H29 春　基本情報技術者試験（FE）

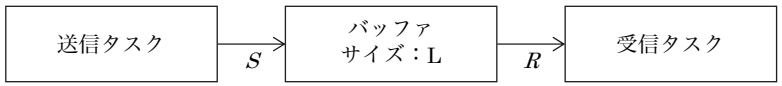
問 11　4T バイトのデータを格納できるように RAID1 の外部記憶装置を構成するとき，フォーマット後の記憶容量が 1T バイトの磁気記憶装置は少なくとも何台必要か。

ア　4　　イ　5　　ウ　6　　エ　8

問 12　システムの性能を向上させるために，スケールアウトが適しているシステムはどれか。

ア　一連の大きな処理を一括して実行しなければならないので，並列処理が困難な処理が中心のシステム
イ　参照系のトランザクションが多いので，複数のサーバで分散処理を行っているシステム
ウ　データを追加するトランザクションが多いので，データの整合性を取るためのオーバヘッドを小さくしなければならないシステム
エ　同一のマスタデータベースがシステム内に複数配置されているので，マスタを更新する際にはデータベース間で整合性を保持しなければならないシステム

問 17　図の送信タスクから受信タスクに T 秒間連続してデータを送信する。1 秒当たりの送信量を S，1 秒当たりの受信量を R としたとき，バッファがオーバフローしないバッファサイズ L を表す関係式として適切なものはどれか。ここで，受信タスクよりも送信タスクの方が転送速度は速く，次の転送開始までの時間間隔は十分にあるものとする。



ア　$L < (R - S) \times T$　　イ　$L < (S - R) \times T$
ウ　$L \geqq (R - S) \times T$　　エ　$L \geqq (S - R) \times T$

問 21　変形を感知するセンサを用いると，高架道路などの状態を監視してメンテナンスすることが可能である。この目的で使用されているセンサはどれか。

ア　サーミスタ　　イ　ジャイロ　　ウ　ひずみゲージ　　エ　ホール素子

問 27　RDBMS が二つの表を結合する方法のうち，ソートマージ結合法に関する記述はどれか。

ア　一方の表の結合する列がインデックスに含まれている場合，もう一方の表の結合する列とインデックスの値で結合する。
イ　一方の表の結合する列の値でハッシュ表を作成し，もう一方の表の結合する列と結合する。
ウ　一方の表の結合する列の値を順に読み出し，もう一方の表の結合する列と結合する。
エ　結合する列の値で並べ替えたそれぞれの表の行を，先頭から順に結合する。

問 34　IPv4 アドレス 128.0.0.0 を含むアドレスクラスはどれか。

ア　クラス A　　イ　クラス B　　ウ　クラス C　　エ　クラス D

問 35　OpenFlow を使った SDN（Software-Defined Networking）の説明として，適切なものはどれか。

ア　RFID を用いる IoT（Internet of Things）技術の一つであり，物流ネットワークを最適化するためのソフトウェアアーキテクチャ
イ　音楽や動画，オンラインゲームなどの様々なソフトウェアコンテンツをインターネット経由で効率的に配信するために開発された，ネットワーク上のサーバの最適配置手法
ウ　データ転送と経路制御の機能を論理的に分離し，データ転送に特化したネットワーク機器とソフトウェアによる経路制御の組合せで実現するネットワーク技術
エ　データフロー図やアクティビティ図などを活用して，業務プロセスの問題点を発見し改善を行うための，業務分析と可視化ソフトウェアの技術

問 36　攻撃者が用意したサーバ X の IP アドレスが，A 社 Web サーバの FQDN に対応する IP アドレスとして，B 社 DNS キャッシュサーバに記憶された。この攻撃によって，意図せずサーバ X に誘導されてしまう利用者はどれか。ここで，A 社，B 社の各従業員は自社の DNS キャッシュサーバを利用して名前解決を行う。

ア　A 社 Web サーバにアクセスしようとする A 社従業員
イ　A 社 Web サーバにアクセスしようとする B 社従業員
ウ　B 社 Web サーバにアクセスしようとする A 社従業員
エ　B 社 Web サーバにアクセスしようとする B 社従業員

