問 1

正解 □ 完璧 □ 直前チェック □

JIS Q 27001:2014（情報セキュリティマネジメントシステム－要求事項）において，ISMSに関するリーダーシップ及びコミットメントをトップマネジメントが実証する上で行う事項として挙げられているものはどれか。

ア　ISMSの有効性に寄与するよう人々を指揮し，支援する。
イ　ISMSを組織の他のプロセスと分けて運営する。
ウ　情報セキュリティ方針に従う。
エ　情報セキュリティリスク対応計画を策定する。

問 2

正解 □ 完璧 □ 直前チェック □

経済産業省とIPAが策定した“サイバーセキュリティ経営ガイドライン（Ver 1.1）”が，自社のセキュリティ対策に加えて，実施状況を確認すべきとしている対策はどれか。

ア　自社が提供する商品及びサービスの個人利用者が行うセキュリティ対策
イ　自社に出資している株主が行うセキュリティ対策
ウ　自社のサプライチェーンのビジネスパートナが行うセキュリティ対策
エ　自社の事業所近隣の地域社会が行うセキュリティ対策

問1　ア

解説 JIS Q 27001:2014は，組織の事業リスク全般に対する考慮のもとで文書化したISMS（Information Security Management System）の確立，導入，運用，監視，レビュー，維持及び改善のための要求事項が規定されている。ISMSでは，トップマネジメントがISMSの有効性に寄与するよう人々を指揮し，支援する。

イ：ISMSは，組織の他のプロセスと合わせて運営する。
ウ：トップマネジメントは，情報セキュリティ方針を承認し周知する。
エ：トップマネジメントは，情報セキュリティ対応計画を承認する。

問2　ウ

解説 **サイバーセキュリティ経営ガイドライン**は，大企業及び中小企業（小規模事業者除く）のうち，ITに関するシステムやサービス等を供給する企業及び経営戦略上ITの利活用が不可欠である企業の経営者を対象に，経営者のリーダーシップの下で，サイバーセキュリティ対策を推進するためのガイドラインである。

サイバー攻撃から企業を守る観点で，経営者が認識する必要のある「3原則」，及び経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO：Chief Information Security Officer）等に指示すべき「10項目」がまとめられている。

指示すべき10項目に，自社のサプライチェーンのビジネスパートナが行うセキュリティ対策が記載されている。

指示1：サイバーセキュリティリスクへの対応について，組織の内外に示すための方針（セキュリティポリシー）の策定。
指示2：CISO等からなる適切な管理体制を構築と責任の明確化。
指示3：守るべき資産の特定と，セキュリティリスク対処に向けた計画の策定。
指示4：計画が確実に実施され，改善が図られるよう，PDCAを実施すること。
指示5：系列企業やサプライチェーンのビジネスパートナーを含めPDCA（Plan-Do-Check-Act）の運用を含むサイバーセキュリティ対策を行わせること。
指示6：サイバーセキュリティ対策の予算・人材育成など，資源の確保を検討。
指示7：ITシステムの運用を自組織で対応する部分と他組織に委託する部分の適切な切り分け。また，委託先への攻撃を想定したサイバーセキュリティの確保を確認。
指示8：情報共有活動に参加し，最新の状況を自社の対策に反映すること。また，可能な限り，同様の被害が社会全体に広がることの未然防止に貢献すること。
指示9：サイバー攻撃による被害拡大を防ぐため，体制の整備，初動対応マニュアルの策定など緊急時の対応体制を整備。定期的かつ実践的な演習を実施。
指示10：サイバー攻撃を受けた場合に備え，被害発覚後の通知先や開示が必要な情報項目の整理と，組織の内外に対し，経営者がスムーズに説明ができるよう準備する。

問 3 正解 完璧 直前チェック

組織的なインシデント対応体制の構築を支援する目的でJPCERT/CCが作成したものはどれか。

ア　CSIRTマテリアル
イ　ISMSユーザーズガイド
ウ　証拠保全ガイドライン
エ　組織における内部不正防止ガイドライン

問 4 正解 完璧 直前チェック

ディザスタリカバリを計画する際の検討項目の一つであるRPO（Recovery Point Objective）はどれか。

ア　業務の継続性を維持するために必要な人員計画と要求される交代要員のスキルを示す指標
イ　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
ウ　災害発生時に業務を代替する遠隔地のシステム環境と，通常稼働しているシステム環境との設備投資の比率を示す指標
エ　システムが再稼働したときに，災害発生前のどの時点の状態までデータを復旧しなければならないかを示す指標

問 5 正解 完璧 直前チェック

JIS Q 31000:2010（リスクマネジメント－原則及び指針）において，リスクマネジメントを効果的なものにするために，組織が順守することが望ましいこととして挙げられている原則はどれか。

ア　リスクマネジメントは，静的であり，変化が生じたときに終了する。
イ　リスクマネジメントは，組織に合わせて作られる。
ウ　リスクマネジメントは，組織の主要なプロセスから分離した単独の活動である。
エ　リスクマネジメントは，リスクが顕在化した場合を対象とする。

問3　ア

解説　JPCERT/CC（JPCERTコーディネーションセンター）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け付け，対応の支援，発生状況の把握，手口の分析，再発防止のための対策の検討や助言などを，技術的な立場から行っている。

CSIRT（Computer Security Incident Response Team：シーサート）：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。

CSIRTマテリアル：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作成されたガイドである。

イ：JPDDEC（一般社団法人 日本情報経済会社推進協会）から発行されている，ISMS（Information Security Management System）を構築する場合のガイドである。

ウ：特定非営利活動法デジタル・フォレンジック研究会から発行されている。事故や不正行為，犯罪といったインシデントに関わる電磁的証拠の保全の手続きに関するガイドラインである。

エ：独立行政法人情報処理推進機構（IPA）から発行されている。内部不正対策の整備を行うためのガイドラインである。

問4　エ

解説　**RPO**（Recovery Point Objective：目標復旧時点）とは，再開時に事業活動が実施できるようにするために，事業活動で使用される情報がどの状態まで復旧されなければならないかを示す指標である。

ア，ウ：事業継続計画（BCP：Business Continuity Planning）において検討する内容である。

イ：RTO（Recovery Time Objective：目標復旧時間）の説明である。

問5　イ

解説　**JIS Q 31000:2010**は，組織のステークホルダとのコミュニケーション及び協議や，更なるリスク対応が必要とならないことを確実にするためのリスク及びリスクを軽減するための管理策の体系的かつ論理的なプロセスを詳細に記述している。

