. 資料A, Bの組合せのうち, 資料Aと資料Bを突き合わせて確認することによって, 退職者に発行されていた利用者 ID の削除漏れが最も確実に発見できるものはどれか.

	資料A	資料B
ア	組織の現在の所属者の名簿	退職に伴う利用者 ID の削除申請書
イ	退職者の一覧	組織の現在の所属者の名簿
ウ	利用者 ID とそれが発行されている者の一覧	組織の現在の所属者の名簿
エ	利用者 ID とそれが発行されている者の一覧	退職に伴う利用者 ID の削除申請書

正解:ウ

「利用者 ID とそれが発行されている者の一覧」に「組織の現在の所属者の名簿」に掲載されていない者がいれば, それは「退職者に発行されていた利用者 ID の削除漏れ」だと分ります.
アとイは(名簿が正しければ)突き合わせても合致する者がいませんので不適切です.
エは「利用者 ID とそれが発行されている者の一覧」に「退職に伴う利用者 ID の削除申請書」に掲載されている者がいれば削除申請書の処理モレを発見できますが, 削除申請書が出されていない場合は確認できませんので, 最も確実とはいえません.

問8 ＜テクノロジ系＞ JIS Q 27000 におけるリスク評価はどれか.

ア 対策を講じることによって, リスクを修正するプロセス.
イ リスクが受容可能か否かを決定するために, リスク分析の結果をリスク基準と比較するプロセス.
ウ 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.
エ リスクの発見, 認識及び記述を行うプロセス.

正解:イ

JIS Q 27000(1.2.8 参照)ではリスクアセスメントを **リスク特定**(1.2.4 参照), **リスク分析**(1.2.4 参照)及び **リスク評価**(1.2.4 参照)のプロセス全体と定義しており, リスク評価を「リスクが受容可能か否かを決定するために, リスク分析の結果をリスク基準と比較するプロセス」と規定しています.
アは JIS Q 27000 における **リスク対応**(1.2.5 参照)の説明です.

ウは JIS Q 27000 におけるリスク分析の説明です.
エは JIS Q 27000 におけるリスク特定の説明です.

問9 ＜テクノロジ系＞ JIS Q 31000:2010 における, 残留リスクの定義はどれか.

ア 監査手続を実施しても監査人が重要な不備を発見できないリスク.
イ 業務の性質や本来有する特性から生じるリスク.
ウ 利益を生む可能性に内在する損失発生の可能性として存在するリスク.
エ リスク対応後に残るリスク.

正解:エ

JIS Q 31000(1.2.1 参照)は, リスクマネジメントについての国際標準規格 ISO 31000 を JIS 化したもので, **残留リスク**(1.2.5 参照)を「リスク対応後に残るリスク」と定義しています.
アは **監査リスク**(8.1.1 参照)の説明です.
イは監査リスクに含まれる **固有リスク**(8.1.1 参照)の説明です.
ウは **投機リスク**(1.2.3 参照)の説明です.

問 10 ＜テクノロジ系＞ 情報セキュリティ意識向上のための教育の実施状況を JIS Q 27002 に従ってレビューした. 情報セキュリティを強化する観点から, 改善が必要な状況はどれか.

ア 従業員の受講記録を分析し, 教育計画を見直していた.
イ 従業員の職務内容や職制に応じた内容の教育を実施していた.
ウ 出張中で受講できなかった従業員を対象に, 追加の教育を実施していた.
エ 正規従業員と同様の業務に従事している派遣従業員を除いて, 教育を実施していた.

正解:エ

JIS Q 27002(1.2.8 参照)は ISMS の実施基準として制定された ISO/IEC 17799 を JIS 化したものです.
情報セキュリティ意識向上のための教育であれば, 正規従業員と同様の業務に従事している派遣従業員も教育の対象にする必要があります.
ア, イ, ウはどれも改善が必要な状況ではありません.

問 11 ＜テクノロジ系＞ システム管理者に対する施策のうち, IPA"組織における内部不正防止ガイドライン"に照らして, 内部不正防止の観点から適切なものはどれか.

ア システム管理者間の会話・情報交換を制限する.
イ システム管理者の操作履歴を本人以外が閲覧することを制限する.

ウ　システム管理者の長期休暇取得を制限する.
エ　夜間・休日のシステム管理者の単独作業を制限する.

正解:エ

組織における内部不正防止ガイドライン(1.4.1 参照)における内部不正防止の施策としては, システムに対する強い権限を有するシステム管理者が不正行為を起こしやすい状態を防止することがあります. よって, 選択肢の中では「夜間・休日のシステム管理者の単独作業の制限」が適切です.
アは内部不正防止の施策とは無関係です.
イはシステム管理者が不正行為を起こしやすい状態にしてしまいます.
ウは内部不正防止の施策とは無関係であり, しかも, **労働基準法**(2.3.1 参照)に抵触する恐れがあります.

問 12　<テクノロジ系>　ボットネットにおける C&C サーバの役割はどれか.

ア　Web サイトのコンテンツをキャッシュし, 本来のサーバに代わってコンテンツを利用者に配信することによって, ネットワークやサーバの負荷を軽減する.
イ　遠隔地からインターネットを経由して社内ネットワークにアクセスする際に, CHAP などのプロトコルを用いることによって, 利用者認証時のパスワードの盗聴を防止する.
ウ　遠隔地からインターネットを経由して社内ネットワークにアクセスする際に, チャレンジレスポンス方式を採用したワンタイムパスワードを用いることによって, 利用者認証時のパスワードの盗聴を防止する.
エ　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.