問 39　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 41　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(こう)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 54　システム開発の進捗管理などに用いられるトレンドチャートの説明はどれか。

ア　作業に関与する人と責任をマトリックス状に示したもの
イ　作業日程の計画と実績を対比できるように帯状に示したもの
ウ　作業の進捗状況と，予算の消費状況を関連付けて折れ線で示したもの
エ　作業の順序や相互関係をネットワーク状に示したもの

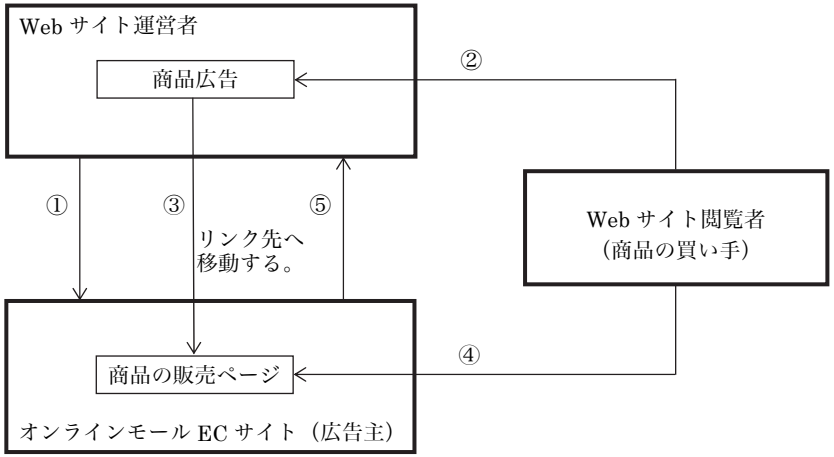
問 63　ホスティングサービスの特徴はどれか。

ア　運用管理面では，サーバの稼働監視，インシデント対応などを全て利用者が担う。
イ　サービス事業者が用意したサーバの利用権を利用者に貸し出す。
ウ　サービス事業者の高性能なサーバを利用者が専有するような使い方には対応しない。
エ　サービス事業者の施設に利用者が独自のサーバを持ち込み，サーバの選定や組合せは自由に行う。

問 69　アンゾフが提唱した成長マトリクスにおいて，既存市場に対して既存製品で事業拡大する場合の戦略はどれか。

ア　市場開発　　イ　市場浸透　　ウ　製品開発　　エ　多角化

問 74　インターネット広告などで見られるアフィリエイトプログラムのモデル例の⑤に当てはまるものはどれか。ここで，①～⑤はこのモデルでの業務順序を示し，①，②，④，⑤はア～エのいずれかに対応する。



ア　Web サイト上の掲載広告をクリックする。
イ　アフィリエイトプログラムに同意し参加する。
ウ　希望する商品を購入する。
エ　商品の売上に応じた成功報酬を支払う。

問 75　会議におけるファシリテータの役割として，適切なものはどれか。

ア　技術面や法律面など，自らが専門とする特定の領域の議論に対してだけ，助言を行う。
イ　議長となり，経営層の意向に合致した結論を導き出すように議論をコントロールする。
ウ　中立公平な立場から，会議の参加者に発言を促したり，議論の流れを整理したりする。
エ　日程調整・資料準備・議事録作成など，会議運営の事務的作業に特化した支援を行う。

H29 春　応用情報技術者試験（AP）

問 12　Web システムにおける CDN（Contents Delivery Network）に関する記述として，適切なものはどれか。

ア　Web サーバ，アプリケーションサーバ，データベースサーバの三つの構成要素に分けることによってコンテンツの検索を容易にすると同時に，システムの拡張性も高める。
イ　コミュニティ型の Web サイト及びネットワークサービスによって，人と人とのつながりを促進するコンテンツを共有する。
ウ　動画再生や音楽再生に必要なプログラム部品をインターネット経由で入手し，Web ブラウザに組み込む。
エ　動画や音声などの大容量のデータを利用する際に，インターネット回線の負荷を軽減するようにサーバを分散配置する。

