問 1

正解 □ 完璧 □ 直前チェック □

アジャイル開発プロセスにおいて，Bill Wakeが提案した“INVEST”と呼ばれる六つの観点を用いて行うことはどれか。

ア　効率よくアクティビティ図を作成する。
イ　コード化できるレベルまで詳細化されたデータフロー図を作成する。
ウ　再利用しやすいソフトウェアパターンとなっているかどうかを評価する。
エ　質の高いユーザストーリとなっているかどうかを評価する。

問 2

正解 □ 完璧 □ 直前チェック □

機能要件と非機能要件のうちの，機能要件を満たすために行う設計はどれか。

ア　業務システムを開発するための開発環境を設計する。
イ　業務の重要度を分析して障害発生時の復旧時間を明確にする。
ウ　業務を構成する要素間のデータの流れを明確にする。
エ　部門業務の効率性と業務間の関連性を考慮して最適なサーバ配置を設計する。

問1　エ

解説　**INVEST**とは次の六つの観点を用いて，そのソフトウェアが提供する機能が優れたユーザストーリとなっているかを評価することである。アジャイル開発においてユーザストーリとは，主要なシステムの振る舞いと，ユーザからの観点における価値を記述したものである。

Independent：独立しているか。他のストーリの影響を受けていないか。
Negotiable：交渉可能であるか。ストーリは開発しながら開発側と顧客側との間の交渉を通じて調整と変更を重ねていく。
Valuable：ストーリが顧客にとって価値があるか。
Estimable：見積り可能であるか。見積りできるだけの情報がストーリに含まれているか。
Sized Right：適切な大きさか。長すぎるストーリとなっていないか。
Testable：テスト可能か。ストーリが収束したかどうかを確認できるか。

問2　ウ

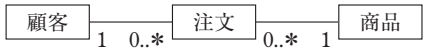
解説　**機能要件**とは，業務システムを開発する上で，業務システムで必要とされる機能を示す要件。

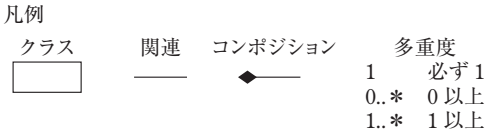
非機能要件とは，機能要件以外の全ての要件。例えば，セキュリティ対応やシステムの可用性など，業務とは直接には関連しないが要件としては定義しなければならないもの。

ア，イ，エ：非機能要件である。
ウ：機能要件である。

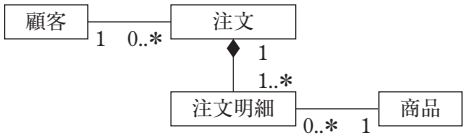
問 3 正解 完璧 直前チェック

図は“顧客が商品を注文する”を表現したUMLのクラス図である。“顧客が複数の商品をまとめて注文する”を表現したクラス図はどれか。ここで，注文明細は注文に含まれる一つの商品に対応し，注文は一つ以上の注文明細を束ねたもので，一つの注文に対応する。

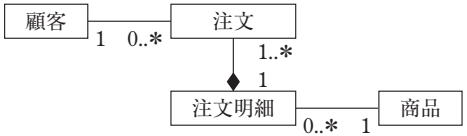




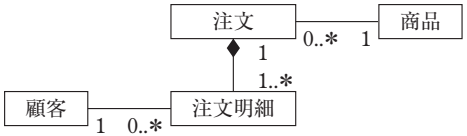
ア



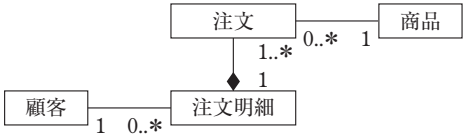
イ



ウ

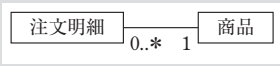


エ



問3 ア

解説 注文明細は1種類の商品に対応するので，

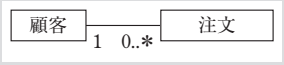


となる。注文明細から見れば商品は必ず一つであるが，商品から見れば複数の注文明細に対応できるとともに，対応する注文明細が存在しなくてもよい。したがって多重度は「0..＊」となる。

