問 1

正解 □ 完璧 □ 直前チェック □

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が識別できるので，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カードの配送には同封せず，別経路で利用者に知らせる。

問 2

正解 □ 完璧 □ 直前チェック □

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。

問 3

正解 □ 完璧 □ 直前チェック □

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　電子政府推進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。

問1　エ

解説　**PIN**（Personal Identification Number）は，パスワードや暗証番号など，個人を識別するための番号のことである。

ア：セキュリティを向上させるために，全て異なるPINを用いるべきである。
イ：紛失したICカードの失効処理を行ってから，新たなICカードの発行を行う。紛失したICカードを利用して新たなICカードの操作をできないようにするためである。
ウ：ICカードが不正に使用されるリスクを避けるために，ICカードの刻印情報をPINに使用するべきではない。
エ：ICカードの配送時に，不正にPINを利用されるのを避けるため別経路で利用者に知らせる。

問2　イ

解説　**JIS Q 31000:2010**は，全ての組織，全てのリスクに適用できる原則及び一般的な指針を示す。枠組みとリスクマネジメントプロセスの両方を継続的に改善していく体系が提示されている。

地震保険に加入するという対応は，事象が発生したときに他者とリスクを共有することである。

ア：地震保険に加入することで，リスクが増加することはない。
ウ：リスク源はリスクを生じさせることを潜在的に持っている要素である。地震保険に加入しても地震によるリスクを除去できない。
エ：地震発生の有無は，意思決定によって変化することではないため回避できない。

問3　ウ

解説　**JPCERT/CC**（Japan Computer Emergency Response Team Coordination Center）は，インターネットを介して発生する侵入やサービス妨害などのコンピュータセキュリティインシデントについて，日本国内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などを，技術的な立場から行っている。特定の政府機関や企業からは独立した中立の組織として，日本における情報セキュリティ対策活動を行っている組織である。

ア：**日本工業標準調査会**（JIS：Japanese Industrial Standards Committee）の説明である。
イ：**暗号技術検討会及び関連委員会**（CRYPTREC：Cryptography Research and Evaluation Committees）の説明である。
エ：**内閣サイバーセキュリティセンター**（NISC：National center of Incident readiness and Strategy for Cybersecurity）の説明である。

問 4

正解 □ 完璧 □ 直前チェック □

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

問 5

正解 □ 完璧 □ 直前チェック □

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。

問 6

正解 □ 完璧 □ 直前チェック □

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。

問4　ウ

解説　**JVN**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**である。JPCERT/CCと，独立行政法人情報処理推進機構（IPA）が共同運営している。
ア：**CVSS**（Common Vulnerability Scoring System）の説明である。
イ：**CVE**（Common Vulnerabilities and Exposures）の説明である。
エ：**CSIRT**（Computer Security Incident Response Team）の説明である。

問5　ア

解説　システムの**可用性**（availability）とは，システムの利用者が必要とするときにシステムを使用できるかどうかに関する性能の評価である。評価指標の一つに稼働率がある。
ア：正しい。ストレージを二重化することで，障害発生時の停止を軽減することは可用性を向上させることにつながる。
イ，ウ，エ：セキュリティ上のリスク軽減となるが，可用性は変わらない。

問6　ア

解説　**ベースラインアプローチ**とは，すでにあるガイドラインや規定をもとに，確保すべき一定のセキュリティ対策のレベルを設定し，セキュリティレベルの到達度合いを分析してリスクを評価する手法である。システム全体のリスクを短時間で網羅的にチェックできるメリットがある。チェック内容さえ決定すれば，担当者の力量にあまり依存しないでリスク評価ができる。デメリットは，未知のリスク，業界・業種・業能特有のリスクに対応できないことである。
ア：正しい。基準となる対策と現状のギャップを分析することは，ベースラインアプローチの手法である。
イ：ベースラインアプローチは，担当者の経験に左右されにくい。
ウ：ベースラインアプローチは，情報資産単位ではなく，組織などの共通の資産をリスク分析する。
エ：ベースラインアプローチは，一定の基準で実施する形のため，分析精度の向上を図るものではない。効率化を主としている。

問 7 正解 完璧 直前チェック

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

問 8 正解 完璧 直前チェック

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

問7　ウ

解説　IDの発行・削除が申請に基づき行われるとしても，次のように削除の申請が行われない場合が想定される。

組織の所属者が増員されると，IDの発行を申請しなければ業務ができないため必ず申請を行う。しかし，退職者のID削除申請は，申請しなくても業務が継続できるため申請が行われないことがある。