ア：リスクマネジメントは，動的で繰り返し行われ変化に対応する。

イ：正しい。

ウ：リスクマネジメントは，組織の全てのプロセスにおいて不可欠な部分である。

エ：リスクマネジメントは，リスクが顕在化する前に行う。

問 6

正解 □ 完璧 □ 直前チェック □

JIS Q 31000:2010（リスクマネジメント－原則及び指針）において，リスクマネジメントは，“リスクについて組織を指揮統制するための調整された活動”と定義されている。そのプロセスを構成する活動の実行順序として，適切なものはどれか。

ア　リスク特定 → リスク対応 → リスク分析 → リスク評価
イ　リスク特定 → リスク分析 → リスク評価 → リスク対応
ウ　リスク評価 → リスク特定 → リスク分析 → リスク対応
エ　リスク評価 → リスク分析 → リスク特定 → リスク対応

問 7

正解 □ 完璧 □ 直前チェック □

JIS Q 27000:2014（情報セキュリティマネジメントシステム－用語）における“リスクレベル”の定義はどれか。

ア　脅威によって付け込まれる可能性のある，資産又は管理策の弱点
イ　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
ウ　対応すべきリスクに付与する優先順位
エ　リスクの重大性を評価するために目安とする条件

問 8

正解 □ 完璧 □ 直前チェック □

A社は，情報システムの運用をB社に委託している。当該情報システムで発生した情報セキュリティインシデントについての対応のうち，適切なものはどれか。

ア　情報セキュリティインシデント管理を一元化するために，委託契約継続可否及び再発防止策の決定をB社に任せた。
イ　情報セキュリティインシデントに迅速に対応するために，サービスレベル合意書（SLA）に緊急時のセキュリティ手続を記載せず，B社の裁量に任せた。
ウ　情報セキュリティインシデントの発生をA社及びB社の関係者に迅速に連絡するために，あらかじめ定めた連絡経路に従ってB社から連絡した。
エ　迅速に対応するために，特定の情報セキュリティインシデントの一次対応においては，事前に定めた対応手順よりも，経験豊かなB社担当者の判断を優先した。

問6　イ

解説　**JIS Q 31000:2010**では，リスクについて組織を指揮統制するための調整された活動のなかで，リスクアセスメントの順序を示している。リスク特定，リスク分析，リスク評価，リスク対応の順序となる。

リスク特定：リスクを発見，認識及び記述するプロセスである。
リスク分析：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である。
リスク評価：リスク及び大きさが，受容可能かまたは許容可能かを決定するために，リスク分析し結果をリスク基準と比較するプロセスである。
リスク対応：リスクを修正するプロセスである。

問7　イ

解説　**JIS Q 27000:2014**は，組織の事業リスク全般に対する考慮のもとで文書化したISMS（Information Security Management System）の規格である。

リスクレベル：結果と，その起こりやすさの組合せとして表現される，リスクの大きさである。
ア：**ぜい弱性**の説明である。
ウ：**リスク評価**の結果から，実施判断される内容である。
エ：**リスク基準**の説明である。

問8　ウ

解説　**情報セキュリティインシデント**とは，情報漏洩事故・事件などの情報セキュリティに関して発生する事象を指す。主に，企業へ不利になる事件や事故が該当する。
ア：委託契約の継続可否や再発防止策の決定は，契約元のA社が行う。
イ：緊急時の対応は，SLAに記載し，あらかじめ合意すべきである。
ウ：正しい。あらかじめ手順を定め，B社から関係者に連絡することは問題ない。
エ：事前に定めた手順通りに実施する必要がある。

問 9 正解 完璧 直前チェック

暗号の危殆化に該当するものはどれか。

ア　暗号化通信を行う前に，データの伝送速度や，暗号の設定情報などを交換すること
イ　考案された当時は容易に解読できなかった暗号アルゴリズムが，コンピュータの性能の飛躍的な向上などによって，解読されやすい状態になること
ウ　自身が保有する鍵を使って，暗号化されたデータから元のデータを復元すること
エ　元のデータから一定の計算手順に従って疑似乱数を求め，元のデータをその疑似乱数に置き換えること

問 10 正解 完璧 直前チェック

情報セキュリティにおけるタイムスタンプサービスの説明はどれか。

ア　公式の記録において使われる全世界共通の日時情報を，暗号化通信を用いて安全に表示するWebサービス
イ　指紋，声紋，静脈パターン，網膜，虹彩などの生体情報を，認証システムに登録した日時を用いて認証するサービス
ウ　電子データが，ある日時に確かに存在していたこと，及びその日時以降に改ざんされていないことを証明するサービス
エ　ネットワーク上のPCやサーバの時計を合わせるための日時情報を途中で改ざんされないように通知するサービス

問 11 正解 完璧 直前チェック

JIS Q 27001:2014（情報セキュリティマネジメントシステム－要求事項）において，組織の管理下で働く人々が認識をもたなければならないとされているのは，“ISMSの有効性に対する自らの貢献”及び“ISMS要求事項に適合しないことの意味”ともう一つはどれか。

ア　情報セキュリティ適用宣言書
イ　情報セキュリティ内部監査結果
ウ　情報セキュリティ方針
エ　情報セキュリティリスク対応計画

問9　イ

解説　**危殆化**とは，コンピュータの計算性能の向上により，解読に必要な計算時間が現実的な時間に近づくことで，解読される可能性が生じ，暗号の安全性が低下することである。
ア：暗号化通信の接続手順の説明である。
ウ：復号化の説明である。
エ：暗号化の説明である。

問10　ウ

解説　**タイムスタンプサービス**とは，ファイルなどの電子データにおいて，その作成や更新などが行われた日時を証明するサービス。タイムスタンプ機関によるタイムスタンプは，電子データに対して正確な日付情報を付与し，その時点での電子データの存在証明と非改ざん証明を行う仕組み，あるいは技術を意味する。タイムスタンプは電子公証，電子署名法において利用され，知的財産やプレスリリースといった新規性の証明や発行日時の証明が必要な電子文書に付与する。
ア：日本の時刻は，日本標準時である。NICTインターネット時刻供給サービスが，提供している。
イ：生体認証の日時を登録するものではない。
エ：日常情報の改ざん検知は，タイムスタンプサービスとは関連していない。

問11　ウ

解説
JIS Q 27001:2014：組織の事業リスク全般に対する考慮のもとで文書化したISMS（Information Security Management System）の確立，導入，運用，監視，レビュー，維持及び改善のための要求事項が規定されている。規格内では，組織の管理下で働く人々は，次の事項に関して認識をもたなければならないとされる。
a）　情報セキュリティ方針
b）　情報セキュリティパフォーマンスの向上によって得られる便益を含む，ISMSの有効性に対する自らの貢献
c）　ISMS要求事項に適合しないことの意味
情報セキュリティ適用宣言書：必要な管理策及びそれらの管理策を含めた理由である。
情報セキュリティ内部監査結果：内部監査の結果である。
情報セキュリティリスク対応計画：組織の情報セキュリティに対するリスクをどのように対応するかの計画書である。