注文は複数の注文明細を束ねているので，注文が全体，注文明細が部分の関係である。これはコンポジションの関係である。ひし形は全体側のクラスに付けるので，

となる。一つの注文に対して注文明細は一つ以上なので，多重度は「1..＊」となる。

この注文が注文の全体であるから，顧客は複数の注文を行うこと，あるいは注文をしないことができるので，0個以上の注文に対応する。したがって，



となる。これらを組み合わせた選択肢アが正解となる。

問 4

正解 □ 完璧 □ 直前チェック □

複数のシステムの組合せによって実現するSoS（System of Systems）をモデル化するのに適した表記法であるSysMLの特徴はどれか。

ア　オブジェクト図によって，インスタンスの静的なスナップショットが記述できる。
イ　単純な図形と矢印によって，システムのデータの流れが記述できる。
ウ　パラメトリック図によって，モデル要素間の制約条件が記述できる。
エ　連接，反復，選択の記述パターンによって，ソフトウェアの構造を分かりやすく視覚化できる。

問 5

正解 □ 完璧 □ 直前チェック □

ソフトウェアパターンのうち，GoFのデザインパターンの説明はどれか。

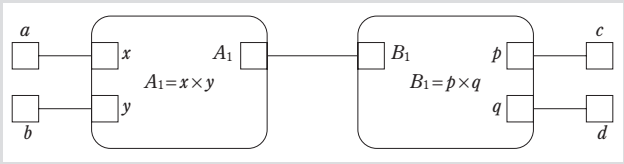
ア　Javaのパターンとして引数オブジェクト，オブジェクトの可変性などで構成される。
イ　オブジェクト指向開発のためのパターンとして生成，構造，振る舞いの三つのカテゴリで分類される。
ウ　構造，分散システム，対話型システム及び適合型システムの四つのカテゴリで分類される。
エ　抽象度が異なる要素を分割して階層化するためのLayers，コンポーネント分割のためのBrokerなどで構成される。

問4　ウ

解説　**SysML**とはシステムの記述に適したモデリング言語である。**UML**の仕様の一部を利用したものに独自の仕様を拡張したもの。

SoSとは，自律分散的な複数のシステムが何らかの目的のために一つのシステムとして統合されたもの。その統合されたシステムの全体がSoSである。**超システム**と訳されることもある。

ア：UMLに関する説明である。
イ：**DFD**（Data Flow Diagram）に関する説明である。
ウ：SysMLに関する説明である。パラメトリック図とはシステムを構成する要素間の数学的な制約を記述する図法である。



エ：流れ図に関する説明である。

問5　イ

解説　**ソフトウェアパターン**とは，ソフトウェア開発における設計ノウハウや問題解決手段といった知識を再利用できるように抽象化・形式化してまとめたもの。

GoFデザインパターンとは，GoF（Gang of Fourと呼ばれる4人組の開発者チーム）は著書『オブジェクト指向における再利用のためのデザインパターン』のなかで5種の生成パターン，7種の構造パターン，11種の振る舞い，計23種のデザインパターンを示した。

ア：Java Beansパターンに関する説明である。
イ：生成・構造・振る舞いの三つのカテゴリで構成されている。これはGoFの説明である。
ウ，エ：POSA（Pattern-Oriented Software Architecture）のアーキテクチャパターンの説明である。

問 6

正解 完璧 直前チェック

組込みシステムの開発における，ハードウェアとソフトウェアのコデザインを適用した開発手法の説明として，適切なものはどれか。

ア　ハードウェアとソフトウェアの切分けをシミュレーションによって十分に検証し，その後もシミュレーションを活用しながらハードウェアとソフトウェアを並行して開発していく手法
イ　ハードウェアの開発とソフトウェアの開発を独立して行い，それぞれの完了後に組み合わせて統合テストを行う手法
ウ　ハードウェアの開発をアウトソーシングし，ソフトウェアの開発に注力することによって，短期間に高機能の製品を市場に出す手法
エ　ハードウェアをプラットフォーム化し，主にソフトウェアで機能を差別化することによって，短期間に多数の製品ラインアップを構築する手法

問 7

正解 完璧 直前チェック

イベント駆動型のアプリケーションにおけるイベント処理のタイミングを設計するのに有用なものはどれか。

ア　DFD　　イ　E-R図　　ウ　シーケンス図　　エ　ペトリネット

問 8

正解 完璧 直前チェック

フェールセーフの考えに基づいて設計したものはどれか。

ア　乾電池のプラスとマイナスを逆にすると，乾電池が装填できないようにする。
イ　交通管制システムが故障したときには，信号機に赤色が点灯するようにする。
ウ　ネットワークカードのコントローラを二重化しておき，故障したコントローラの方を切り離しても運用できるようにする。
エ　ハードディスクにRAID1を採用して，MTBFで示される信頼性が向上するようにする。