ア：現在の所属名簿とIDの削除申請の比較では，だれが所属部門から退職したのかがわからないため削除漏れは検出できない。
イ：現在の利用者IDの一覧がなければ，だれを削除する必要があるかわからない。
ウ：正しい。
エ：利用者IDの一覧とIDの削除申請の比較では，だれが所属部門から退職したのかがわからないため削除漏れは検出できない。

問8　イ

解説　**JIS Q 27000**は，情報セキュリティのためのマネジメントシステム規格で，**ISMS**（Information Security Management Systems）に関連する用語及び定義について規定している。

リスク評価は，リスク及びその大きさが，受容可能か又は許容可能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である。

ア：**管理策**（control）の説明である。
イ：**リスク評価**（risk evaluation）の説明である。
ウ：**リスク分析**（risk analysis）の説明である。
エ：**リスク特定**（risk identification）の説明である。

問 9 正解 完璧 直前チェック

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

問 10 正解 完璧 直前チェック

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。

問 11 正解 完璧 直前チェック

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。

問9　エ

解説　**JIS Q 31000:2010**は，リスクマネジメントを効果的なものにするために満たされる必要のあるいくつかの原則を規定している。この規格は，リスクの運用管理のためのプロセスを組織の全体的な統治，戦略及び計画策定，運用管理，報告プロセス，方針，価値観並びに文化の中に統合することを目的とした枠組みを，組織が構築，実践及び継続的に改善することを推奨している。

残留リスク（residual risk）は，リスク対応後に残るリスクである。

ア，ウ：残留リスクは，対応後のリスクである。不備の発見ができないリスクではない。
イ：**リスク源**（risk source）の要素である。リスク源とは，それ自体又はほかとの組合せによって，リスクを生じさせる力を本来潜在的にもっている要素。有形の場合も無形の場合もある。

問10　エ

解説　**JIS Q 27002**はISMS（Information Security Management System）についての標準である。情報資産に危害を与える可能性をもつ，好ましくない偶発的事故の潜在的な原因を脅威と呼ぶ。ある脅威が情報資産の脆弱性を利用して資産への損失あるいは損害を与える可能性のことを**リスク**と呼ぶ。

ア，イ，ウ：セキュリティ強化の観点として正しい内容である。
エ：正規従業員と同様の派遣従業員の教育が実施されていない場合は，セキュリティリスクとなるため改善が必要である。

問11　エ

解説　組織における**内部不正防止ガイドライン**は，これまで内部不正対策について考慮されていない又は，対応方法が不明という企業に対して，内部不正対策の整備を可能とすることを目指したガイドラインである。また，ガイドラインでは，内部不正防止だけではなく，発生してしまった際の早期発見・拡大防止をも視野に入れた構成となっている。

ア：システム管理者間の情報交換の制限は，内部不正と関連しない。
イ：システム管理者の操作履歴は，本人以外が確認することで内部不正を防止できる。
ウ：長期休暇取得と内部不正は関連しない。
エ：正しい。夜間・休日の単独作業は内部不正となる可能性がある。

問 12

正解 □ 完璧 □ 直前チェック □

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。

問 13

正解 □ 完璧 □ 直前チェック □

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，情報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 Content Management）

ウ　LTE（Long Term Evolution）

エ　MDM（Mobile Device Management）

問12　エ

解説　**ボットネット**は，マルウェアに感染したコンピュータで構成されるネットワークである。マルウェア同士が不正情報を通信し，データ交換を行う。

C&Cサーバは，ボットネット内で，マルウェアに感染したコンピュータに不正な操作を命令（Command）することや，制御（Control）を行うサーバである。Commandと，Controlの頭文字から，C&Cサーバと呼ばれる。

問13　エ

解説　**MDM**はスマートフォンやタブレット端末など，持ち運ぶことができる高性能端末のセキュリティを管理するために用いられる。端末の状態・利用・アクセス権の管理がそれにあたる。

端末状態の管理：端末紛失時のロックや設定の一元管理の機能である。

端末利用の管理：カメラ機能の禁止，特定のアプリケーション利用禁止などの機能である。

アクセス権の管理：データやアプリケーションへのアクセスを管理する機能である。

ア：**BYOD**：個人所有の端末を業務利用することである。企業は，社員用に端末を用意するコストを低減するメリットがあり，個人は，携帯電話やスマートフォンを個人用・会社用と複数台もち歩く必要がなくなるなど，管理面でのメリットがある。