問 12 正解 完璧 直前チェック

情報セキュリティ管理を行う上での情報の収集源の一つとしてJVNが挙げられる。JVNが主として提供する情報はどれか。

ア　工業製品などに関する技術上の評価や製品事故に関する事故情報及び品質情報
イ　国家や重要インフラに影響を及ぼすような情報セキュリティ事件・事故とその対応情報
ウ　ソフトウェアなどの脆弱性関連情報や対策情報
エ　日本国内で発生した情報セキュリティインシデントの相談窓口に関する情報

問 13 正解 完璧 直前チェック

NIDS（ネットワーク型IDS）を導入する目的はどれか。

ア　管理下のネットワークへの侵入の試みを検知し，管理者に通知する。
イ　実際にネットワークを介してWebサイトを攻撃し，侵入できるかどうかを検査する。
ウ　ネットワークからの攻撃が防御できないときの損害の大きさを判定する。
エ　ネットワークに接続されたサーバに格納されているファイルが改ざんされたかどうかを判定する。

問 14 正解 完璧 直前チェック

内部不正による重要なデータの漏えいの可能性を早期に発見するために有効な対策はどれか。

ア　アクセスログの定期的な確認と解析
イ　ウイルス対策ソフトの導入
ウ　重要なデータのバックアップ
エ　ノートPCのHDD暗号化

問12　ウ

解説 JVN（Japan Vulnerability Notes）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コーディネーションセンター（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：**NITE**（National Institute of Technology and Evaluation：独立行政法人 製品評価技術基盤機構）が実施する内容である。
イ：**NISC**（National center of Incident readiness and Strategy for Cybersecurity：内閣サイバーセキュリティセンター）が実施する内容である。
エ：**IPA**（Information-technology Promotion Agency, Japan：独立行政法人 情報処理推進機構）が実施する内容である。

問13　ア

解説 NIDS（ネットワーク型IDS：Intrusion Detection System）は，保護する機器へのネットワーク経路上に設置して，ネットワーク上流れる通信内容で不正アクセス等の可能性があると判断されたものをネットワーク管理者に通知するシステムである。

イ：ペネトレーションテストの説明である。
ウ：リスク分析の説明である。
エ：ホスト型IDSの説明である。

問14　ア

解説 内部不正による重要なデータの漏えいの可能性をチェックするためには，アクセスログの定期的な確認と解析が有効である。内部不正は，システムにアクセスできる人の犯行であるため，だれがどのような行動をとっているかを確認することが必要である。

イ：ウイルス対策では，ウイルスによる情報漏洩の対策となるが，内部不正は検知できない。
ウ：データのバックアップは，システム障害などで情報の損失を回避できるが，内部不正は検知できない。
エ：ノートPCのHDD暗号化は，情報漏洩対策であるが，内部不正は検知できない。

問 15

正解 □ 完璧 □ 直前チェック □

ディジタルフォレンジックスの説明として，適切なものはどれか。

ア　あらかじめ設定した運用基準に従って，メールサーバを通過する送受信メールをフィルタリングすること

イ　外部からの攻撃や不正なアクセスからサーバを防御すること

ウ　磁気ディスクなどの書換え可能な記憶媒体を廃棄する前に，単に初期化するだけではデータを復元できる可能性があるので，任意のデータ列で上書きすること

エ　不正アクセスなどコンピュータに関する犯罪に対してデータの法的な証拠性を確保できるように，原因究明に必要なデータの保全，収集，分析をすること

問 16

正解 □ 完璧 □ 直前チェック □

サーバへのログイン時に用いるパスワードを不正に取得しようとする攻撃とその対策の組合せのうち，適切なものはどれか。

	辞書攻撃	スニッフィング	ブルートフォース攻撃
ア	推測されにくいパスワードを設定する。	パスワードを暗号化して送信する。	ログインの試行回数に制限を設ける。
イ	推測されにくいパスワードを設定する。	ログインの試行回数に制限を設ける。	パスワードを暗号化して送信する。
ウ	パスワードを暗号化して送信する。	ログインの試行回数に制限を設ける。	推測されにくいパスワードを設定する。
エ	ログインの試行回数に制限を設ける。	推測されにくいパスワードを設定する。	パスワードを暗号化して送信する。

問15　エ

解説　**ディジタルフォレンジックス**とは，コンピュータやデジタル記憶媒体に残された法的な証拠に関わる科学的調査のことである。コンピュータの状態や記録の証拠性を確保し，法的問題を解決するための手法である。例えばシステムのファイルやログの収集・分析，ハードディスクの解析・復旧・復元などを行うとき，データの証拠性が失われないように，改ざん防止や改ざん検出の手段が講じられていることが必要である。このような，コンピュータ犯罪の調査・分析をして証拠を検出するための取組みのことである。

ア：メールフィルタリングの説明である。

イ：ファイアーウォールの説明である。

ウ：データの完全消去の手順である。

問16　ア

解説

辞書攻撃：辞書にある単語を利用してパスワードを不正に取得する方式。辞書に載らないようなランダムなパスワードを付けることで防ぐことが可能。

スニッフィング：パスワードを盗聴することで不正に取得する方式。パスワードを平文で送らず，暗号化することで防ぐことが可能。

ブルートフォース攻撃：総当り攻撃とも呼ばれる。パスワードとなり得る文字列を全て試行してパスワードを不正に取得する方式。攻撃の回数が多くなるため，ログイン時の失敗回数でロックをかけるなどの制限で防ぐことが可能。

問 17 正解 完璧 直前チェック

1台のファイアウォールによって，外部セグメント，DMZ，内部セグメントの三つのセグメントに分割されたネットワークがある。このネットワークにおいて，Webサーバと，重要なデータをもつデータベースサーバから成るシステムを使って利用者向けのサービスをインターネットに公開する場合，インターネットからの不正アクセスから重要なデータを保護するためのサーバの設置方法のうち，最も適切なものはどれか。ここで，ファイアウォールでは，外部セグメントとDMZとの間及びDMZと内部セグメントとの間の通信は特定のプロトコルだけを許可し，外部セグメントと内部セグメントとの間の直接の通信は許可しないものとする。

ア　Webサーバとデータベースサーバを DMZに設置する。
イ　Webサーバとデータベースサーバを内部セグメントに設置する。
ウ　Webサーバを DMZに，データベースサーバを内部セグメントに設置する。
エ　Webサーバを外部セグメントに，データベースサーバを DMZに設置する。

問 18 正解 完璧 直前チェック

2要素認証に該当する組みはどれか。

ア　クライアント証明書，ハードウェアトークン
イ　静脈認証，指紋認証
ウ　パスワード認証，静脈認証
エ　パスワード認証，秘密の質問の答え

問17　ウ

解説 **DMZ**（DeMilitarized Zone）は，ファイアウォールによってネットワーク上に隔離された区画を作り，外部とのアクセスの中継となるサーバを配置する。