正解:エ

C&C(Command and Control)サーバ(1.1.4 参照)はボットへの指令サーバであり, 同一の指令サーバの配下にある複数のボットが, 指令サーバを中心とするネットワークを組んだものがボットネットです.
アは **プロキシサーバ**(5.2.2 参照)の機能の一部.
イは **認証サーバ**(1.5.2 参照)の機能です.
ウは **CHAP**(1.1.11 参照)の説明です.

問 13　<テクノロジ系>　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して, スマートフォンの利用状況などを一元管理する仕組みはどれか.

ア　BYOD(Bring Your Own Device)
イ　ECM(Enterprise Contents Management)

ウ　LTE(Long Term Evolution)
エ　MDM(Mobile Device Management)

正解:エ

MDM(Mobile Device Management)(1.4.3 参照)は，モバイル端末と社内システムとの認証，アプリケーションとの同期，外部サービスとの接続等を管理するシステムです．
アの **BYOD(Bring Your Own Device)**(9.2.1 参照)は H28 春午前問 11(14 章参照)の通り，従業員が私的に保有する情報端末を業務に利用することです．
イの **ECM(Enterprise Contents Management)**(8.1.2 参照)は企業などが保有するコンテンツ(文書，画像，音声，動画などのデータ)を統合的に管理する仕組みやツールです．
ウの **LTE(Long Term Evolution)**(5.5.5 参照)は第 4 世代移動体通信規格の一種です．

問 14　＜テクノロジ系＞　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はどれか．

ア　RFID
イ　rootkit
ウ　TKIP
エ　web beacon

正解:イ

rootkit(1.1.9 参照)は攻撃者がコンピュータに不正侵入した後に利用するためのソフトウェアをまとめたパッケージです．
アの **RFID(Radio Frequency Identification)**(5.2.1 参照)は極小の集積回路にアンテナを組み合わせたもので電子荷札に利用されます．
ウの **TKIP(Temporal Key Integrity Protocol)**(1.4.2 参照)は暗号鍵を一定時間ごとに自動的に更新するプロトコル，または機能．
エの **web beacon**(5.5.2 参照)は Web ページや HTML 形式電子メールに1ドット程度の非常に小さなサイズの画像を埋め込む手法，またはその画像．

問 15　＜テクノロジ系＞　SIEM(Security Information and Event Management)の機能として，最も適切なものはどれか．

ア　機密情報を自動的に特定し，機密情報の送信や出力など，社外への持出しに関連する操作を検知しブロックする．
イ　サーバやネットワーク機器などのログデータを一括管理，分析して，セキュリティ上の脅威を発見し，通知する．
ウ　情報システムの利用を妨げる事象を管理者が登録し，各事象の解決・復旧までを

管理する.
エ　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.

正解:イ

SIEM(1.4.3 参照)はセキュリティ情報およびイベント管理の製品群で，ログデータの一元管理とリアルタイム分析，レポーティング機能などを含みます.
アは **DLP**(1.4.3 参照)の機能です.
ウは **サービスマネジメントプロセス**(7.3 参照)の一連の管理活動です.「情報システムの利用を妨げる事象」は **インシデント**(7.3.6 参照)に該当します.
エは **IDS**(1.4.3 参照)の機能です.

問 16　＜テクノロジ系＞　SPF(Sender Policy Framework)を利用する目的はどれか.

ア　HTTP 通信の経路上での中間者攻撃を検知する.
イ　LAN への PC の不正接続を検知する.
ウ　内部ネットワークへの不正侵入を検知する.
エ　メール送信元のなりすましを検知する.

正解:エ

SPF（1.4.2 参照）は電子メールの送信元アドレスの偽装を防止する技術. SPAM 対策の一つです.
アの **中間者攻撃（Man-in-the-middle）**（1.1.9 参照）とは，攻撃者がクライアントとサーバとの通信の間に割り込み，クライアントと攻撃者との間の通信を攻撃者とサーバとの間の通信として中継することによって正規の相互認証が行われているようにしてセキュリティを破る攻撃手法です.
イを目的の一つとする手法としては**検疫ネットワーク**（1.4.2 参照）があります.
ウは **IDS**(1.4.3 参照)です.

問 17　＜テクノロジ系＞　次の電子メールの環境を用いて，秘密情報を含むファイルを電子メールに添付して社外の宛先の利用者に送信したい. その際のファイルの添付方法，及びその添付方法を使う理由として，適切なものはどれか.

〔電子メールの環境〕

- 電子メールは，Web フラウザから利用できる電子メールシステム(Web メール)を用いて送信する.
- Web ブラウザと Web メールのサーバとの通信は HTTP over TLS(HTTPS)で行う.
- 社外の宛先ドメインのメールサーバは SMTP と POP3 を使用している.
- IP 層以下は暗号化していない.