イ：**ECM**：業務に関連するコンテンツや文書を収集・管理・蓄積・保護・配布するための技術やツール，手法のことである。

ウ：**LTE**：第3世代（3G）携帯電話のデータ通信を高速化した規格である。3.9Gともいわれ，第4世代（4G）になるためのつなぎの規格として位置付けられている。近年では，LTEは4Gの一種と解釈するのが一般的になっている。

問 14 正解 完璧 直前チェック

サーバにバックドアを作り，サーバ内での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

問 15 正解 完璧 直前チェック

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。

問 16 正解 完璧 直前チェック

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。

問14　イ

解説

RFID (Radio Frequency IDentification)：微小な無線チップを用いてバーコードと同様の情報を提供する仕組みである。複数のRFIDを同時に識別することができる。物流におけるタグや交通機関で用いるプリペイドカード，IC定期券などに応用されている。

rootkit：クラッカがセキュリティホールなどを利用して不正侵入した後に，侵入の隠ぺい，バックドアの確保，踏み台による攻撃などに用いる機能をまとめたツール群のことである。

TKIP (Temporal Key Integrity Protocol)：無線LANの暗号化方式の一つ。一定時間経過後に暗号鍵を自動的に変更する機能である。

web beacon (webビーコン)：利用者のアクセス履歴を収集するために，Webページ やHTMLメールで利用される小さな画像(およそ1×1ドット)のことである。Webページにアクセスすると，利用者側からサーバ側へ画像データの要求が送信される。そのWebページにwebビーコンが埋め込まれていると，その要求がサーバ側に記録される。サーバ側では，利用者に知られずにアクセス履歴を収集することができる。

問15　イ

解説 **SIEM**は，サーバやネットワーク機器のログを集め一括で管理・分析し，セキュリティ上の脅威を発見・通知する仕組みである。

ア：**DLP** (Data Loss Prevention) の説明である。
ウ：**インシデント管理**の説明である。
エ：**NIDS** (Network Intrusion Detection System) の説明である。

問16　エ

解説 **SPF**は，差出人のメールアドレスが他のドメインになりすましていないかどうかを検出する，電子メールにおける送信ドメイン認証の仕組み。

ア：**中間者攻撃**は，(Man-in-the-Middle) 攻撃と呼ばれる。
イ：**IDS** (Intrusion Detection System) の機能である。
ウ：**NIDS** (Network Intrusion Detection System) の機能である。
IDSはサーバや，PCへの侵入検知，NIDSはネットワークのパケットを参照して侵入を検知する。

問 17 正解 完璧 直前チェック

次の電子メールの環境を用いて，機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ブ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。

問 18 正解 完璧 直前チェック

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。

問17　イ

解説　機密情報を含むファイルを電子メールで添付して社外に送信する場合は，情報漏洩のセキュリティリスクを回避する必要がある。
Webメールの利用：PCにインストールされている，メールソフトと同等の機能であると考えてよい。
Webブラウザの通信：Webサーバとの通信は，HTTPSで行っている。そのためPCとメール送信のWebサーバ間は暗号化されている。HTTPの場合は暗号化されないため注意が必要である。
宛先ドメイン：SMTPとPOP3を使用しているため，暗号化されていない。
IP層以下：暗号化していない。
ア，エ：ファイルを平文のまま添付すると宛先ドメインのメールサーバは暗号化していないため情報漏洩のセキュリティリスクがある。
イ：正しい。
ウ：Base64形式は，バイナリファイルをテキスト化するためのエンコードで，暗号化機能はなく，情報漏洩のセキュリティリスクがある。

問18　エ

解説　**ビヘイビア法**は，ウイルスの感染や発病による異常な振る舞い（システム領域の書込み動作や，通信量の増加など）を監視し，ウイルスを検出する手法である。ビヘイビア法の特徴としては，システム上の異常な振る舞いを監視しているため，既存のウイルスの亜種や未知のウイルスであっても検出できる。
ア，ウ：**チェックサム法**の説明である。
イ：**コンペア法**の説明である。