春 秋

問6　ア

解説　**コデザイン**（協調設計）とは，ハードウェアとソフトウェアの開発を協調しながら並行に進める手法である。設計の初期段階ではハードウェアとソフトウェアをあえて区別せずにシステム全体の仕様を記述し，そこからハードウェアの設計とソフトウェアの設計を導き出す。上流工程におけるシステム方式・システム設計の段階でハードウェアとソフトウェアのいずれもが仕様を満たしていることを確認できる。

問7　ウ

解説　**イベント駆動型のアプリケーション**とは，データ入出力の終了やコマンドの入力などのイベントを引き金にして実行されるアプリケーションである。

DFD：システムに流れるデータを中心にデータと処理の流れを図式化したもの。

E-R図：取り扱うデータを実体（Entity），実体どうしの関係性を関連（Relationship）として，各データの関係性を表現したもの。

シーケンス図：クラスやオブジェクト間のやりとりを時間軸に沿って表現する図。

ペトリネット：非同期的かつ並列的に動作するシステムにおける情報の流れや制御を記述して，解析するために考案された図法。

問8　イ

解説　**フェールセーフ**とは，システムの障害や誤操作が発生することを想定し，発生した際の影響を最小限にするようにシステムを設計することである。例えば電車線路の踏切が故障した場合には，電車との衝突事故を回避するために自動的に遮断器をおろして事故を未然に防ぐ方向に動作する。

ア：乾電池のプラスとマイナスを逆にした状態で乾電池が入らないようにすることは，誤操作が発生しないように設計する考え方であり，**プールプルーフ**と呼ばれる。

ウ：故障した部分を切り離してシステムの運用を継続するという考え方は，**フォールトトレランス**の考え方である。

エ：**RAID1**（ミラーリング）のディスク構成は，ディスクシステムの故障率を低下させるための構成手法である。

問 9 正解 完璧 直前チェック

ソフトウェアの潜在エラー数を推定する方法の一つにエラー埋込み法がある。100個のエラーを意図的に埋め込んだプログラムを，そのエラーの存在を知らない検査グループがテストして30個のエラーを発見した。そのうち20個は意図的に埋め込んでおいたものであった。この時点で，このプログラムの**埋込みエラーを除く残存エラー数**は幾つと推定できるか。

ア　40　　イ　50　　ウ　70　　エ　150

問 10 正解 完璧 直前チェック

ハードウェアの経験が豊富なプログラマAと，経験の少ないプログラマBがペアプログラミングの手法を利用して組込みシステムの開発を進める。ペアプログラミングによる開発の進め方として，適切なものはどれか。

ア　Aがデバイスドライバの開発を担当し，Bがアプリケーションの開発を担当する。
イ　Aがプロジェクトマネージャとして，プロジェクトの調整役になる。
ウ　AとBがエディタの画面を共有し，Bが記述したコードに対してAが助言する。
エ　ハードウェアとソフトウェアの切分けをシミュレーションで検証してから，AとBとで分担して開発する。

問 11 正解 完璧 直前チェック

探索的テスト技法の説明はどれか

ア　起こり得る全ての条件と，それに対して実行すべき動作とを組み合わせた表に基づいてテストする技法
イ　経験に基づいて，起こりがちなエラーを推測してテストケースを決定する技法
ウ　経験や推測から重要と思われる領域に焦点を当ててテストし，その結果を基にした新たなテストケースを作成して，テストを繰り返す技法
エ　システムの取り得る状態と，状態を遷移させる事象又は条件を示した図に基づいてテストする技法

問9　ア

解説　**エラー埋込み法**とは，ソフトウェアのテストを行うときに故意にソフトウェアにエラーを埋め込むテスト手法。エラーを埋め込んだことを知らないテスト担当者がテストを実行し，テストにより発見されたエラーのなかに埋め込んだエラーが幾つかあるかをカウントし，その結果によりプログラムに残っている本来の検出すべきエラーの数を推定する方法。