本問の場合，Webサーバは外部からのアクセスが必要となるため外部からの通信が可能となるDMZに設置する。DBサーバは，外部からの直接アクセスができないよう内部セグメントに設置する。

問18　ウ

解説 **2要素認証**は，ICカードと生体認証といった異なる二つの情報を組合せ認証することで認証の安全性を高める考え方である。一般的に認証に用いられる情報は，本人のみが知っている情報（例えばパスワード）や，ワンタイムパスワードのトークン，生体情報となる。

ア：クライアント証明書と，ハードウェアトークンは同様の仕組みであるため1要素となる。
イ：静脈認証と声紋認証は，本人の生体認証であるため1要素となる。
ウ：パスワード認証と，静脈認証は，2要素となる。
エ：パスワード認証と，パスワードリマインダは，本人のみが知っている情報であるため1要素である。

問 19 正解 完璧 直前チェック

二者間で商取引のメッセージを送受信するときに，送信者のディジタル証明書を使用して行えることはどれか。

ア　受信者が，受信した暗号文を送信者の公開鍵で復号することによって，送信者の購入しようとした商品名が間違いなく明記されていることを確認する。
イ　受信者が，受信した暗号文を送信者の公開鍵で復号することによって，メッセージの盗聴を検知する。
ウ　受信者が，受信したディジタル署名を検証することによって，メッセージがその送信者からのものであることを確認する。
エ　送信者が，メッセージに送信者のディジタル証明書を添付することによって，メッセージの盗聴を防止する。

問 20 正解 完璧 直前チェック

ディジタル署名などに用いるハッシュ関数の特徴はどれか。

ア　同じメッセージダイジェストを出力する二つの異なるメッセージは容易に求められる。
イ　メッセージが異なっていても，メッセージダイジェストは全て同じである。
ウ　メッセージダイジェストからメッセージを復元することは困難である。
エ　メッセージダイジェストの長さはメッセージの長さによって異なる。

問 21 正解 完璧 直前チェック

ソーシャルエンジニアリングに該当するものはどれか。

ア　オフィスから廃棄された紙ごみを，清掃員を装って収集して，企業や組織に関する重要情報を盗み出す。
イ　キー入力を記録するソフトウェアを，不特定多数が利用するPCで動作させて，利用者IDやパスワードを窃取する。
ウ　日本人の名前や日本語の単語が登録された辞書を用意して，プログラムによってパスワードを解読する。
エ　利用者IDとパスワードの対応リストを用いて，プログラムによってWebサイトへのログインを自動的かつ連続的に試みる。

問19　ウ

解説　**ディジタル証明書**は，二者間でメッセージ送信する場合に，送信者が受信者にメッセージを改ざんされていないことを保証するための仕組みに利用される。
ア，イ：公開鍵暗号方式の説明である。
エ：ディジタル証明書は，改ざん検知であるが，盗聴の防止はできない。盗聴の防止は，公開鍵暗号方式によって行う。

問20　ウ

解説　**ハッシュ関数**は，メッセージから一定長のメッセージダイジェスト(MD)を生成されるために用いられる。ハッシュ関数に求められる性質は，異なるメッセージから同じMDが容易に生成できないことや，MDから元のメッセージが復元できないことである。
ア：二つの異なるメッセージは，容易に求められない必要がある。
イ：メッセージが異なっていると，メッセージダイジェストも異なる。
エ：メッセージダイジェストは一定長である。

問21　ア

解説
ソーシャルエンジニアリング：コンピュータやネットワークの管理者や利用者に対して，話術や盗み見(聴き)など「社会的」な手段によって，パスワードなどの重要情報を入手することである。攻撃者は人間の心理的な隙や行動のミスにつけ込み不正に情報を得る。
イ：キーロガーによる情報搾取の説明である。
ウ：辞書攻撃の説明である。
エ：パスワードリスト攻撃の説明である。

問 22 正解 完璧 直前チェック

ディジタル署名に用いる鍵の組みのうち，適切なものはどれか。

	ディジタル署名の作成に用いる鍵	ディジタル署名の検証に用いる鍵
ア	共通鍵	秘密鍵
イ	公開鍵	秘密鍵
ウ	秘密鍵	共通鍵
エ	秘密鍵	公開鍵

問 23 正解 完璧 直前チェック

ディレクトリトラバーサル攻撃に該当するものはどれか。

ア　攻撃者が，Webアプリケーションの入力データとしてデータベースへの命令文を構成するデータを入力し，管理者の意図していないSQL文を実行させる。

イ　攻撃者が，パス名を使ってファイルを指定し，管理者の意図していないファイルを不正に閲覧する。

ウ　攻撃者が，利用者をWebサイトに誘導した上で，Webアプリケーションによる HTML出力のエスケープ処理の欠陥を悪用し，利用者のWebブラウザで悪意のあるスクリプトを実行させる。

エ　セッションIDによってセッションが管理されるとき，攻撃者がログイン中の利用者のセッションIDを不正に取得し，その利用者になりすましてサーバにアクセスする。

問22　エ

解説　**ディジタル署名**とは，電子文書の送信者の正当性と電子文書の非改ざん性を保証するために付加された，暗号化された署名情報である。送信者は，自身の秘密鍵（署名鍵）で暗号化した署名を電子文書に付加して送る。受信者は，送信者の公開鍵を用いて署名を復号して，正しい内容かどうかを確認する。また，第三者によって電子文書が改ざんされていないか，偽造されたものでないかを確認することもできる。

問23　イ

解説　**ディレクトリトラバーサル攻撃**とは，Webサーバなどで相対パス記法を利用して，管理者や利用者の想定とは別のディレクトリのファイルを指定するソフトウェアの攻撃方法である。相対パス記法を悪用したディレクトリトラバーサル攻撃を受けた場合，許可されたディレクトリ・ファイル以外の意図しないファイルが読み出され，情報が漏えいすることや，既存のファイルが破壊されるなどの危険がある。

ア：SQLインジェクションの説明である。

ウ：クロスサイトスクリプティングの説明である。

エ：セッションハイジャックの説明である。

問 24 正解 完璧 直前チェック

JIS Q 27000:2014（情報セキュリティマネジメントシステム―用語）における真正性及び信頼性に対する定義 a ～ d の組みのうち，適切なものはどれか。