問 19　オープンソースライセンスの GNU GPL（GNU General Public License）の説明のうち，適切なものはどれか。

ア　GPL であるソースコードの実現する機能を利用する，別のプログラムのソースコードを作成すると，GPL が適用される。
イ　GPL であるソースコードの全てを使って派生物を作った場合に限って，GPL が適用される。
ウ　GPL であるソースコードの派生物のライセンスは，無条件に GPL となる。
エ　GPL であるソースコードを組み込んだ派生物を GPL にするか否かは，派生物の開発者が決める。

問 20　エネルギーハーベスティングの適用例として，適切なものはどれか。

ア　AC 電源で充電したバッテリで駆動される携帯電話機
イ　インバータ制御を用いるエアーコンディショナの室外機
ウ　スイッチを押す力を電力に変換して作動する RF リモコン
エ　無停電電源装置を備えたデータサーバ

問 25　表示装置には色彩や濃淡などの表示能力に限界がある。一つ一つの画素では表現可能な色数が少ない環境でも，幾つかの画素を使って見掛け上表示できる色数を増やし，滑らかで豊かな階調を表現する手法はどれか。

ア　インデックスカラー　　イ　オーバレイ
ウ　カーニング　　エ　ディザリング

問 34　OpenFlow を使った SDN（Software-Defined Networking）の説明として，適切なものはどれか。（高度共通午前Ⅰ　問 11）

ア　単一の物理サーバ内の仮想サーバ同士が，外部のネットワーク機器を経由せずに，物理サーバ内部のソフトウェアで実現された仮想スイッチを経由して，通信する方式
イ　データを転送するネットワーク機器とは分離したソフトウェアによって，ネットワーク機器を集中的に制御，管理するアーキテクチャ
ウ　プロトコルの文法を形式言語を使って厳密に定義する，ISO で標準化された通信プロトコルの規格
エ　ルータやスイッチの機器内部で動作するソフトウェアを，オープンソースソフトウェア（OSS）で実現する方式

問 35　ブロードキャストストームの説明として，適切なものはどれか。

ア　1 台のブロードバンドルータに接続する PC の数が多過ぎることによって，インターネットへのアクセスが遅くなること
イ　IP アドレスを重複して割り当ててしまうことによって，通信パケットが正しい相手に到達せずに，再送が頻繁に発生すること
ウ　イーサネットフレームの宛先 MAC アドレスが FF-FF-FF-FF-FF-FF で送信され，LAN に接続した全ての PC が受信してしまうこと
エ　ネットワークスイッチ間にループとなる経路ができることによって，特定のイーサネットフレームが大量に複製されて，通信が極端に遅くなったり通信できなくなったりすること

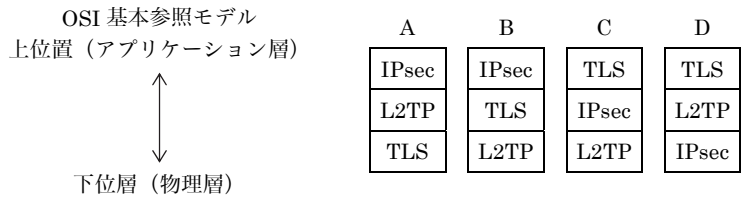
問 39　経済産業省と IPA が策定した“サイバーセキュリティ経営ガイドライン（Ver 1.1）”の説明はどれか。（高度共通午前Ⅰ　問 14）

ア　企業が IT 活用を推進していく中で，サイバー攻撃から企業を守る観点で経営者が認識すべき 3 原則と，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に，経営者が指示すべき事項をまとめたもの
イ　経営者が，情報セキュリティについて方針を示し，マネジメントシステムの要求事項を満たすルールを定め，組織が保有する情報を CIA の観点から維持し，継続的に見直すためのプロセス及び管理策を体系的に規定したもの
ウ　事業体の IT に関する経営者の活動を大きく IT ガバナンス（統制）と IT マネジメント（管理）に分割し，具体的な目標と工程として 37 のプロセスを定義したもの
エ　世界的規模で生じているサイバーセキュリティ上の脅威に関して，企業の経営者を支援する施策を総合的かつ効果的に推進するための国の責務を定めたもの