問 19 正解 完璧 直前チェック

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）

問 20 正解 完璧 直前チェック

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

問19　イ

解説　時刻同期用の通信プロトコルは，**NTP**（Network Time Protocol）である。

FTP（File Transfer Protocol）：インターネットなどのTCP/IP環境でファイルを転送する際に使われるプロトコルである。

SMTP（Simple Mail Transfer Protocol）：電子メールを転送するためのプロトコル。サーバ間のメールの転送やクライアントがサーバにメールを送信する際に使われる。

SNMP（Simple Network Management Protocol）：LANの構成機器の動作や状態を監視・管理・通知するためのプロトコルである。ネットワーク上にある機器でSNMPエージェントを動作させると，SNMPマネージャで一括管理可能となる。管理対象の機器は，管理情報データベースMIB（Management Information Base）をもつ。対象となる機器は，L2，L3スイッチのネットワーク機器だけでなく，サーバや，ストレージ装置など，SNMPに対応している危機は全て管理可能となる。

問20　ア

解説　**CAPTCHA**（Completely Automated Public Turing test to tell Computers and Humans Apart）：わざとゆがんだ文字を表示しその文字の入力を促すことによって，人間のみが電子掲示板やブログなどへの投稿ができるようにすることで，プログラムによる大量投稿や迷惑なコメントの掲載を防止するための技術である。

QRコード：小さな正方形の点を縦横同じ数だけ並べたマトリックス型2次元コード。携帯電話やスマートフォンのアドレス読み取り機能や工場の部品管理などに利用されている。

短縮URL：短いURLを入力することで，長い文字列のURLに対して，リダイレクトし，本来の長いURLに接続することである。

トラックバックping：ブログの主要機能の一つであるトラックバックの設置をリンク先へ通知する機能である。相手の記事へのリンク設定などの際に通知される機能である。

問 21 正解 完璧 直前チェック

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

問 22 正解 完璧 直前チェック

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をする。
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，データの改ざんや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ないページに直接ジャンプする。

問21　ア

解説　情報セキュリティでは，重要だと考える「情報資産」に対して，機密を守り（**機密性**），誤った使用や改ざんを防ぎ（**完全性**），必要なときに安全で確実に利用できる（**可用性**）ことが必要である。

機密性（Confidentiality）：認可されていない個人，エンティティまたはプロセスに対して，情報を使用不可または非公開にする特性。

完全性（Integrity）：情報が常に正確かつ一貫性を維持していることを表す特性。

可用性（Availability）：認可されたエンティティが要求したとき，アクセス及び使用が可能である特性。

ア：完全性への脅威である。
イ，エ：機密性への脅威である。
ウ：可用性への脅威である。

問22　ア

解説　**クロスサイトスクリプティング**は，動的にWebページを生成するアプリケーションの脆弱性を利用した攻撃である。たとえば，攻撃者によって掲示板に悪意のスクリプトコードが書き込まれた場合に，スクリプトコードをチェックせずに掲示板に載せることで，その掲示板にアクセスしたブラウザが悪意のスクリプトを実行する。対策としては，入力されたデータをチェックして，スクリプトの文字列を置き換えて無効化するサニタイジングが有効である。

イ：**クラッキング**の説明である。
ウ：**バッファオーバフロー攻撃**の説明である。
エ：**ディレクトリトラバーサル攻撃**の説明である。

問 23

正解 □ 完璧 □ 直前チェック □

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。

問 24

正解 □ 完璧 □ 直前チェック □

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。

問 25

正解 □ 完璧 □ 直前チェック □

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

問23　ア

解説　**サイバーセキュリティ戦略**は，2014年11月に制定された「**サイバーセキュリティ基本法**」が位置づけとなり，国や地方公共団体といった関係者の責務を明確化するとともに，サイバーセキュリティ政策に係る政府の司令塔としてサイバーセキュリティ戦略本部を位置付け，国の行政機関に対する勧告権等の権限を付与したものである。5つの基本原則は，「**情報の自由な流通の確保**」「**法の支配**」「**開放性**」「**自立性**」「**多様な主体の連携**」からなる。

ア：正しい。**開放性**に該当する。
イ：国家が全て代替えすることはできない。**自立性**に該当する。
ウ：発信された情報は，不当に検閲されてはならない。**情報の自由な流通の確保**に該当する。
エ：サイバー空間においても法の支配が貫徹される。**法の支配**に該当する。

多様な主体の連携：政府に限らず，重要インフラ事業者，企業，個人といったサイバー空間に関係する全てのステークホルダーが，サイバーセキュリティに係るビジョンを共有し，それぞれの役割や責務を果たす。