〔定義〕

a　意図する行動と結果とが一貫しているという特性

b　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

c　認可されたエンティティが要求したときに，アクセス及び使用が可能であるという特性

d　認可されていない個人，エンティティ又はプロセスに対して，情報を使用させず，また，開示しないという特性

	真正性	信頼性
ア	a	c
イ	b	a
ウ	b	d
エ	d	a

問 25 正解 完璧 直前チェック

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データはどれか。

ア　CA　　イ　CP　　ウ　CPS　　エ　CRL

問24　イ

解説　**JIS Q 27000:2014**は，組織の事業リスク全般に対する考慮のもとで文書化したISMS（Information Security Management System）の規格である。

a：**信頼性**の説明である。

b：**真正性**の説明である。

c：**可用性**の説明である。

d：**機密性**の説明である。

問25　エ

解説

CA（Certification Authority：認証局）：取引当事者の公開鍵証明のためのディジタル証明書を発行することや，有効期限切れ証明書のリスト発行などを行う。

CP（Certificate Policy：証明書ポリシー）：電子証明書の利用目的や，適用範囲などの方針を示した文書である。

CPS（Certification Practice Statement：証明局運用規定）：CPを運営するための実施手順などを示したものである。

CRL（Certificate Revocation List：証明書失効リスト）：有効期間中に失効した公開鍵証明書を記載したリストで，認証局から発行される。公開鍵証明書の検証時の公開鍵証明書失効確認に使用するため，常に参照される。

問 26 正解 完璧 直前チェック

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，技術面及び運用面の要件を定めたものはどれか。

ア　ISMS適合性評価制度　　イ　PCI DSS
ウ　特定個人情報保護評価　　エ　プライバシーマーク制度

問 27 正解 完璧 直前チェック

不正が発生する際には“不正のトライアングル”の3要素全てが存在すると考えられている。“不正のトライアングル”の構成要素の説明として，適切なものはどれか。

ア　“機会”とは，情報システムなどの技術や物理的な環境，組織のルールなど，内部者による不正行為の実行を可能又は容易にする環境の存在である。
イ　“情報と伝達”とは，必要な情報が識別，把握及び処理され，組織内外及び関係者相互に正しく伝えられるようにすることである。
ウ　“正当化”とは，ノルマによるプレッシャなどのことである。
エ　“動機”とは，良心のかしゃくを乗り越える都合の良い解釈や他人への責任転嫁など，内部者が不正行為を自ら納得させるための自分勝手な理由付けである。

問26　イ

解説

ISMS適合評価制度：国際的に整合性のとれた情報セキュリティマネジメントに対する第三者適合性評価制度で，情報セキュリティ全体の向上に貢献するとともに，諸外国からも信頼を得られる情報セキュリティレベルを達成することを目的としたものである。

PCI DSS（Payment Card Industry Data Security Standard）：クレジットカードのカード会員のデータセキュリティを強化し，均一なデータセキュリティ評価基準を推進するために策定されたものである。

特定個人情報保護評価：特定個人情報ファイルを保有しようとする，または保有する国の行政機関や地方公共団体等が，個人のプライバシー等の権利利益に与える影響を予測した上で特定個人情報の漏えいその他の事態を発生させるリスクを分析し，そのようなリスクを軽減するための適切な措置を講ずることを宣言するものである。

プライバシーマーク制度：個人情報保護に関して一定の要件を満たした事業者に対し，財団法人日本情報処理開発協会（JIPDEC）から使用を認められる登録商標（サービスマーク）のことである。プライバシーマーク取得にあたっては JIS Q 15001（個人情報保護マネジメントシステム－要求事項）に適合した個人情報保護体制を構築・運用していることが必要である。

問27　ア

解説　**不正のトライアングル**とは，米国の犯罪学者D.R.クレッシーが提唱した，人が不正行為を実現化するときの理論である。不正行為は，①機会，②動機，③正当化が揃ったときに実行され，逆に，この三つが揃わないと不正は発生しない。

ア：機会の説明である。
イ：情報と伝達は，不正のトライアングルの構成要素ではない。
ウ：動機の説明である。
エ：正当化の説明である。

問 28 正解 □ 完璧 □ 直前チェック □

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）”と“暗号ペイロード（ESP）”の二つのプロトコルを含むものはどれか。

ア　IPsec　　イ　S/MIME　　ウ　SSH　　エ　XML暗号

問 29 正解 □ 完璧 □ 直前チェック □

WAF（Web Appication Firewall）におけるブラックリスト又はホワイトリストの説明のうち，適切なものはどれか。

ア　ブラックリストは，脆弱性があるwebサイトのIPアドレスを登録するものであり，該当する通信を遮断する。
イ　ブラックリストは，問題が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又は無害化する。
ウ　ホワイトリストは，暗号化された受信データをどのように復号するかを定義したものであり，復号鍵が登録されていないデータを遮断する。
エ　ホワイトリストは，脆弱性がないWebサイトのFQDNを登録したものであり，登録がないWebサイトへの通信を遮断する。

問28　ア

解説

IPsec（IP Security Protocol）：データの完全性検証に用いるAH（Authentication Header）と，データの暗号化に用いるESP（Encapsulating Security Payload）の二つのセキュリティプロトコルから構成されている。

S/MIME（Secure / Multipurpose Internet Mail Extensions）：MIME（電子メールの機能を拡張する規格）に暗号化とディジタル署名の機能を追加した規格のことである。メールアドレスごとに公開鍵を用意する。

SSH（Secure Shell）：リモートからホストのシェルを操作する際に，通信路を暗号化技術を用いて保護する仕組みである。

XML暗号　XML（Extensible Markup Language）：文書を構造的に記述するためのマークアップ言語の暗号化を規定する内容である。

問29　イ

解説

WAF：Webアプリケーションのやり取りを把握・管理することによって不正侵入を防御するファイアウォール。プログラムに渡される入力内容などを直接に検査することによって，不正と見なされたアクセス要求を遮断する仕組みが採用されている。クライアントの操作するWebブラウザとWebサーバ間に介在し，ブラウザとの直接的なやり取りをWAFが受け持つ。SQLインジェクションやクロスサイトクリプティング，強制ブラウジングといった要求はWAFが遮断する。

ブラックリスト：問題のある通信データパターンが定義される。ブラックリストに登録された通信は遮断もしくは無効化される。

ホワイトリスト：問題のない正規の通信データパターンが定義されている。ホワイトリストに登録された通信は通過できるが，それ以外の通信は遮断もしくは無効化される。

ア：脆弱性があるWebサイトを登録するものではない。通過させたなくない場合に登録する。
ウ：暗号化，復号化の定義ではない。
エ：脆弱性がないWebサイトを登録するものではない。通過させる場合に登録する。

問 30 正解 完璧 直前チェック

Webサーバの検査におけるポートスキャナの利用目的はどれか。

ア　Webサーバで稼働しているサービスを列挙して，不要なサービスが稼働していないことを確認する。
イ　Webサーバの利用者IDの管理状況を運用者に確認して，情報セキュリティポリシからの逸脱がないことを調べる。
ウ　Webサーバへのアクセス履歴を解析して，不正利用を検出する。
エ　正規の利用者IDでログインし，Webサーバのコンテンツを直接確認して，コンテンツの脆弱(ぜい)性を検出する。