問 44　攻撃に HTTP over TLS（HTTPS）が使われた場合に起こり得ることはどれか。

ア　HTTPS を使った SQL インジェクション攻撃を受けると，Web アプリケーションでデータベースへの不正な入力をチェックできないので，悪意のある SQL が実行されてしまう。
イ　HTTPS を使ったクロスサイトスクリプティング攻撃を受けると，Web ブラウザでプログラムやスクリプトを実行しない設定にしても実行を禁止できなくなるので，悪意のある Web サイトからダウンロードされたプログラムやスクリプトが実行されてしまう。
ウ　HTTPS を使ったブルートフォース攻撃を受けると，ログイン試行のチェックができないので，Web アプリケーションでアカウントロックなどの対策が実行できなくなってしまう。
エ　攻撃者が社内ネットワークに仕掛けたマルウェアによって HTTPS が使われると，通信内容がチェックできないので，秘密情報が社外に送信されてしまう。

問 45　VPN で使用されるセキュアなプロトコルである IPsec，L2TP，TLS の，OSI 基本参照モデルにおける相対的な位置関係はどれか。



ア　A　　イ　B　　ウ　C　　エ　D

問 46　組込み機器のソフトウェア開発にプラットフォーム開発を適用する利点として，適切なものはどれか。

ア　機器ごとにソフトウェアを新規に設計するので，最小のコードサイズで最大の性能を実現できる。
イ　機器ごとのハードウェアとソフトウェアの結合テストを不要にできる。
ウ　ソフトウェアを複数の異なる機器に共通して利用することが可能になるので，ソフトウェア開発効率を向上できる。
エ　複数の機器に共通のバグが発生したとき，ソフトウェアのプラットフォーム部分をバグの原因から除外できる。

問 49　アジャイル開発で“イテレーション”を行う目的のうち，適切なものはどれか。
（高度共通午前Ⅰ　問 17）

ア　ソフトウェアに存在する顧客の要求との不一致を解消したり，要求の変化に柔軟に対応したりする。
イ　タスクの実施状況を可視化して，いつでも確認できるようにする。
ウ　ペアプログラミングのドライバとナビゲータを固定化させない。
エ　毎日決めた時刻にチームメンバが集まって開発の状況を共有し，問題が拡大したり，状況が悪化したりするのを避ける。

問 65　組込みシステム開発において，製品に搭載する LSI を新規に開発したい。LSI 設計を自社で行い，LSI 製造を外部に委託する場合の委託先として，適切なものはどれか。

ア　IP プロバイダ　　イ　デザインハウス
ウ　ファウンドリ　　エ　ファブレスメーカ

問 68　事業戦略のうち，浸透価格戦略に該当するものはどれか。
（高度共通午前Ⅰ　問 26）

ア　売上高をできるだけ維持しながら，製品や事業に掛けるコストを徐々に引き下げていくことによって，短期的なキャッシュフローの増大を図る。
イ　事業を分社化し，その会社を売却することによって，投下資金の回収を図る。
ウ　新規事業に進出することによって，企業を成長させ，利益の増大を図る。
エ　低価格戦略と積極的なプロモーションによって，新製品のマーケットシェアの増大を図る。

問 72　インターネットを活用した広告手法のうち，行動ターゲティングの説明はどれか。

ア　インターネット検索エンジンで，利用者が入力した特定の検索キーワードに関連する商品の広告を表示する。
イ　サービス運営会社が発行する広告タグを埋め込んだ Web サイトを訪れた利用者に対して，その Web サイトのコンテンツに関連した広告を自動的に表示する。
ウ　スマートフォンなどの GPS 機能を使い，利用者の現在地に合わせて，近隣の商業施設の広告を，利用者が見ている Web サイトに表示する。
エ　利用者の Web サイトの検索履歴，アクセスしたページや購買履歴から利用者の興味・関心を解析し，関連した広告を利用者が見ている Web サイトに表示する。