ア　Web ブラウザから Web メールのサーバまでの通信が暗号化されているので，ファイルは平文のままでメールに添付する．
イ　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るが，その後の通信が暗号化されないこともあるので，ファイルを暗号化してメールに添付する．
ウ　Web ブラウザから宛先の利用者がメールを受信する PC まで，全ての通信は暗号化されるので，ファイルは平文のままでメールに添付する．
エ　Web メールのサーバから宛先ドメインのメールサーバまでの通信は暗号化されないが，サーバ間の通信は Base64 形式でエンコードすれば盗聴できないので，ファイルは Base64 形式でエンコードしてメールに添付する．

正解：イ

Web ブラウザから Web メールのサーバまでの通信は，**HTTP over TLS(HTTPS)**（5.3.2 参照）で行いますので暗号化されます．しかし「社外の宛先ドメインのメールサーバは **SMTP**（5.3.2 参照）と **POP3**（5.3.2 参照）を使用しているので，その後の通信が暗号化される保証はありません．「秘密情報を含むファイルを電子メールに添付して社外の宛先の利用者に送信したい」のですから，ファイルを暗号化してメールに添付する必要があります．
エの「**Base64 形式**（5.5.1 参照）でエンコードすれば盗聴できない」は誤りです．

問 18　＜テクノロジ系＞　ウイルス検出におけるビヘイビア法に分類されるものはどれか．

ア　あらかじめ検査対象に付加された，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とを比較する．
イ　検査対象と安全な場所に保管してあるその原本とを比較する．
ウ　検査対象のハッシュ値と既知のウイルスファイルのハッシュ値とを比較する．
エ　検査対象をメモリ上の仮想環境下で実行して，その挙動を監視する．

正解：エ

ビヘイビア法（1.4.3 参照）はウイルスをあえて動作させる手法で，未知のウイルスにも適応できます．
アは **チェックサム／インテグリティチェック法**（1.4.3 参照），イは比較法で，感染の有無を検出できることがあります．
ウはハッシュ値を用いたチェックで，既知のウイルスであれば種類も検出できることがあります．

問 19　＜テクノロジ系＞　インターネットと社内サーバの間にファイアウォールが設置されている環境で，時刻同期の通信プロトコルを用いて社内サーバがもつ時計をインターネット上の時刻サーバの正確な時刻に同期させる．このとき，ファイアウォールで許可すべき時刻サーバとの間の通信プロトコルはどれか．

ア FTP(TCP, ポート番号 21)
イ NTP(UDP, ポート番号 123)
ウ SMTP(TCP, ポート番号 25)
エ SNMP(TCP 及び UDP, ポート番号 161 及び 162)

正解:イ

時刻同期の通信プロトコルは **NTP(Network Time Protocol)**(5.3.2 参照)です. 社内サーバがもつ時計をインターネット上の時刻サーバの正確な時刻に同期させるには, この通過をファイアウォールで許可せねばなりません.
アの **FTP**(5.3.2 参照)はファイル転送プロトコルです.
ウの **SMTP**(5.3.2 参照)はメール転送プロトコルです.
エの **SNMP**(5.3.2 参照)はネットワーク管理プロトコルです.

問 20 <テクノロジ系> 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はどれか.

ア CAPTCHA
イ QR コード
ウ 短縮 URL
エ トラックバック ping

正解:ア

CAPTCHA(1.1.12 参照)は入力フォームへのソフトウェアによる自動入力を排除するための手法です.
イの **QR コード**(2.5.1 参照)は2次元バーコードの代表例.
ウの **短縮 URL**(5.5.2 参照)は通常の URL を短縮する Web サービス. 特に文字数の制限がある SNS において活用されています.
エの **トラックバック ping**(5.5.2 参照)はブログにおいてトラックバックを利用してリンクを作成したことを相手に通知するためのプロトコルです.

問 21 <テクノロジ系> 情報の"完全性"を脅かす攻撃はどれか.

ア Web ページの改ざん
イ システム内に保管されているデータの不正コピー
ウ システムを過負荷状態にする DoS 攻撃
エ 通信内容の盗聴

正解:ア

完全性(1.1.1 参照)を脅かす攻撃としては改ざんやデータ破壊などがあります.
イとエは **機密性**(1.1.1 参照)を脅かす攻撃.
ウは **可用性**(1.1.1 参照)を脅かす攻撃.

問 22 ＜テクノロジ系＞ クロスサイトスクリプティングの手口はどれか.

ア Web アプリケーションに用意された入力フィールドに, 悪意のある JavaScript コードを含んだデータを入力する.
イ インターネットなどのネットワークを通じてサーバに不正にアクセスしたり, データの改ざん・破壊を行ったりする.
ウ 大量のデータを Web アプリケーションに送ることによって, 用意されたバッファ領域をあふれさせる.
エ パス名を推定することによって, 本来は認証された後にしかアクセスが許可されていないページに直接ジャンプする.

正解:ア

クロスサイトスクリプティング(1.1.9 参照)は, 訪問者の入力データをそのまま画面に表示する脆弱性がある Web サイトを悪用する攻撃です.
イは **クラッキング**(1.1.3 参照), ウは **バッファオーバフロー攻撃**(1.1.9 参照), エは **ディレクトリトラバーサル**(1.1.9 参照)です.

問 23 ＜テクノロジ系＞ 内閣は, 2015 年 9 月にサイバーセキュリティ戦略を定め, その目的達成のための施策の立案及び実施に当たって, 五つの基本原則に従うべきとした. その基本原則に含まれるものはどれか.

ア 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.
イ サイバー空間上の脅威は, 国を挙げて対処すべき課題であり, サイバー空間における秩序維持は国家が全て代替することが適切である.
ウ サイバー空間においては, 安全確保のために, 発信された情報を全て検閲すべきである.
エ サイバー空間においては, 情報の自由な流通を尊重し, 法令を含むルールや規範を適用してはならない.