問24　イ

解説

ア：**ショルダーハッキング**の説明である。
イ：正しい。**スクリプトキディ**の説明である。
ウ：**ソーシャルエンジニアリング**の説明である。
エ：**スパムメール**の説明である。

問25　ア

解説　コンピュータ内部からではなく，組織内部の人間から情報を入手する不正な行為を**ソーシャルエンジニアリング**と呼ぶ。

トロイの木馬：有益なソフトを装って悪意のあるプログラムを実行させる。
踏み台攻撃：本当の攻撃元を隠すために，他人のコンピュータを用いて攻撃する攻撃手法である。
ブルートフォース（総当たり）攻撃：考えられるパターンを手当たり次第に試す暗号読解法の一種である。

問 26 正解 完璧 直前チェック

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　想定し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によってタブレット端末へのログインを試行する。

問 27 正解 完璧 直前チェック

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

問 28 正解 完璧 直前チェック

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　送信元のメールアドレスがECサイトで利用されているアドレスである。
イ　送信元の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は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。

春 秋

問26　ウ

解説　**パスワードリスト攻撃**は，複数サイトで同一のIDとパスワードを使っている利用者がいることを前提とした攻撃手法である。不正に入手したサイトのIDとパスワードの一覧表を用いてログインを不正に行う。
ア：**辞書攻撃**の説明である。
イ：**事前計算攻撃**（**レインボーアタック**）の説明である。
エ：**ピクチャパスワード**は，画面をなぞることで認証するパスワードである。なぞるパターンを録画することでログインすることができる。

問27　エ

解説　**ランサムウェア**とは，マルウェアの一種で，PCのネットワークアクセスを制限・遮断するコンピュータウイルスである。制限・遮断の解除と引き換えに身代金（ランサム）を要求することから，ランサムウェアと呼ばれる。
ア：**バックドア**となるマルウェアの説明である。
イ：**情報漏洩**を行うマルウェアの説明である。
ウ：**キーロガー**によって操作を盗み出すマルウェアの説明である。

問28　ウ

解説　**なりすましメール**ではないことを明確に証明できる方法は，メールに信頼できる組織から発行された**ディジタル証明書**がついている場合となる。
ア，イ：送信元メールアドレスやドメインは偽装可能である。
エ：テキスト形式で書かれた署名がECサイトのものであったとしても，偽装されている可能性がある。

問 29 正解 完璧 直前チェック

PKI（公開鍵基盤）における認証局が果たす役割はどれか。

ア　共通鍵を生成する。
イ　公開鍵を利用してデータを暗号化する。
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。

問 30 正解 完璧 直前チェック

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

問 31 正解 完璧 直前チェック

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。

問29　ウ

解説　**PKI**（Public Key Infrastructure：公開鍵基盤）はインターネット上で本人であることを証明するもので，公開鍵と所有者の対応付けを保証する証明書を認証局が発行する。信頼できる認証局が発行した証明書によって，公開鍵の正当性が保証される。**認証局**（CA：Certificate Authority）が電子証明書を発行し，管理する。

ア，イ：認証局は，ディジタル証明書を発行する。

ウ：失効したディジタル証明書の一覧は，**CRL**（Certificate Revocation List）と呼ばれる。有効期限内のディジタル証明書のうち破棄されているディジタル証明書と破棄された日時の対応が提示される。よって正解となる。

エ：認証局は，データ改ざんの検証は行わない。

問30　ウ

解説　**コモンクライテリア**（CC：Common Criteria）は，ISO/IEC 15408で規格化されている。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及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ある。情報技術に関連した製品のセキュリティ機能の適切性，確実性を第三者機関が評価し，その結果を公的に認証する。

ISO 9001：提供する製品やサービスの品質を一定に保つためのマネジメントを実現する規格である。

ISO 14004：環境マネジメントシステムを確立・実施・維持・改善することに関する，組織のための指針である。

ISO/IEC 27005：情報セキュリティ管理とリスク管理プロセスに係わる作業を規格化したガイドラインである。

問31　エ

解説　**プロバイダ責任制限法**とは，インターネット上でプライバシーや著作権の侵害が発生した場合に，プロバイダが負うべき責任や義務の範囲を定めたものである。プロバイダだけでなく，掲示板の運営者なども同様の責任と義務を負う。