問 2　SSL/TLS のダウングレード攻撃に該当するものはどれか。

ア　暗号化通信中にクライアント PC からサーバに送信するデータを操作して，強制的にサーバのディジタル証明書を失効させる。
イ　暗号化通信中にサーバからクライアント PC に送信するデータを操作して，クライアント PC の Web ブラウザを古いバージョンのものにする。
ウ　暗号化通信を確立するとき，弱い暗号スイートの使用を強制することによって，解読しやすい暗号化通信を行わせる。
エ　暗号化通信を盗聴する攻撃者が，暗号鍵候補を総当たりで試すことによって解読する。

問 5　セッション ID の固定化（Session Fixation）攻撃の手口はどれか。

ア　HTTPS 通信で Secure 属性がない Cookie にセッション ID を格納する Web サイトにおいて，HTTP 通信で送信されるセッション ID を悪意のある者が盗聴する。
イ　URL パラメタにセッション ID を格納する Web サイトにおいて，Referer によってリンク先の Web サイトに送信されるセッション ID が含まれた URL を，悪意のある者が盗用する。
ウ　悪意のある者が正規の Web サイトから取得したセッション ID を，利用者の Web ブラウザに送り込み，利用者がそのセッション ID でログインして，セッションがログイン状態に変わった後，利用者になりすます。
エ　推測が容易なセッション ID を生成する Web サイトにおいて，悪意のある者がセッション ID を推測し，ログインを試みる。

問 6　DNS 水責め攻撃（ランダムサブドメイン攻撃）の手口と目的に関する記述のうち，適切なものはどれか。

ア　ISP が管理する DNS キャッシュサーバに対して，送信元を攻撃対象のサーバの IP アドレスに詐称してランダムかつ大量に生成したサブドメイン名の問合わせを送り，その応答が攻撃対象のサーバに送信されるようにする。
イ　オープンリゾルバとなっている DNS キャッシュサーバに対して，攻撃対象のドメインのサブドメイン名をランダムかつ大量に生成して問い合わせ，攻撃対象の権威 DNS サーバを過負荷にさせる。
ウ　攻撃対象の DNS サーバに対して，攻撃者が管理するドメインのサブドメイン名をランダムかつ大量に生成してキャッシュさせ，正規の DNS リソースレコードを強制的に上書きする。
エ　攻撃対象の Web サイトに対して，当該ドメインのサブドメイン名をランダムかつ大量に生成してアクセスし，非公開の Web ページの参照を試みる。

問 11　インターネットバンキングの利用時に被害をもたらす MITB（Man-in-the-Browser）攻撃に有効な対策はどれか。

ア　インターネットバンキングでの送金時に Web ブラウザで利用者が入力した情報と，金融機関が受信した情報とに差異がないことを検証できるよう，トランザクション署名を利用する。
イ　インターネットバンキングでの送金時に接続する Web サイトの正当性を確認できるよう，EV SSL サーバ証明書を採用する。
ウ　インターネットバンキングでのログイン認証において，一定時間ごとに自動的に新しいパスワードに変更されるワンタイムパスワードを用意する。
エ　インターネットバンキング利用時の通信を SSL ではなく TLS を利用して暗号化する。

問 13　ウイルス対策ソフトでの，フォールスネガティブに該当するものはどれか。

ア　ウイルスに感染していないファイルを，ウイルスに感染していないと判断する。
イ　ウイルスに感染していないファイルを，ウイルスに感染していると判断する。
ウ　ウイルスに感染しているファイルを，ウイルスに感染していないと判断する。
エ　ウイルスに感染しているファイルを，ウイルスに感染していると判断する。

問 19　PC やスイッチングハブがもつイーサネットインタフェース（物理ポート）の，Automatic MDI/MDI-X の機能はどれか。

ア　コネクタの送信端子と受信端子が正しい組合せとなるように，自動で判別して切り替える機能
イ　接続した機器のアドレスを学習し，イーサネットフレームを該当するインタフェースにだけ転送する機能
ウ　通信経路のループを自動的に検出する機能
エ　通信速度や，全二重と半二重のデータ通信モードを自動的に設定する機能