問 31 正解 完璧 直前チェック

電子署名法に関する記述のうち，適切なものはどれか。

ア　電子署名には，電磁的記録以外で，コンピュータ処理の対象とならないものも含まれる。
イ　電子署名には，民事訴訟法における押印と同様の効力が認められる。
ウ　電子署名の認証業務を行うことができるのは，政府が運営する認証局に限られる。
エ　電子署名は共通鍵暗号技術によるものに限られる。

問 32 正解 完璧 直前チェック

インターネットショッピングで商品を購入するとき，売買契約が成立するのはどの時点か。

ア　消費者からの購入申込みが事業者に到達した時点
イ　事業者が消費者宛てに承諾の通知を発信した時点
ウ　事業者からの承諾の通知が消費者に到達した時点
エ　商品が消費者の手元に到達した時点

問30　ア

解説　**ポートスキャナ**(Port Scanner)とは，PCやサーバなどネットワークに接続されている機器のアクセス可能な通信ポートを確認するツールである。不要なサービスの起動について確認することなどに利用する。
イ：ポートスキャナで利用者IDの管理状況を確認することはできない。
ウ：ポートスキャナではアクセス履歴の解析はできない。
エ：ポートスキャナではログインする形での確認は行わない。

問31　イ

解説　**電子署名法**は，「電子署名に関し，電磁的記録の真正な成立の推定，特定認証業務に関する認定の制度その他必要な事項を定めることにより，電子署名の円滑な利用の確保による情報の電磁的方式による流通及び情報処理の促進を図る」法律である。電子署名には，民事訴訟法における押印と同様の効力が認められている。
ア：電子署名には，電磁的記録以外は含まれない。
ウ：民間の認証業者では，認証業務のうち一定の基準を満たすものは総務大臣，経済産業大臣及び法務大臣の認定を受けることで実施することができる。
エ：電子署名の暗号方式は指定されていない。

問32　ウ

解説　**売買契約**は，インターネットショッピングの売主が財産権を移転する義務を負い，買主がその代金を支払う義務を負うことについて契約で定めたものとなる。消費者が購入を申し込み，事業者からの承諾の通知が消費者に到達した時点で売買契約は成立する。

問 33

正解 □ 完璧 □ 直前チェック □

不正競争防止法で保護されるものはどれか。

ア　特許権を取得した発明
イ　頒布されている自社独自のシステム開発手順書
ウ　秘密として管理していない，自社システムを開発するための重要な設計書
エ　秘密として管理している，事業活動用の非公開の顧客名簿

問 34

正解 □ 完璧 □ 直前チェック □

著作権法による保護の対象となるものはどれか。

ア　ソースプログラムそのもの
イ　データ通信のプロトコル
ウ　プログラムに組み込まれたアイディア
エ　プログラムのアルゴリズム

問 35

正解 □ 完璧 □ 直前チェック □

時間外労働に関する記述のうち，労働基準法に照らして適切なものはどれか。

ア　裁量労働制を導入している場合，法定労働時間外の労働は従業員の自己管理としてよい。
イ　事業場外労働が適用されている営業担当者には時間外手当の支払はない。
ウ　年俸制が適用される従業員には時間外手当の支払はない。
エ　法定労働時間外の労働を労使協定（36協定）なしで行わせるのは違法である。

問33　エ

解説　**不正競争防止法とは**，市場における競争が公正に行われるよう，営業秘密の保護，信用の保護などを定めている。また，公正な競争を阻害する不当な行為や不法行為を禁止している。不正競争防止法で保護されるトレードシークレットは，秘密性，有用性，非公知性の三つの要件をみたすことが求められる。

ア：特許権は特許法で保護される。
イ：頒布されていることから，非公知性がみたされない。
ウ：秘密として管理されている有用な顧客名簿であり，公知されていないことから，トレードシークレットとして不正競争防止法で保護される。
エ：顧客名簿は，個人情報保護法の対象である。

問34　ア

解説　**著作権法**とは，知的財産権の一つである著作権について定めた法律である。著作物の創作者である著作者に著作権（著作財産権）や著作者人格権という権利を付与し，利益を保護する。操作マニュアルなど作成されたものは著作権によって保護される。アルゴリズム，プログラム言語，プロトコルは著作権法によって保護されない。

問35　エ

解説　**労働基準法**とは，労働に関する規制等を定める法律。賃金，就業時間，休息その他の勤労条件に関する基準が定められている。時間外および休日の労働を認めるためには労使の協定を必要とする。「会社」と「従業員の過半数で組織された労働組合」，労働組合がない場合は労働者の過半数を代表する者が協定書面を締結し，行政官庁（労働基準監督署）に届け出ることが労働基準法第36条（36協定）に定められている。

ア：裁量労働制であっても，法定労働時間外の管理は会社にて管理しなければならない。
イ：事業場外であっても，時間外労働手当の支給は必要である。
ウ：年俸制であっても，時間外労働手当の支給は必要である。
エ：36協定なしで時間外労働を行わせるのは違法である。

問 36

正解 □ 完璧 □ 直前チェック □

特権ID（システムの設定，データの操作，それらの権限の設定が可能なID）の不正使用を発見するコントロールとして，最も有効なものはどれか。

ア　特権IDの貸出し及び返却の管理簿と，特権IDの利用ログを照合する。
イ　特権IDの使用を許可された者も，通常の操作では一般利用者IDを使用する。
ウ　特権IDの使用を必要とする者は，使用の都度，特権IDの貸出しを受ける。
エ　特権IDの設定内容や使用範囲を，用途に応じて細分化する。

問 37

正解 □ 完璧 □ 直前チェック □

システムテストの監査におけるチェックポイントのうち，最も適切なものはどれか。

ア　テスト計画は事前に利用者側の責任者だけで承認されていること
イ　テストは実際に業務が行われている環境で実施されていること
ウ　テストは独立性を考慮して，利用者側の担当者だけで行われていること
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

問36　ア

解説　**特権ID**とは，システムの設定，データの操作，それらの権限の設定が可能なIDで，システムに対して各種作業が可能となる。そのため，不正に利用することで重要なデータの持ち出しなどが可能となるため，厳密に管理するIDである。

ア：利用ログの照合は不正使用の発見に有効な手段である。
イ：不正使用の発見とは関連していない。通常の利用方法の説明である。
ウ：特権IDの貸し付けを受けるだけでは，不正使用される可能性を確認できない。
エ：特権IDの使用範囲の細分化は，不正使用の範囲を狭めることはできるが，不正使用の発見にはならない。