ア，ウ：個人情報保護法，不正アクセス禁止法などの法律に違反する可能性が高い。

イ：他のプロバイダへの不当な違約金は，刑法や民法などに抵触する可能性が高い。

エ：正しい。

問 32 正解 完璧 直前チェック

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ページを不正な手段によって改変し，その企業の信用を傷つける情報を流す。

問 33 正解 完璧 直前チェック

“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，事業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。

問32　ウ

解説　**電子計算機使用詐欺罪**は，電子計算機に虚偽の情報や不正な指令を与えて財産上不法の利益を得たり，他人に利益を与えたりする行為である。銀行のシステムに虚偽の情報を与え，違法な振込みを行うことがこれに該当する。

ア：ねずみ講は，無限連鎖講の防止に関する法律に該当する。
イ：特定商取引に関する法律に該当する。
エ：**電子計算機損壊等業務妨害罪**に該当する。Webページの改ざんがなく侵入のみの場合は，**不正アクセス禁止法**違反となる。

問33　ウ

解説　**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）**は，「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」いわゆる**番号法**での**個人番号（マイナンバー）**の取扱いに関するガイドラインである。特定個人情報ファイルは，マイナンバーを含む個人情報ファイルをいう。

ア：特定個人情報ファイルは，保存期間を経過した場合には，速やかに廃棄又は削除しなければならない。
イ：特定個人情報ファイルを扱う担当者は，適切なアクセス制御を行う必要がある。
ウ：特定個人情報ファイルは，法令に基づき行う従業員等の源泉徴収票作成事務，健康保険・厚生年金保険被保険者資格取得届作成事務等に限って，特定個人情報ファイルを作成することができる。これらの場合を除き特定個人情報ファイルを作成してはならない。よって正解。
エ：個人の営業成績を管理するために，マイナンバーを利用することはできない。

問 34

正解 □ 完璧 □ 直前チェック □

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。

問 35

正解 □ 完璧 □ 直前チェック □

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。

問 36

正解 □ 完璧 □ 直前チェック □

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

問34　ウ

解説　**特定電子メール法**は，正式には「**特定電子メールの送信の適正化等に関する法律**」という。目的は「一時に多数の者に対してされる特定電子メールの送信等による電子メールの送受信上の支障を防止する必要性が生じていることにかんがみ，特定電子メールの送信の適正化のための措置等を定めることにより，電子メールの利用についての良好な環境の整備を図り，もって高度情報通信社会の健全な発展に寄与すること」である。

ア，イ，エ：同意を得ていない場合，不特定多数にメールを送信してはならない。特定電子メール法施行時には，未承諾公告を明示することで送信可能であったが，法律が改正され未承諾公告の表示での配信も不可となった。また，送信者の連絡先や，受信拒否ができることなどの記載を必須項目としている。

問35　エ

解説　**不正アクセス禁止法**は，コンピュータの不正利用を禁止する法律。アクセス制御機能を有するコンピュータに対して，インターネットなどを通じて他人のID，パスワードなどを入力し（他人になりすまし）て不正に利用する行為や，セキュリティホール（プログラムの不備など）を突いて不正に利用する行為およびその準備行為が禁止されている。

ア：すでに使用されていないパスワードを実例として載せることは可能である。
イ：意図せずにダウンロードした場合は，処罰の対象とならない。
ウ：**電子計算機使用詐欺罪**が適用対象となる。
エ：正しい。不正アクセスを目的として他人のID，パスワード取得した場合，不正に利用していなくても不正アクセス禁止法違反となる。

問36　ウ

解説　**準委任契約**は支援契約とも呼ばれる。一般に，明確な成果物を提示することのできないコンサルタント契約や顧問契約などが該当する。明確な成果物を提示し得ないので，役務を完成して引き渡す責任はない。コンサルタントや顧問業務など，任された役割を行う契約となる。

ア，イ：**請負契約**の説明である。
ウ：正しい。**準委任契約**の説明である。
エ：**労働者派遣契約**の説明である。

問 37 正解 完璧 直前チェック

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認証期間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。

問 38 正解 完璧 直前チェック

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

問 39 正解 完璧 直前チェック

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　重要事項は複製せずに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。

春
秋

問37　エ

解説　**JIS Q 27001**は，情報セキュリティマネジメントシステム（ISMS）の規格である。組織のマネジメントとして，自らのリスクアセスメントにより必要なセキュリティレベルを決め，システムを運用することである。内部監査を行う場合，前回までの監査結果を考慮し実施する必要がある。