H29 春　データベーススペシャリスト試験（DB）　午前Ⅱ

問 8　“社員”表から，部署コードごとの主任の人数と一般社員の人数を求める SQL 文とするために，a に入る字句はどれか。ここで，実線の下線は主キーを表す。

社員（社員コード，部署コード，社員名，役職）

〔SQL 文〕

```
SELECT 部署コード,
    COUNT(CASE WHEN 役職 = '主任' [ a ] END) AS 主任の人数,
    COUNT(CASE WHEN 役職 = '一般社員' [ a ] END) AS 一般社員の人数
FROM 社員 GROUP BY 部署コード
```

〔結果の例〕

部署コード	主任の人数	一般社員の人数
AA01	2	5
AA02	1	3
BB01	0	1

ア　THEN 1 ELSE -1　　イ　THEN 1 ELSE 0
ウ　THEN 1 ELSE NULL　　エ　THEN NULL ELSE 1

問 9　SQL が提供する 3 値論理において，A に 5，B に 4，C に NULL を代入したとき，次の論理式の評価結果はどれか。

（A ＞ C）or（B ＞ A）or（C ＝ A）

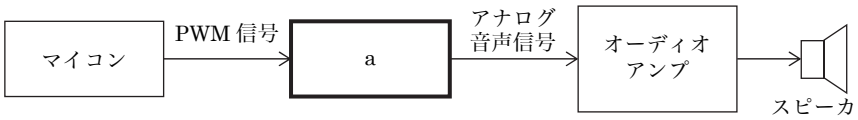
ア　ϕ（空）　　イ　false（偽）
ウ　true（真）　　エ　unknown（不定）

H29 春　エンベデッドシステムスペシャリスト試験（ES）　午前Ⅱ

問 3　SLC（Single-Level Cell）型と比較したとき，MLC（Multi-Level Cell）型のフラッシュメモリの優れている点はどれか。

ア　1 セル当たりの書換え時間が短い。　イ　1 セル当たりの記憶容量が大きい。
ウ　書換え可能回数が多い。　ウ　データ保持期間が長い。

問 4　PWM 信号を用いて音声を出力するとき，次の図の a に該当するものはどれか。



ア　A/D 変換器　　イ　D/A 変換器
ウ　ハイパスフィルタ　　エ　ローパスフィルタ

問 9　プログラムを構成するモジュールや関数の実行回数，実行時間など，性能改善のための分析に役立つ情報を収集するツールはどれか。

ア　エミュレータ　　イ　シミュレータ
ウ　デバッガ　　ウ　プロファイラ

問 10　Linux の拡張モジュールである SELinux（Security-Enhanced Linux）を使用することによって可能になることはどれか。

ア　スーパユーザによるリソースへのアクセスを制限して，侵入された際の影響を最小限に抑える。
イ　接続元や使用するポート番号を制限して，侵入を防ぐ。
ウ　通信文を暗号化して，盗聴を防ぐ。
エ　ファイルを以前の状態と比較して，改ざんを検知する。

問 22　ヒューマンインタフェースをもつシステムにおいて，機能とヒューマンインタフェースの相互依存を弱めることによって，修正性や再利用性を向上させることを目的としたアーキテクチャパターンはどれか。