正解:ア

サイバーセキュリティ戦略の基本原則(1.2.9 参照)は「情報の自由な流通の確保」「法の支配」「開放性」「自律性」「多様な主体の連携」であり, アは「開放性」に該当します.
イは「自律性」の原則から不適切です.
ウは「情報の自由な流通の確保」の原則から不適切です.
エは「法の支配」の原則から不適切です.

問 24 ＜テクノロジ系＞ スクリプトキディの典型的な行為に該当するものはどれか.

ア PC の利用者が Web サイトにアクセスし，利用者 ID とパスワードを入力するところを後ろから盗み見して，メモをとる.
イ 技術不足なので新しい攻撃手法を考え出すことはできないが，公開された方法に従って不正アクセスを行う.
ウ 顧客になりすまして電話でシステム管理者にパスワードの再発行を依頼し，新しいパスワードを聞き出すための台本を作成する.
エ スクリプト言語を利用してプログラムを作成し，広告や勧誘などの迷惑メールを不特定多数に送信する.

正解:イ

スクリプトキディ(1.1.7 参照)は技術不足によりクラッカー(攻撃者)にはなりきれない幼稚な者ですが，攻撃者予備群となりやすいと言われています.
アは **ショルダハッキング**(1.1.3 参照)の一例です.
ウ:スクリプトキディはスクリプト(台本)作成者とは限らない(その技術がない)ので不適切.
エ:スクリプトキディはスクリプト言語を悪用するとは限らない(その技術がない)ので不適切.

問 25 ＜テクノロジ系＞ 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，どれに分類されるか.

ア ソーシャルエンジニアリング
イ トロイの木馬
ウ 踏み台攻撃
エ ブルートフォース攻撃

正解:ア

ソーシャルエンジニアリング(1.1.3 参照)は IT を用いない攻撃手法の総称です.
イの **トロイの木馬** は 1.1.4 参照.
ウの **踏み台攻撃** は，**ボット**(1.1.4 参照)による遠隔操作のことです.
エの **ブルートフォース攻撃** は **総当り攻撃**(1.1.9 参照)のことです.

問 26 ＜テクノロジ系＞ パスワードリスト攻撃に該当するものはどれか.

ア 一般的な単語や人名からパスワードのリストを作成し，インターネットバンキングへのログインを試行する.
イ 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する.
ウ 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.
エ　ピクチャパスワードの入力を録画してリスト化しておき，それを利用することでタブレット端末へのログインを試行する.

正解：ウ

パスワードリスト攻撃（1.1.9 参照）は他のサイトから漏えいした ID/パスワードの一覧表を悪用する手法です．複数の Web サイトで同一の ID とパスワードを使っているユーザを狙う攻撃です.
アは **辞書攻撃**（1.1.9 参照），イは **レインボー攻撃**（1.1.9 参照）です.
エはタブレット端末における **ピクチャパスワード**（1.1.12 参照）を用いた自動入力防止に対抗する手法です.

問 27　＜テクノロジ系＞　ランサムウェアに分類されるものはどれか.

ア　感染した PC が外部と通信できるようプログラムを起動し，遠隔操作を可能にするマルウェア
イ　感染した PC に保存されているパスワード情報を盗み出すマルウェア
ウ　感染した PC のキー操作を記録し，ネットバンキングの暗証番号を盗むマルウェア
エ　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

正解：エ

ランサムウェア（1.1.4 参照）は身代金を要求するマルウェアです.
アは **ボット**（1.1.4 参照），イは **スパイウェア**（1.1.4 参照），ウは **キーロガー**（1.1.4 参照）に該当します.

問 28　＜テクノロジ系＞　なりすましメールでなく，EC(電子商取引)サイトから届いたものであることを確認できる電子メールはどれか.

ア　送信元メールアドレスが EC サイトで利用されているアドレスである.
イ　送信元メールアドレスのドメインが EC サイトのものである.
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.
エ　電子メール本文の末尾にテキスト形式で書かれた送信元の連絡先に関する署名のうち，送信元の組織を表す組織名が EC サイトのものである.

正解：ウ

なりすましではないことを確認するには，悪意を持つ者が偽装できない情報が必要です．その一つが **ディジタル署名**（1.1.11 参照）で，署名者の **ディジタル証明書**（1.1.14

参照）の発行元が信頼できる組織のものであれば，本人だと確認できます．
アの「送信元メールアドレス」，イの「送信元メールアドレスのドメイン」，エの「送信元の連絡先に関する署名」は，悪意を持つ者が偽装できますので確認できません．

問 29 ＜テクノロジ系＞ PKI(公開鍵基盤)の認証局が果たす役割はどれか．

ア 共通鍵を生成する．
イ 公開鍵を利用しデータの暗号化を行う．
ウ 失効したディジタル証明書の一覧を発行する．
エ データが改ざんされていないことを検証する．

正解：ウ

PKI（1.1.14 参照）は公開鍵基盤で，公開鍵暗号方式を用いた技術・製品の総称です．これを支える **認証局**（1.1.14 参照）の役割は公開鍵が被認証者（認証されたい者）のものであることを示す **ディジタル証明書**（1.1.14 参照）を発行することで，これを補足するために，失効したディジタル証明書の一覧である **CRL**（1.1.14 参照）も発行しています．
認証局は「共通鍵の生成」「データの暗号化」「改ざん検証」は行いません．