ア：ISMSの内部監査員は，研修の終了を問わず任命できる。
イ：監査責任者は，経営者が任命するが，代表取締役である必要はない。
ウ：監査範囲は，組織の情報セキュリティマネジメント対する取り組みとなるため，JIS Q 27001の範囲外の内容を追加することもできる。

問38　ウ

解説

コンティンジェンシープラン（緊急時対応計画，非常事態対応計画）：企業内の全システムを復旧させる必要はない。重要度（緊急事態発生時予想損害額），対応コストを考慮して復旧させるシステムを選択し，有効性の高い対策を検討する。

サンプリング：証拠の中でいくつかのサンプルを抽出し検査する手法。全件検査しないため，検査では見つからない内容が内在する可能性がある。

ディジタルフォレンジックス：パソコンやサーバなどのコンピュータ機器が犯罪や裁判で証拠となりえるときにデータを保全し賠償などに備えることや，内容を分析し，鑑定するための手段や技術である。

ベンチマーキング：基準となる指標などと比較して監査結果を抽出し，改善していく方法である。システム監査基準等を用いる場合がある。

問39　ア

解説　**事業継続計画（BCP**：Business Continuity Plan）は，自然災害，伝染病，停電などによる都市機能の麻痺や情報セキュリティインシデントなどが発生した際に，事業を継続できるように必要な組織体制対策をあらかじめ決めておくことである。経営方針や事業継続に対する考え方にもよるが，事業継続ガイドラインを作成し，影響度評価の結果や取引先および行政との関係，社会的使命等を踏まえ，企業にとってその重要業務の常識が許されると考えられる復旧目標時間などを定義する。

ア：緊急連絡先の作成と，最新版への更新は，監査結果として正しいと判断できる。
イ：重要書類を複製せずに1か所で集中管理している場合，消失などのリスクがある。
ウ：優先度なしの同一水準でBCPを策定している場合は，業務の重要度，復旧時間の判断ができないため不適切である。
エ：BCPは常時公開し，訓練などを実施すべきである。

問 40 正解 完璧 直前チェック

“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。

問 41 正解 完璧 直前チェック

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 既存システムの実データ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 既存の他システム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，要求された全ての機能を満たしていることを確認する。

問 42 正解 完璧 直前チェック

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

問40 ウ

解説 **情報セキュリティ監査基準**は，情報セキュリティに係るリスクマネジメントが効率的に実施されるよう，リスクマネジメントに基づくコントロールの整備・運用の状況を評価する。
ア：情報セキュリティ監査基準は，経済産業省から発行されているため，情報セキュリティマネジメントシステムの国際規格とは別である。
イ：情報セキュリティ監査人は，他の専門家を招集し，支援を受け監査することができる。
ウ：正しい。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。
エ：監査人は，被監査部門を客観的に評価する者としての立場を堅持するために，**独立性**が必要である。

問41 ア

解説 **移行テスト**の目的は，一般的に既存システムから新システムへの移行の際にトラブルの発生要因をチェックし，作業手順を明確化することである。安全性・効率性の観点から，切替え手順や問題を確認することは正しい。
イ：新システムの性能テストは，移行テストの前に検証すべきである。
ウ：新規機能追加は，開発段階でテストする。
エ：ユーザの要求仕様のチェックは，移行時に行うものではない。

問42 ウ

解説 **インシデント**とは，サービスの品質を阻害することや，阻害する可能性のある事象のことをいう。インシデント管理とは，IT サービスの利用者が何らかの理由によりサービスを利用できない状態にあるとき，サービスの利用を早期に回復するための運用管理プロセスである。
ア：**イベント**に該当する。
イ：**プログラムのバグ**に該当する。
ウ：**インシデント**に該当する。
エ：**緊急保守対応**に該当する。

問 43

正解 □ 完璧 □ 直前チェック □

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。

問 44

正解 □ 完璧 □ 直前チェック □

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。

問 45

正解 □ 完璧 □ 直前チェック □

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　サーバが故障したときの復旧
ウ　データベースの構築　　エ　ログインアカウントの作成と削除