検出すべきエラーの数をxとして，埋め込んだエラーの数との比率を表すと，

$30 : 20 = (x + 100) : 100$

$x = 50$

検出すべきエラーの数は50個と推定される。50個のうちすでに10個は発見されているから，残存エラー数は40個と推定できる。

問10　ウ

解説　**ペアプログラミング**は，2人1組でプログラム開発を行う手法である。1人がキー入力を担当し，プログラムの具体的なコードを作成して細かい機能を実装する。もう1人はプログラムの概要の確認，プログラムの簡潔化，エラーの検討など必要な調査を行う。

ア：別々のプログラムを別々に開発しているので，ペアプログラミングではない。
イ：プロジェクトの推進における役割分担である。
ウ：ペアプログラミングによる開発の進め方の説明である。
エ：**コデザイン**による開発手法の説明である。

問11　ウ

解説

ア：**デシジョンテーブル**を用いたテストケース設計技法に関する説明である。
イ：**エラー推測**と呼ばれる手法。過去のテスト事例を反映したテストケースが反映されるが，論理的・効率的とは必ずしもいえない。
ウ：**探索的テスト技法**に関する説明である。テスト仕様書によらずに経験や推測に基づいてテストケースを設定してテストを行い，その結果に基づいてさらにテストケースを設定してテストを繰り返していく手法。
エ：**状態遷移図**を用いた状態遷移テスト。

問 12 正解 完璧 直前チェック

故障の予防を目的とした解析手法であるFMEAの説明はどれか。

ア　個々のシステム構成要素に起こり得る潜在的な故障モードを特定し，それらの影響度を評価する。
イ　故障を，発生した工程や箇所などで分類し，改善すべき工程や箇所を特定する。
ウ　発生した故障について，故障の原因に関係するデータ，事象などを収集し，“なぜ”を繰り返して原因を掘り下げ，根本的な原因を追求する。
エ　発生した故障について，その引き金となる原因を列挙し，それらの関係を木構造で表現する。

問 13 正解 完璧 直前チェック

銀行の勘定系システムなどのような特定の分野のシステムに対して，業務知識，再利用部品，ツールなどを体系的に整備し，再利用を促進することによって，ソフトウェア開発の効率向上を図る活動や手法はどれか。

ア　コンカレントエンジニアリング　　イ　ドメインエンジニアリング
ウ　フォワードエンジニアリング　　エ　リバースエンジニアリング

問 14 正解 完璧 直前チェック

IT投資を，投資目的によって表のように分類した。IT投資評価のKPIのうち，戦略的投資に対するKPIの例はどれか。

分類	投資目的
業務効率投資	業務の効率向上，業務の生産性向上など
情報活用投資	ナレッジの共有，管理精度の向上など
戦略的投資	競争優位の確立，ビジネスの創出など
IT基盤投資	ITコスト削減，システム性能向上など

ア　システムの障害件数　　イ　新製品投入後の市場シェア
ウ　提案事例の登録件数　　エ　連結決算処理の所要日数

春 秋

問12　ア

解説　**FMEA**（Failure Mode and Effects Analysis）とは，製品やシステムの構成要素に発生する故障モード（Failure Mode）と呼ばれる故障状態，例えば劣化や摩耗，断線などの状態を分類して，それらが製品やシステムの故障にどのように影響を与えるかを解析する手法。

ア：FMEAに関する説明である。
イ：**故障解析**と呼ばれる手法の説明。
ウ：**なぜなぜ分析**と呼ばれる手法。問題の真の要因を追求するために“なぜ”を繰り返す。ある問題の原因を明らかにし，さらにその原因が発生した原因，つまり原因の原因を“なぜ”の繰り返しによって明らかにする。
エ：**FTA**（Fault Tree Analysis）に関する説明である。頂上に解析すべき事象を置き，その下にその原因となる事象を木構造で表現する。FMEAがボトムアップの手法であったのに対して，FTAはトップダウンの手法である。

問13　イ

解説

コンカレントエンジニアリング：製品の開発プロセスを構成する複数の工程を同時並行で進め，各部門間での情報共有や共同作業を行うことにより，開発期間の短縮やコストの削減を図る手法。
ドメインエンジニアリング：特定の分野のシステムに対して，業務知識，再利用部品，ツールなどを体系的に整備し，再利用を促進することによってソフトウェア開発の効率向上を図る活動や手法。
フォワードエンジニアリング：リバースエンジニアリングによって明らかになった既存のソフトウェアやシステムの仕様を利用して，新しいシステムやソフトウェアを開発すること。
リバースエンジニアリング：ソフトウェアやハードウェアの解析・分解を行い，その仕組みや仕様，要素技術を明らかにすること。