問 30 ＜テクノロジ系＞ 情報技術セキュリティ評価のための国際標準であり，コモンクライテリア(CC)と呼ばれるものはどれか．

ア ISO 9001
イ ISO 14004
ウ ISO/IEC 15408
エ ISO/IEC 27005

正解：ウ

ISO/IEC 15408（1.3.1 参照）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，正しく実装されていることを評価するための国際標準です．
アの **ISO 9001** は，品質マネジメントシステムおよび品質保証のための国際標準規格群である **ISO 9000 ファミリー**（2.5.1 参照）に含まれる品質マネジメントシステムに関する要求事項を規定した規格です．
イの **ISO 14004** は，環境マネジメントシステムのための国際標準規格群である **ISO 14000 ファミリー**（2.5.1 参照）に含まれる，環境マネジメントシステムの実施の一般指針を規定した規格です．
エの **ISO/IEC 27005** は，情報セキュリティマネジメントシステムのための国際標準規格群である **ISO/IEC 27000 ファミリー**（2.5.1 参照）に含まれる，リスクマネジメントの規格です．

問 45 ＜テクノロジ系＞ クライアントサーバシステムを構築する. Web ブラウザによってクライアント処理を行う場合, 専用のアプリケーションによって行う場合と比較して, 最も軽減される作業はどれか.

ア クライアント環境の保守
イ データベースの構築
ウ サーバが故障したときの復旧
エ ログインアカウントの作成と削除

正解:ア

クライアントサーバシステム(3.1.2 参照)で Web システムを構築し, クライアント処理を Web ブラウザによってクライアント処理を行うことで, クライアントへのアプリケーションのインストールが不要になります. よって, クライアント環境の保守の作業が軽減されます.
イ:データベースの構築は主にサーバ側の作業ですので, クライアント処理を変えても作業軽減にはなりません.
ウ:サーバが故障したときの復旧はサーバ側のの作業ですので, クライアント処理を変えても作業軽減にはなりません.
エ:ログインアカウントの作成と削除は管理者の作業ですので, クライアント処理を変えても作業軽減にはなりません.

問 46 ＜テクノロジ系＞ E-R 図に関する記述として, 適切なものはどれか.

ア 関係データベースの表として実装することを前提に表現する.
イ 管理の対象をエンティティ及びエンティテイ間のリレーションシップとして表現する.
ウ データの生成から消滅に至るデータ操作を表現する.
エ リレーションシップは, 業務上の手順を表現する.

正解:イ

E-R 図(Entity Relationship Diagram)(10.2.2 参照)は業務で扱う情報を抽象化し, 実体(エンティティ)と実体間の関連(リレーションシップ)を表現する図です.

ア:E-R 図は業務分析や要件定義に用いられる汎用の手法であり, 関係データベースの表として実装することが前提ではありません.
ウ:**DFD(Data Flow Diagram)**(10.2.2 参照)の説明です.
エ:リレーションシップは, 業務上の手順(プロセス)ではなく, エンティティ間の関連を表現します.

問 47 ＜テクノロジ系＞ IP アドレスの自動設定をするために DHCP サーバが設置された LAN 環境の説明のうち, 適切なものはどれか.

ア　DHCP による自動設定を行う PC では，IP アドレスは自動設定できるが，サブネットマスクやデフォルトゲートウェイアドレスは自動設定できない．
イ　DHCP による自動設定を行う PC と，IP アドレスが固定の PC を混在させることはできない．
ウ　DHCP による自動設定を行う PC に，DHCP サーバのアドレスを設定しておく必要はない．
エ　一度 IP アドレスを割り当てられた PC は，その後電源が切られた期間があっても必ず同じ IP アドレスを割り当てられる．

正解：ウ

DHCP（5.3.1 参照）は IP アドレスを与えられた範囲で自動採番し，ネットワーク利用に必要な情報と共に返す TCP/IP アプリケーション層のプロトコルです．
ア：**サブネットマスク**（5.3.1 参照）や **デフォルトゲートウェイアドレス**（5.3.1 参照）も自動設定できますので誤りです．
イ：自動設定を行う PC と，IP アドレスが固定の PC を混在できますので誤りです．
エ：アドレスの有効活用のために，必ずしも同じ IP アドレスを割り当てられるとは限らないので誤りです．

16.2 第2回午前試験＜ストラテジ系＞の問題と解説

問 31　＜ストラテジ系＞　プロバイダ責任制限法において，損害賠償責任が制限されるプロバイダの行為に該当するものはどれか．ここで，"利用者"とはプロバイダに加入してサービスを利用している者とする．

ア　契約書に記載した利用者の個人情報を，本人の同意を得ずに関連会社に渡した．
イ　他のプロバイダに移転する利用者に対して，不当に高い違約金を請求した．
ウ　利用者の送信メールの内容を盗聴し，それを興味本位で他人に伝えた．
エ　利用者の電子掲示板への書込みが，他人の権利を侵害しているとは知らずに放置した．

正解：エ

プロバイダ責任制限法（2.2.5 参照）で損害賠償責任が制限されるプロバイダの行為としては，利用者の電子掲示板への書込みが他人の権利を侵害している場合に，これを利用者の許可なく削除すること，侵害の事実に気付かずに放置すること，などがあります．
アはプロバイダ責任制限法とは無関係の行為で，**個人情報保護法**（2.2.3 参照）に触れる可能性があります．
イもプロバイダ責任制限法とは無関係の行為で，消費者契約法に触れる可能性があります．