問43　ア

解説　前日の状態までに復旧できるようにするには，バックアップを日次で実行する必要がある。
ア：2週間分のフルバックアップと，毎日差分バックアップを行うことで前日まで復旧できる。よって適切である。
イ：複数のディスクに分散しても，データが消えた場合前日のデータを戻すことはできない。
ウ：ディスクのミラーリングは，ディスク障害に備えた対策であるが，データ消失時はバックアップ方法が変わらないため，前日のデータを戻すことはできない。
エ：メールサーバのディスクへのバックアップは，ディスクが故障した場合消失するため対応は誤りである。

問44　イ

解説　**ステークホルダ**：利害関係者のこと。プロジェクトに関わるステークホルダにはプロジェクトの委託先（組織の外部の場合もある）やプロジェクトの成果によって利益を得る者，不利益を被る者が該当する。ステークホルダの広義には株主，消費者（顧客），従業員，得意先，地域社会などが挙げられる。
ア：組織の外部にいることも多い。たとえば，プロジェクトの一部業務を委託するケース。
ウ：間接的な関与もある。たとえば，利用者として要望するケース。
エ：ステークホルダは組織（集団）の場合もあるので必ずしも個人として特定できなくてもよい。

問45　ア

解説　本問は，ユーザがアプリケーションを利用する際に，Webブラウザでアクセスする場合と，専用アプリケーションをインストールして実行する場合を想定している。一般的に，Webブラウザはパソコンにあらかじめインストールされている。このように全ユーザに統一されたアクセス環境が用意されていることは，クライアント環境の保守作業を軽減することにつながる。一方，専用アプリケーションを利用した場合は，クライアント環境に依存した動作不良や問合せ対応の負荷が発生する。
イ，ウ：サーバ側の作業であるため，Webブラウザや専用アプリケーションとは関係なく作業負荷が発生する。
エ：ログインアカウントは，Webブラウザ，専用アプリケーションのどちらでも同様の作業負荷が発生する。

問 46 正解 完璧 直前チェック

E-R図に関する記述のうち，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ィ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。

問 47 正解 完璧 直前チェック

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。

問 48 正解 完璧 直前チェック

BPOの説明はどれか。

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。

問46　イ

解説 **E-R図**は概念モデルの一種で，システムに関する記述を実体（エンティティ）と関連（リレーションシップ）で表現する手法である。

ア：E-R図は，主に関係データベースシステムの設計時に利用されるが，それだけとはいえない。
イ：E-R図の説明である。
ウ：**DFD**（Data Flow Diagram：データフロー図）に関する記述である。
エ：リレーションシップは，実体の関連性を表現する。

問47　ウ

解説 **DHCP**（Dynamic Host Configuration Protocol）は，IPアドレスなど各種設定の自動割り当てを行うプロトコルである。他に設定できる項目として，デフォルトゲートウェイ，サブネットマスク，DNS サーバなどがある。一般的に企業内LANでの利用や，プロバイダとの接続時に利用される。

ア：サブネットマスクや，デフォルトゲートウェイアドレスの自動取得は可能である。
イ：DHCPと固定IPアドレスの混在は可能。DHCPが利用するIPアドレスの範囲指定ができる。
ウ：正しい。DHCPは，同一ネットワーク上であれば受信できるため，DHCPサーバの設定は不要である。
エ：DHCPでは，一度IPアドレスが割り当てられた後，保持期限を過ぎるとIPアドレスが解放され，別のIPアドレスになる可能性がある。

問48　イ

解説 **BPO**（Business Process Outsourcing）は，業務プロセスの一部を社外の事業者に依頼する経営手法。経理，人事などの業務を委託する場合もある。

ア：**BCP**（Business Continuity Plan）の説明である。
ウ：**MRP**（Material Requirements Planning）の説明である。
エ：**BSC**（Balanced Score Card）の説明である。

問 49 正解 完璧 直前チェック

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・事業の目的及び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事項

問 50 正解 完璧 直前チェック

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。

問49　ウ

解説　**企画プロセス**では，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を定義する。

ア，イ：要件定義プロセスで定義される。

エ：開発プロセスで定義される。

問50　イ

解説　**マトリックス組織**：複数の目的を同時に達成するために，地域別・職能別・製品別・顧客別などの異なる編成原理をミックスし，多元的に設計した組織形態である。職能別組織がもつ職能ごとの専門スキルの維持・向上などのメリットと，事業部組織がもつ市場適応性などのメリットを同時に達成することを狙っている。

ア：**事業部制組織**の説明である。

ウ：**職能別組織**の説明である。

エ：**プロジェクト組織**の説明である。