ア　MVC　　イ　イベントシステム
ウ　マイクロカーネル　　エ　レイヤ

問 24　自動車分野の機能安全規格 ISO 26262 においてテスト指標として用いられる C1 カバレージの説明として，適切なものはどれか。

ア　最初にターゲットとする顧客ユースケースのテスト範囲
イ　プログラムの分岐網羅率
ウ　保証する動作温度範囲
エ　ユーザの振舞いや外部仕様を基にしたテスト

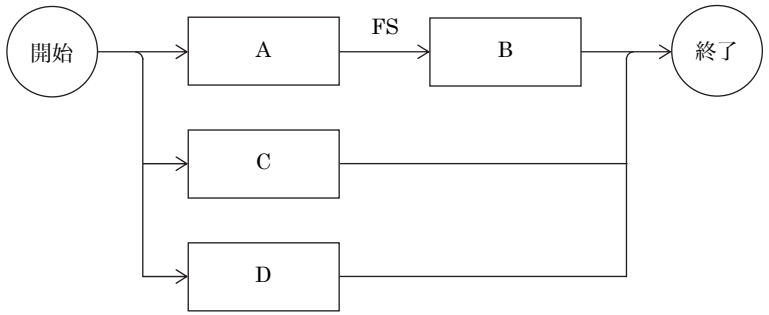
H29 春　プロジェクトマネージャ試験（PM）　午前Ⅱ

問 7　チームの発展段階を五つに区分したタックマンモデルによれば，メンバの異なる考え方や価値観が明確になり，メンバがそれぞれの意見を主張し合う段階はどれか。

ア　安定期（Norming）　　イ　遂行期（Performing）
ウ　成立期（Forming）　　エ　動乱期（Storming）

問 10　四つのアクティビティ A～D によって実行する開発プロジェクトがある。図は，各アクティビティの依存関係を PDM（プレシデンスダイアグラム法）によって表している。各アクティビティの実行に当たっては，専門チームの支援が必要である。条件に従ってアクティビティを実行するとき，開発プロジェクトの最少の所要日数は何日か。

〔アクティビティの依存関係〕



〔条件〕
・各アクティビティの所要日数及び実行に当たっての専門チームの支援期間は，次のとおりである。

アクティビティ名	所要日数（日）	専門チームの支援期間
A	10	実行する期間の最初の 4 日間
B	5	実行する期間の最初の 2 日間
C	10	実行する期間の最初の 4 日間
D	4	実行する期間の全て

・専門チームは，同時に複数のアクティビティの支援をすることはできない。
・専門チームは，各アクティビティを連続した日程で支援する。
・専門チーム以外の資源に各アクティビティ間の競合はない。

ア　15　　イ　16　　ウ　17　　エ　18

問 11　アジャイル型開発プロジェクトの管理に用いるベロシティの説明はどれか。

ア　開発規模を見積もる際の規模の単位であり，ユーザストーリ同士を比較し，相対的な量で表すものである。
イ　完了待ちのプロダクト要求事項と成果物を組み合わせたものをビジネスにおける優先度順に並べたものである。
ウ　定められた期間で完了した作業量と残作業量をグラフにして進捗状況を表すものである。
エ　チームの生産性の測定単位であり，定められた期間で製造，妥当性確認，及び受入れが行われた成果物の量を示すものである。

H29 春　システム監査技術者試験（AU）　午前Ⅱ

問 11　JIS Q 20000-2:2013（サービスマネジメントシステムの適用の手引）によれば，サービスレベル合意書（SLA）の作成指針のうち，最も適切なものはどれか。

ア　SLA では，顧客の責任は規定せずに，サービス提供者の責任を規定する。
イ　SLA において設定する目標は，サービス提供者の視点でできるだけ多く定義する。
ウ　ある顧客に対して複数のサービスを提供する際に，一つの SLA で複数のサービスに対処してもよい。
エ　利用するサービスに関する情報は，サービスカタログに収録されている情報についても，必ず SLA に記載する。

H29 春　情報セキュリティマネジメント試験（SG）

問 1　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　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 3　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 5　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 6　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　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 9　暗号の危殆（たい）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 11　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 14　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 25　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 26　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 46　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。