ウもプロバイダ責任制限法とは無関係の行為で，電気通信事業法に触れる可能性があります．

問 32 ＜ストラテジ系＞ 刑法の電子計算機使用詐欺罪が適用される違法行為はどれか．

ア いわゆるねずみ講方式による取引形態の Web ページを開設する．
イ インターネット上に，実際よりも良品と誤認させる商品カタログを掲載し，粗悪な商品を販売する．
ウ インターネットを経由して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．
エ 企業の Web ページを不法な手段で改変し，その企業の信用を傷つける情報を流す．

正解：ウ

刑法の **電子計算機使用詐欺罪**（2.2.4 参照）はコンピュータに虚偽情報や不正な命令を与えて，不正なデータを作成し不法な利益を得ることです．
アは無限連鎖講の防止に関する法律が適用される可能性があります．
イは不当景品類及び不当表示防止法が適用される可能性があります．
エは刑法の **電子計算機損壊等業務妨害罪**（2.2.4 参照）に触れる可能性があります．

問 33 ＜ストラテジ系＞ ″特定個人情報ファイル″の取扱いのうち，国の個人情報保護委員会が制定した″特定個人情報の適正な取扱いに関するガイドライン(事業者編)″で，認められているものはどれか．

ア 個人番号関係事務を行う必要がなくなり，かつ，法令による保存期間を経過した場合は，暗号化した上で保管する．
イ 事業者内の誰でも容易に参照できるよう，事務取扱担当者を限定せず従業員全員にアクセス権を設定する．
ウ 従業員の個人番号を含む源泉徴収票を，業務委託先の税理士に作成させる．
エ 従業員の個人番号を利用して営業成績を管理する．

正解：ウ

特定個人情報の適正な取扱いに関するガイドライン（2.2.3 参照）は，個人番号（マイナンバー）を取り扱う事業者が特定個人情報の適正な取扱いを確保するための具体的な指針を定めたものです．このガイドラインでは，従業員の個人番号を含む源泉徴収票を，業務委託先の税理士に作成させることを認めています．
アは「個人番号をできるだけ速やかに廃棄又は削除しなければならない」となっていますので誤りです．
イは「事務取扱担当者が正当なアクセス権を有する」となっていますので誤りです．
エは「利用目的を超えた個人番号の利用禁止」「利用目的を超えて個人番号を利用

する必要が生じた場合には，当初の利 用目的と相当の関連性を有すると合理的に認められる範囲内」となっていますので誤りです．

問 34 ＜ストラテジ系＞ 広告宣伝の電子メールを送信する場合，特定電子メール法に照らして適切なものはどれか．

ア 送信の許諾を通知する手段を電子メールに表示していれば，同意を得ていない不特定多数の人に電子メールを送信することができる．
イ 送信の同意を得ていない不特定多数の人に電子メールを送信する場合は，電子メールの表題部分に未承諾広告であることを明示する．
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．
エ メールアドレスを自動的に生成するプログラムを利用して電子メールを送信する場合は，送信者の氏名・連絡先を電子メールに明示する．

正解：ウ

特定電子メール法（2.2.5 参照）では，取引関係にあるなどの一定の場合を除き，**オプトイン方式**（2.2.3 参照）をとることを定めています．
アとイはオプトイン方式になっていませんので不適切です．
エの「メールアドレスを自動的に生成するプログラムを利用して電子メールを送信する」行為は不適切です．

問 35 ＜ストラテジ系＞ 不正アクセス禁止法による処罰の対象となる行為はどれか．

ア 推測が容易であるために，悪意のある攻撃者に侵入される原因となった，パスワードの実例を，情報セキュリティに関するセミナの資料に掲載した．
イ ネットサーフィンを行ったところ，意図せずに他人の利用者 ID とパスワードをダウンロードしてしまい，PC 上に保管してしまった．
ウ 標的とする人物の親族になりすまし，不正に現金を振り込ませる目的で，振込先の口座番号を指定した電子メールを送付した．
エ 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が，これまでに不正アクセスは行っていない．

正解：エ

不正アクセス禁止法（2.2.2 参照）はネットワークへの侵入，アクセス制御のための符号提供などを一律に犯罪の対象としています．よって，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時点で処罰の対象となります．
ア，イは法に触れる行為ではありません．
ウは不正アクセス禁止法ではなく刑法に触れる行為です．

問 36 ＜ストラテジ系＞ 準委任契約の説明はどれか．

ア　成果物の対価として報酬を得る契約.
イ　成果物を完成させる義務を負う契約.
ウ　善管注意義務を負って作業を受託する契約.
エ　発注者の指揮命令下で作業を行う契約.

正解:ウ

準委任契約(2.3.3 参照)は善管注意義務を負って作業を受託する契約です.
ア, イは **請負契約**(2.3.3 参照)です.
エは **労働者派遣契約**(2.3.2 参照)です.

問 48　<ストラテジ系>　BPO を説明したものはどれか.

ア　災害や事故で被害を受けても, 重要事業を中断させない, 又は可能な限り中断期間を短くする仕組みを構築すること.
イ　社内業務のうちコアビジネスでない事業に関わる業務の一部又は全部を, 外部の専門的な企業に委託すること.
ウ　製品を生産しようとするときに必要となる部品の数量や, 調達する資材の所要量, 時期を計算する生産管理手法のこと.
エ　プロジェクトを, 戦略との適合性や費用対効果, リスクといった観点から評価を行い, 情報化投資のバランスを管理し, 最適化を図ること.