問14　イ

解説　**KPI**（Key Performance Indicator：重要業績指標）とは，目標の達成に向かって業務を遂行するときに，その進捗を測定するための指標である。問題では競争優位の確立が投資の目的と設定されているので，その目的の達成の測定・評価指標がKPIに用いられる。

戦略的投資によって競争優位が実現すれば市場シェアが拡大すると考えられるので，この場合のKPIは市場シェアである。

問 15 正解 完璧 直前チェック

グラントバックの説明はどれか。

ア　異なる分野で特許技術をもつ事業者同士が技術供与協定を締結し，お互いに無償で特許の実施権を許諾すること

イ　自社固有のビジネスモデルに関してビジネスモデル特許を取得した上で，無償で広くその利用を許諾すること

ウ　ライセンスを受けた者が特許技術を改良し，新たに取得した特許は，ライセンスを与えた者に実施権が許諾されること

エ　ライセンスを受けた者が特許技術を改良し，新たに取得した特許は，ライセンスを与えた者へ譲渡される義務が課されること

問 16 正解 完璧 直前チェック

システム開発における発注者とベンダとの契約方法のうち，実費償還型契約はどれか。

ア　委託業務の進行中に発生するリスクはベンダが負い，発注者は注文時に合意した価格を支払う。

イ　インフレ率や特定の製品の調達コストの変化に応じて，あらかじめ取り決められた契約金額を調整する。

ウ　契約時に，目標とするコスト，利益，利益配分率，上限額を合意し，目標とするコストと実際に発生したコストの差異に基づいて利益を配分する。

エ　ベンダの役務や技術に対する報酬に加え，委託業務の遂行に要した費用の全てをベンダに支払う。

問15　ウ

解説

ア：**クロスライセンス**に関する説明である。

イ：そのビジネスモデル特許を無償で許諾することにより，その特許が活用されるマーケットの拡大をはかる手法。競合他社が参入しやすくなるが，それよりも市場拡大の恩恵の方が大きいと考えられる場合に取られる手法。

ウ：**グラントバック契約**に関する説明である。「ライセンスを与えた者に実施権が許諾される」とは，ライセンスを受けた者が新たに取得した特許をライセンスを与えた者が実施する際，実際に技術を改良したライセンスを受けた者の許可は不要となることである。

エ：**アサインバック契約**に関する説明である。ライセンスを与えた者はライセンスを受けた者に対して，特許を譲渡させる見返りに実施権を与えたり対価を支払ったりする条項を設ける場合もある。

問16　エ

解説　**実費償還型契約**とは，実際に発生したコストに納入業者の利益を加えて価格を決定する契約形態である。契約前に作業の範囲を限定できない場合に利用される。作業が終了するまで全体のコストが確定しないというデメリットがある。

ア：**定額契約**に関する説明である。

イ：**経済価格調整つき定額契約**の説明である。

ウ：**定額インセンティブフィー契約**の説明である。

問 17

正解 □ 完璧 □ 直前チェック □

ビッグデータを有効活用し，事業価値を生み出す役割を担う専門人材であるデータサイエンティストに求められるスキルセットを表の三つの領域と定義した。データサイエンス力に該当する具体的なスキルはどれか。

データサイエンティストに求められるスキルセット

ビジネス力	課題の背景を理解した上で，ビジネス課題を整理・分析し，解決する力
データサイエンス力	人工知能や統計学などの情報科学に関する知識を用いて，予測，検定，関係性の把握及びデータ加工・可視化する力
データエンジニアリング力	データ分析によって作成したモデルを使えるように，分析システムを実装，運用する力

ア　扱うデータの規模や機密性を理解した上で，分析システムをオンプレミスで構築するか，クラウドコンピューティングを利用して構築するか判断し設計できる。

イ　事業モデルやバリューチェーンなどの特徴や事業の主たる課題を自力で構造的に理解でき，問題の大枠を整理できる。

ウ　分散処理のフレームワークを用いて，計算処理を複数サーバに分散させる並列処理システムを設計できる。

エ　分析要件に応じ，決定木分析，ニューラルネットワークなどのモデリング手法の選択，モデルへのパラメタの設定，分析結果の評価ができる。

問 18

正解 □ 完璧 □ 直前チェック □

表のCPIと構成比率で，3種類の演算命令が合計1,000,000命令実行されるプログラムを，クロック周波数が1 GHzのプロセッサで実行するのに必要な時間は何ミリ秒か。