問37　エ

解説　システムテストの監査を行う際に，システム管理基準を利用することで監査の指針が明確となる。システム監査基準では，組織体が情報システムにまつわるリスクに対してコントロールを適切に整備・運用することを目的にしている。テストに関しては次の記述がある。

・システムテスト計画は，開発およびテストの責任者が承認すること
・システムテストは，開発当事者以外の者が参画すること
・システムテストは，本番環境と隔離された環境で行うこと
・システム要求事項を網羅してテストケースを設定して行うこと

これらによりアとウは誤りである。システムテストは基本的には開発当事者が行うものであるが，システム管理基準では，開発当事者以外の者の参画を求めている。したがって，イも誤りである。システム管理基準では，例外ケースや異常ケースを想定したテストを直接は求めていないが，システム要求事項を網羅したテストケースを要求している。システム要求事項には例外ケースや異常ケースの場合の対応も含まれると考えられるので，エが適切となる。

問 38 正解 完璧 直前チェック

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目的として，最も適切なものはどれか。

ア　監査依頼者に監査報告書を提出する前に，被監査部門に監査報告を行うため
イ　監査報告書に記載する改善勧告について，被監査部門の責任者の承認を受けるため
ウ　監査報告書に記載する指摘事項及び改善勧告について，事実誤認がないことを確認するため
エ　監査報告書の記載内容に関して調査が不足している事項を被監査部門に口頭で確認することによって，不足事項の追加調査に代えるため

問 39 正解 完璧 直前チェック

システム障害管理の監査で判明した状況のうち，監査人が監査報告書で報告すべき指摘事項はどれか。

ア　システム障害対応マニュアルが作成され，オペレータへの周知が図られている。
イ　システム障害によってデータベースが被害を受けた場合を想定して，規程に従って，データのバックアップをとっている。
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。
エ　全てのシステム障害について，障害記録を残し，責任者の承認を得ることが定められている。

問 40 正解 完璧 直前チェック

システムの利用部門の利用者と情報システム部門の運用者が合同で，システムの運用テストを実施する。利用者が優先して確認すべき事項はどれか。

ア　オンライン処理，バッチ処理などが運用手順どおりに稼働すること
イ　システムが決められた業務手順どおりに稼働すること
ウ　システムが目標とする性能要件を満たしていること
エ　全てのアプリケーションプログラムが仕様どおりに機能すること

問38　ウ

解説　**監査報告書**の原案について被監査部門と意見交換では，監査報告書に記載する指摘事項及び改善勧告について，事実誤認がないことを確認するために行われる。原案の確認は，是正勧告や，事実関係を，報告書として経営者に報告される前にご認識がないことを再確認する。誤った監査結果が報告されると，その後の対応などが非効率になるなど問題が出る可能性があるためである。
ア：監査報告を行うためではない。
イ：責任者の承認を得るためではない。
エ：調査不足の確認ではない。

問39　ウ

解説　システム障害管理の監査では，システム障害の種類や発生箇所，影響度に合わせて報告ルートを定めることが一般的である。重大な障害は経営者への報告や，日常の軽微な障害は，管理担当者への報告など影響度に合わせた対応方法の設定が必要である。
ア，イ，エ：システム障害管理の対応として，正しい内容である。

問40　イ

解説　システム利用部門の利用者と，情報システム部門の運用者の合同での運用テストでは，利用者は，システムが決められた業務手順通りに稼働することを確認する。二つの部門が合同で実施するということであるため，利用者は利用者側の手順を確認することが必要である。
ア，ウ：運用部門が確認する内容である。
エ：開発部門が主に確認する内容である。

問 41 正解 完璧 直前チェック

ITサービスマネジメントにおける運用レベル合意書（OLA）の説明はどれか。

ア　サービス提供者と供給者との間で取り交わした合意文書であり，サービス及びサービス目標を定義した文書である。
イ　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，サービス及びサービス目標を定義した文書である。
ウ　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，サービス及びサービス目標を定義した文書である。
エ　サービス内容を顧客に提示するための文書であり，提供する全てのサービスの種類や構成を定義した文書である。

問 42 正解 完璧 直前チェック

ITサービスマネジメントにおける問題管理プロセスの目的はどれか。

ア　インシデントの解決を，合意したサービス目標及び時間枠内に達成することを確実にする。
イ　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。
ウ　合意した目標の中で，合意したサービス継続及び可用性のコミットメントを果たすことを確実にする。
エ　全ての変更を制御された方法でアセスメントし，承認し，実施し，レビューすることを確実にする。

問41　ウ

解説　**運用レベル合意書**（OLA）とは，SLAを実現するために，サービス提供者が同じ組織内の内部グループとの間で取り交わす合意書。サービスデスクなどの内部グループとサービス提供者との間の合意事項をとりまとめた文書である。
ア：基盤となる契約（UC）に関する説明である。
イ：SLAの説明である。
エ：サービス仕様書もしくはサービス定義書の説明である。

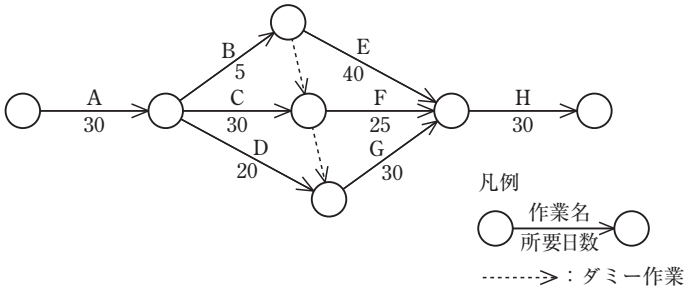
問42　イ

解説
ITサービスマネジメント：顧客が必要としているITサービスを提供するマネジメント活動全般のことである。
問題管理：インシデントの未知の根本原因の追究とその対策，再発防止策の策定を行うプロセスである。
ア：インシデント管理におけるSLAの内容となる。
ウ：ITサービス継続性管理の内容となる。
エ：変更管理の内容となる。

問 43

正解 □ 完璧 □ 直前チェック □

図のアローダイアグラムで表されるプロジェクトは，完了までに最短で何日を要するか。



ア　105　　イ　115　　ウ　120　　エ　125

問 44

正解 □ 完璧 □ 直前チェック □

ホットスタンバイ方式を採用したシステム構成の特徴はどれか。

ア　現用系が故障すると，現用系に対応した待機系に手動で切り替える。正常時には，待機系をバッチジョブに利用できるので，高いシステム稼働率が実現できる。

イ　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。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る。

ウ　システムを3重に冗長化して並列運転し，それらの処理結果の多数決をとって出力する。高い信頼性が実現できる。

エ　ネットワークが異なる複数台の現用系マシンのいずれかが故障すると，1台の予備機を立ち上げて，ネットワークや制御を自動的に切り替える。費用を抑えながら高い可用性が実現できる。