正解:イ

BPO(9.2.1 参照)は業務プロセスのアウトソーシングであり, 社内業務のうち核となっていない事業に関わる業務の一部又は全部を, 外部のアウトソーシング専門企業に委託することです.
アは BCP(11.1.3 参照)です.
ウは MRP(9.2.1 参照)です.
エは **プロジェクト統合マネジメント**(6.1.2 参照)に含まれる行動です.

問 49　<ストラテジ系>　共通フレームによれば, 企画プロセスにおいて明確にするものはどれか.

ア　新しい業務の在り方や手順, 入出力情報, 業務上の責任と権限, 業務上のルールや制約などの事項.
イ　業務要件を実現するために必要なシステムの機能, システムの開発方式, システムの運用手順, 障害復旧時間などの事項.
ウ　経営・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, システム化又はシステム改善を必要とする業務上の課題などの事項.
エ　システムを構成するソフトウェアの機能及び能力, 動作のための環境条件, 外部インタフェース, 運用及び保守の方法などの要求事項.

正解：ウ

企画プロセスは 共通フレーム（10.1.1 参照）の中核を成すテクニカルプロセスにおいて「経営・事業の目的，目標を達成するために必要なシステムに 関係する要件の集合とシステム化の方針，及び，システムを実現するための実施計画を得るプロセス」と説明されています．
アは **要件定義プロセス** に該当します．
イは **システム開発プロセス** に該当します．
エは **ソフトウェア実装プロセス** に該当します．

問 50 ＜ストラテジ系＞ マトリックス組織を説明したものはどれか．

ア 業務遂行に必要な機能と利益責任を，製品別，顧客別又は地域別にもつことによって，自己完結的な経営活動が展開できる組織である．
イ 構成員が，自己の専門とする職能部門と特定の事業を遂行する部門の両方に所属する組織である．
ウ 購買・生産・販売・財務など，仕事の専門性によって機能分化された部門をもつ組織である．
エ 特定の課題の下に各部門から専門家を集めて編成し，期間と目標を定めて活動する一時的かつ柔軟な組織である．

正解：イ

マトリックス組織（11.1.1 参照）職能別または事業部制組織とプロジェクト組織の兼用で，元々所属している組織の上司とプロジェクトリーダの二つの指揮命令系統をもつのが特徴です．
アは **事業部制組織**（11.1.1 参照）です．
ウは **職能別組織**（11.1.1 参照）です．
エは **プロジェクト組織**（11.1.1 参照）です．

16.3 第2回午前試験＜マネジメント系＞の問題と解説

問 37 ＜マネジメント系＞ JIS Q 27001 に準拠して ISMS を運用している場合，内部監査について順守すべき要求事項はどれか．

ア 監査員には ISMS 認証機関が認定する研修の修了者を含まなければならない．
イ 監査責任者は代表取締役が任命しなければならない．
ウ 監査範囲は JIS Q 27001 に規定された管理策に限定しなければならない．
エ 監査プログラムには前回までの監査結果を考慮しなければならない．

正解：エ

JIS Q 27001（1.2.8 参照）は **ISMS**（1.2.8 参照）を確立，実施，維持及び継続的に改善するための要求事項を規定した国際規格です．この規格では「監査プログラムは，関連するプロセスの重要性及び前回までの監査の結果を考慮に入れなければならない」と明示しています．
ア：「監査プロセスの客観性及び公平性を確保する監査員を選定し，監査を実施する」とありますが，研修の修了者であることは求められていません．
イ：監査責任者の任命に関する要求事項はありません．
ウ：「各監査について，監査基準及び監査範囲を明確にする」とありますが，JIS Q 27001 に規定された管理策に限定することは求められていません．

問 38 ＜マネジメント系＞ 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はどれか．

ア コンティンジェンシープラン
イ サンプリング
ウ ディジタルフォレンジックス
エ ベンチマーキング

正解：ウ

ディジタルフォレンジックス（1.4.2 参照）はデジタル鑑識・証拠保全のことで，不正アクセスや情報漏洩などの技術的・人的セキュリティな事件の発生時に，原因の究明や調査に必要な情報の法的な証拠性を明らかにする手段・技術の総称です．
アの **コンティンジェンシープラン**（1.2.6 参照）は緊急時対応計画です．
イの **サンプリング**（11.2.1 参照）は標本化です．
エの **ベンチマーキング**（11.2.1 参照）は相対評価です．

問 39 ＜マネジメント系＞ 事業継続計画(BCP)について監査を実施した結果，適切な状況と判断されるものはどれか．

ア 従業員の緊急連絡先リストを作成し，最新版に更新している．
イ 重要書類は複製せずに 1 か所で集中保管している．
ウ 全ての業務について，優先順位なしに同一水準の BCP を策定している．
エ 平時には BCP を従業員に非公開としている．

正解：ア

事業継続計画(BCP)（11.1.3 参照）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．この中には従業員の緊急連絡先リストの作成と，これを常に最新版に更新することを含むべきです．
イは「複製して同時に被災することのない遠隔地に分散保管する」のが適切です．

ウは「優先順位を検討し，それぞれに必要な水準の BCP を策定する」のが適切です．
エは「BCP は従業員等に公開し周知を図る」のが適切です．

問 40 ＜マネジメント系＞ ″情報セキュリティ監査基準″に関する記述のうち，最も適切なものはどれか．

ア ″情報セキュリティ監査基準″は情報セキュリティマネジメントシステムの国際規格と同一の内容で策定され，更新されている．
イ 情報セキュリティ監査人は，他の専門家の支援を受けてはならないとしている．
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″を用いることとしている．
エ 情報セキュリティ監査は高度な技術的専門性が求められるので，監査人に独立性は不要としている．