平成 29 年度春期 新傾向午前問題ニュース　問題リスト

年度	試験	問 NO	問 題 タ イ ト ル	正解
H29 春	FE	11	RAID1 構成で必要な磁気記憶装置台数	エ
H29 春	FE	12	スケールアウトが適しているシステム	イ
H29 春	FE	17	バッファサイズを表す関係式	エ
H29 春	FE	21	変形を感知するセンサ	ウ
H29 春	FE	27	ソートマージ結合法に関する記述	エ
H29 春	FE	34	IPv4 アドレス 128.0.0.0 を含むアドレスクラス	イ
H29 春	FE	35	OpenFlow を使った SDN の説明	ウ
H29 春	FE	36	DNS キャッシュサーバに対する攻撃	イ
H29 春	FE	39	サイバーセキュリティ経営ガイドラインで確認すべきとされている対策	ウ
H29 春	FE	41	タイムスタンプサービス	ウ
H29 春	FE	54	トレンドチャート	ウ
H29 春	FE	63	ホスティングサービスの特徴	イ
H29 春	FE	69	既存市場に対して既存製品で事業を拡大する戦略	イ
H29 春	FE	74	アフィリエイトプログラムのモデル例	エ
H29 春	FE	75	ファシリテータの役割	ウ
H29 春	AP	12	Web システムにおける CDN	エ
H29 春	AP	19	オープンソースライセンスの GNU GPL	ウ
H29 春	AP	20	エネルギーハーベスティングの適用例	ウ
H29 春	AP	25	表示装置における表現手法	エ
H29 春	AP	34	OpenFlow を使った SDN の説明	イ
H29 春	AP	35	ブロードキャストストームの説明	エ
H29 春	AP	39	サイバーセキュリティ経営ガイドラインの説明	ア
H29 春	AP	44	HTTPoverTLS が使われた場合に起こり得ること	エ
H29 春	AP	45	VPN で使用されるプロトコルの相対的な位置関係	ウ
H29 春	AP	46	プラットフォーム開発を適用する利点	ウ
H29 春	AP	49	アジャイル開発でイテレーションを行う目的	ア
H29 春	AP	65	LSI 設計を自社で行い製造を外部に委託する場合の委託先	ウ
H29 春	AP	68	事業戦略の浸透価格戦略に該当するもの	エ
H29 春	AP	72	行動ターゲティングの説明	エ

年度	試験	問 NO	問 題 タ イ ト ル	正解
H29 春	SC	02	SSL/TLS のダウングレード攻撃	ウ
H29 春	SC	05	セッション ID の固定化攻撃の手口	ウ
H29 春	SC	06	DNS 水責め攻撃の手口と目的	イ
H29 春	SC	11	MITB 攻撃に有効な対策	ア
H29 春	SC	13	フォールスネガティブに該当するもの	ウ
H29 春	SC	19	Automatic MDI/MDI-X の機能	ア
H29 春	DB	08	人数を求める SQL 文	ウ
H29 春	DB	09	論理式の評価結果	エ
H29 春	ES	03	MLC 型のフラッシュメモリの優位点	イ
H29 春	ES	04	PWM 信号を用いた音声出力	エ
H29 春	ES	09	プログラムを分析するための情報収集ツール	ア
H29 春	ES	10	SELinux で可能になること	エ
H29 春	ES	22	修正性や再利用性を向上させるアーキテクチャパターン	ア
H29 春	ES	24	ISO 26262 における C1 カバレージの説明	イ
H29 春	PM	07	タックマンモデル	エ
H29 春	PM	10	PDM による開発プロジェクトの最少所要日数	イ
H29 春	PM	11	ベロシティ	エ
H29 春	AU	11	JIS Q 20000-2:2013 による SLA の作成指針	ウ
H29 春	SG	01	ISMS に関するリーダーシップ及びコミットメント	ア
H29 春	SG	02	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対策	ウ
H29 春	SG	03	JPCERT/CC が作成したもの	ア
H29 春	SG	05	リスクマネジメントを効果的なものにするために順守すること	イ
H29 春	SG	06	リスクマネジメントを構成する活動の実行順序	イ
H29 春	SG	07	リスクレベルの定義	イ
H29 春	SG	09	暗号の危殆化	イ
H29 春	SG	11	組織の管理下で働く人々が認識をもたなければいけないこと	ウ
H29 春	SG	14	内部不正による漏えいの可能性を早期に発見する対策	ア
H29 春	SG	25	失効したディジタル証明書の一覧を示すデータ	エ
H29 春	SG	26	カード会員データのセキュリティ強化	イ
H29 春	SG	46	Web サーバに HTTP でアクセスしたときのエラー	ア

iTEC

人間力を，企業力に。

www.itec.co.jp