問 45

正解 □ 完璧 □ 直前チェック □

ビッグデータの活用例として，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はどれか。

ア　データウェアハウス　　イ　データディクショナリ
ウ　データマイニング　　エ　メタデータ

問43　ウ

解説　最短での日数を指定された日数から計算する。作業順序は，ABEH，ABGH，ACGH，ADGHである。ただし，ABEは，ダミー作業があるACGよりも短いため，ABEHは計算しなくてもよい。

ABGH：30＋5＋30＋30＝95日
ACGH：30＋30＋30＋30＝120日
ADGH：30＋20＋30＋30＝110日

したがって，120日が正解となる。

問44　イ

解説　**ホットスタンバイ**とは，予備機をいつでも動作可能な状態で待機させておき，障害発生時にただちに切り替える方式である。

ア：コールドスタンバイ方式の説明である。
ウ：デュアルシステムの説明である。
エ：フォールトトレランスの，3重系多数決システムの説明である。

問45　ウ

解説

データウェアハウス：情報の倉庫と呼ばれ，データベースとして大量のデータを整理・分類して蓄積し，経営に役立つ情報としてビジネスで活用するための手段を提供するシステムである。企業の様々な活動を介して得られた大量のデータを目的別に整理・統合して蓄積し，意思決定支援などに利用する。

データディクショナリ：データの名称，意味などを定義し管理するものである。

データマイニング：大量に蓄積されるデータ（ビッグデータ）を解析し，そのなかに潜む項目間の相関関係やパターンなどを探し出す技術である。

メタデータ：記述する情報資源の属性を定義したものである。日付や名前の記述形式，属性値の型などがある。

問 46

正解 □ 完璧 □ 直前チェック □

PCからWebサーバにHTTPでアクセスしようとしたところ，HTTPレスポンスのステータスコードが404，説明文字列が“Not Found”のエラーとなった。このエラーの説明として，適切なものはどれか。

ア　Webサーバ内に，URLで指定したページが見つからなかった。
イ　Webサーバのホスト名をDNSで検索したが，見つからなかった。
ウ　WebサーバへのIPパケットの経路が見つからず，HTTPリクエストがタイムアウトになった。
エ　Webサーバへのログイン時に指定した利用者IDが見つからず，ログインが拒否された。

問 47

正解 □ 完璧 □ 直前チェック □

情報戦略の立案時に，必ず整合性を取るべきものはどれか。

ア　新しく登場した情報技術
イ　基幹システムの改修計画
ウ　情報システム部門の年度計画
エ　中長期の経営計画

問 48

正解 □ 完璧 □ 直前チェック □

システム企画段階において業務プロセスを抜本的に再設計する際の留意点はどれか。

ア　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検討する。
イ　業務改善を積み重ねるために，ビジネスモデルの将来像にはこだわらず，現場レベルのニーズや課題への対応を重視して業務プロセスを再設計する。
ウ　経営者や管理者による意思決定などの非定型業務ではなく，一般社員による購買，製造，販売，出荷，サービスといった定型業務を対象とする。
エ　現行業務に関する組織，技術などについての情報を収集し，現行の組織や業務手続に基づいて業務プロセスを再設計する。

問46　ア

解説　HTTPのレスポンスエラーの際に発生する“404 Not Found”は，URLで指定されたWebページが見つからなかった場合に発生するメッセージである。URLの記載間違いや，ページが消えているなどで発生する。

イ，ウ：DNS検索，HTTPリクエストのタイムアウトは，一般的に「サーバが見つかりませんでした」といった内容のエラーとなる。

エ：“403 Forbidden”が該当するエラーである。

問47　エ

解説　**情報戦略の立案**は，経営活動を支援する情報システムのあるべき姿を明確にし，実装する機能を経営戦略に合わせて構築していくことを念頭に行う必要がある。中長期の経営計画と情報戦略の立案は，整合を取って実行していく必要がある。

ア：最新技術の確認は必要であるが，情報戦略の立案と必ず整合を取る必要はない。

イ：既存のシステムの改修であるため，情報戦略の立案時に必ず整合を取る必要はない。

ウ：情報システムの年度計画は，予算作成時に整合を取る必要があるが，情報戦略の立案時に必ず整合を取る必要はない。

問48　ア

解説　業務プロセスを抜本的に再設計することは，**BPR**（Business Process Re-engineering）という。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検討する必要がある。

イ：現場のニーズや課題よりも，ビジネスモデルの将来像にこだわる必要がある。

ウ：経営者や管理者による意思決定プロセスも対象となる。

エ：現行の手続きに基づかず，新たに業務プロセスを再設計する。

問 49

正解 □ 完璧 □ 直前チェック □

受注管理システムにおける要件のうち，非機能要件に該当するものはどれか。

ア　顧客から注文を受け付けるとき，与信残金額を計算し，結果がマイナスになった場合は，入力画面に警告メッセージを表示できること

イ　受注管理システムの稼働率を決められた水準に維持するために，障害発生時は半日以内に回復できること

ウ　受注を処理するとき，在庫切れの商品であることが分かるように担当者に警告メッセージを出力できること

エ　商品の出荷は，顧客から受けた注文情報を受注担当者がシステムに入力し，営業管理者が受注承認入力を行ったものに限ること

問 50

正解 □ 完璧 □ 直前チェック □

企業活動におけるBCPを説明したものはどれか。

ア　企業が事業活動を営む上で，社会に与える影響に責任をもち，あらゆるステークホルダからの要求に対し，適切な説明責任を果たすための取組のこと

イ　形式知だけでなく，暗黙知を含めた幅広い知識を共有して活用することによって，新たな知識を創造しながら経営を実践する経営手法のこと

ウ　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する行動計画のこと

エ　組織体の活動に伴い発生するあらゆるリスクを，統合的，包括的，戦略的に把握，評価，最適化し，価値の最大化を図る手法のこと

問49　イ

解説　各種システムの要件には，大きく機能要件，非機能要件がある。

機能要件：業務システムを開発する上で，業務システムで必要とされる機能を示すもの。

非機能要件：機能要件以外の全てを指す。例えば，セキュリティ対応や，可用性といった直接業務とは関連しないが，要件としては定義する必要があるもの。

ア，ウ，エ：機能要件である。

イ：非機能要件である。

問50　ウ

解説　BCP（Business Continuity Plan）とは，事業継続計画のこと。災害や事故など，不測の事態により企業活動が困難な状況下でも最低限の事業活動を継続し，目標復旧時間以内に再開するために事前に策定される行動計画である。情報システム，事業拠点，工場などの生産設備，物流など，緊急時に維持すべきサービスレベルや継続・復旧の優先順位などを決めておく。

ア：アカウンタビリティの説明である。

イ：ナレッジマネジメントの説明である。

エ：リスクマネジメントの説明である。