正解：ウ

情報セキュリティ監査基準（8.1.2 参照）は情報セキュリティの維持を目的として，情報セキュリティ管理の必要な事項を定めたものです．情報セキュリティ監査は「情報セキュリティ管理基準を監査上の判断の尺度として用い，監査対象が情報セキュリティ管理基準に準拠しているかどうかという視点で行われることを原則とする」と記載されています．
ア：**情報セキュリティ管理基準**（8.1.2 参照）は情報セキュリティマネジメントに関わる国際規格（ISO 27001，27002）に準拠していますが，情報セキュリティ監査基準はそうではありません．
イ：「情報セキュリティ監査人は，情報セキュリティ監査の目的達成上，必要かつ適切と判断される場合には，他の専門職による支援を考慮しなければならない」とありますので不適切です．
エ：監査人には外観上の独立性と精神上の独立性が求められていますので不適切です．

問 41 ＜マネジメント系＞ システムの移行テストを実施する主要な目的はどれか．

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．
イ 既存システムのデータベースのコピーを利用して，新システムでも十分な性能が得られることを確認する．
ウ 既存のプログラムと新たに開発したプログラムとのインタフェースの整合性を確認する．
エ 新システムが要求されたすべての機能を満たしていることを確認する．

正解：ア

移行テスト(7.2.2 参照)は新しいシステムやサービスへ，従来のものから切り替えるにあたっての事前テストです．確実に切り替えられることに加えて，切替直後の業務の効率低下の影響などを考えたテストを行います．
イは新規システムの性能テストの説明であり，移行テストを実施する主要な目的としては不適切です．
ウはシステム結合テストの説明であり，移行テストを実施する主要な目的としては不適切です．
エはシステムテストにおける機能テストの説明です．

問 42 ＜マネジメント系＞ あるデータセンタでは，受発注管理システムの運用サービスを提供している．次の"受発注管理システムの運用中の事象"において，インシデントに該当するものはどれか．

〔受発注管理システムの運用中の事象〕 夜間バッチ処理において，注文トランザクションデータから注文書を出力するプログラムが異常終了した．異常終了を検知した運用担当者から連絡を受けた保守担当者は，緊急出社してサービスを回復し，後日，異常終了の原因となったプログラムの誤りを修正した．

ア 異常終了の検知
イ プログラムの誤り
ウ プログラムの異常終了
エ 保守担当者の緊急出社

正解：ウ

インシデント(7.3.6 参照)はサービスの質を低下させる，または，低下させる可能性がある事象ですので「注文書を出力するプログラムが異常終了した」ことが該当します．
アはインシデントの検知であり，インシデントそのものではありません．
イはインシデントの原因であり，インシデントそのものではありません．
エはインシデントへの対応であり，インシデントそのものではありません．

問 43 ＜マネジメント系＞ メールサーバのディスクに障害が発生して多数の電子メールが消失した．消失した電子メールの復旧を試みたが，2 週間ごとに行っている磁気テープへのフルバックアップしかなかったので，最後のフルバックアップ以降 1 週間分の電子メールが回復できなかった．そこで，今後は前日の状態までには復旧できるようにしたい．対応策として，適切なものはどれか．

ア 2 週間ごとの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．
イ 電子メールを複数のディスクに分散して蓄積する．
ウ バックアップ方法は今のままとして，メールサーバのディスクをミラーリングするようにし，信頼性を高める．

エ　毎日，メールサーバのディスクにフルバックアップを行い，2 週間ごとに，バックアップしたデータを磁気テープにコピーして保管する．

正解：ア

フルバックアップ（4.4.1 参照）を毎日行うのが理想ですが，所要時間や磁気テープなどの記憶メディアの量を勘案して，**差分バックアップ**（4.4.1 参照）を併用するのが一般的です．毎日，差分バックアップを行えば「前日の状態までには復旧できる」ようになります．
イは障害が発生したディスクにあるメールのみを消失することで済みますが，「前日の状態までには復旧できる」こととは無関係です．
ウはディスクの障害による電子メールの消失を完全に防止できますが，目的は「今後は前日の状態までには復旧できるようにしたい」ことですので，**ミラーリング**（1.4.4 参照）のコストを考慮すると不適切です．
エは個々のメールを「前日の状態までには復旧できる」ようになりますが，フルバックアップがメールサーバのディスクにありますので，ディスクに障害が発生したときに，バックアップも含めて失われてしまい，磁気テープに 2 週間前にコピーしたメールしか復旧できませんので不適切です．

問 44　＜マネジメント系＞　プロジェクトに関わるステークホルダの説明のうち，適切なものはどれか．

ア　組織の外部にいることはなく，組織の内部に属している．
イ　プロジェクトの成果が，自らの利益になる者と不利益になる者がいる．
ウ　プロジェクトへの関与が間接的なものにとどまることはなく，プロジェクトには直接参加する．
エ　プロジェクトマネージャのように，個人として特定できることが必要である．

正解：イ

ステークホルダ（6.1.3 参照）は利害関係者であり，プロジェクトの成果が自らの利益になる者だけを指すわけではありません．
ア：得意先のように組織の外部にいるステークホルダもあり，誤りです．
ウ：株主のようにプロジェクトへの関与が間接的なものにとどまるステークホルダもあり，誤りです．
エ：周辺住民のように個人として特定できないステークホルダもあり，誤りです．