演算命令	CPI（Cycles Per Instruction）	構成比率〔%〕
浮動小数点加算	3	20
浮動小数点乗算	5	20
整数演算	2	60

ア　0.4　　イ　2.8　　ウ　4.0　　エ　28.0

問17　エ

解説

ア：分析システムを実装するスキルであるから，**データエンジニアリング力**に該当する。

イ：主たる課題を理解や整理するスキルであるから，**ビジネス力**である。

ウ：並列処理システムを構築するスキルはスキルセットには含まれない。

エ：モデリング手法の選択やパラメタの設定，分析結果の評価は**データサイエンス力**に含まれるスキルである。

問18　イ

解説　CPIの列の数値は，各演算命令を実行するために必要となるクロックサイクル数である。各演算命令の実行に要する時間（クロックサイクル数）と，実行プログラムにおける構成比率が示されているので，このプログラム1命令当たりの平均実行時間（平均クロックサイクル数）の期待値は次式で求められる。

（各命令のCPI×構成比率）の和 $= 3 \times 0.2 + 5 \times 0.2 + 2 \times 0.6$

$= 2.8$〔クロックサイクル〕

したがって，このプログラムの実行に必要な時間は，

$2.8 \times 1{,}000{,}000 = 2.8 \times 10^6$〔クロック〕

となる。クロック周波数が1 GHzであるから，1クロックサイクルは$1/10^9 = 10^{-9}$〔秒〕となる。したがって，このプログラムを実行するために必要な時間は，

$2.8 \times 10^6 \times 10^{-9} = 2.8 \times 10^{-3}$〔秒〕$= 2.8$〔ミリ秒〕

となる。

問 19 正解 完璧 直前チェック

Webブラウザ や HTTP を用いず，独自の GUI とデータ転送機構を用いた，ネットワーク対戦型のゲームを作成する。仕様の(2)の実現に用いることができる仕組みはどれか。

〔仕様〕

(1) ゲームは囲碁や将棋のように2人のプレーヤの間で行われ，ゲームの状態はサーバで管理する。プレーヤはそれぞれクライアントプログラムを操作してゲームに参加する。

(2) プレーヤが新たな手を打ったとき，クライアントプログラムはサーバにある関数を呼び出す。サーバにある関数は，その手がルールに従っているかどうかを調べて，ルールに従った手であればゲームの状態を変化させ，そうでなければその手が無効であることをクライアントプログラムに知らせる。

(3) ゲームの状態に変化があれば，サーバは各クライアントプログラムにその旨を知らせることによって GUI に反映させる。

ア CGI　　イ PHP　　ウ RPC　　エ XML

問 20 正解 完璧 直前チェック

マルチプロセッサによる並列処理で得られる高速化率（単一プロセッサのときと比べた倍率）Eを，次の式によって評価する。$r = 0.9$のアプリケーションの高速化率が$r = 0.3$のものの3倍となるのは，プロセッサが何台のときか。

$$E = \frac{1}{1 - r + \frac{r}{n}}$$

ここで，

n：プロセッサの台数（$1 \leqq n$）

r：対象とする処理のうち，並列化が可能な部分の割合（$0 \leqq r \leqq 1$）

とし，並列化に伴うオーバヘッドは考慮しないものとする。

ア 3　　イ 4　　ウ 5　　エ 6

春 秋

問19　ウ

解説

CGI（Common Gateway Interface）：Webサーバ上でプログラムを動作させる仕組み。

PHP（Hypertext Preprocessor）：Webサーバ上で動作するスクリプト言語。PHPスクリプトが呼び出されると動的にWebページを生成し，Webブラウザにその生成結果を送信する。

RPC（Remote Procedure Call）：ネットワークを経由して他のコンピュータ上のプログラムやサブルーチンを実行させる仕組み。引数と処理実行のメッセージを他のコンピュータに送信することにより，送信先のコンピュータ上でメッセージに基づいて処理が実行される。

XML（eXtensible Markup Language）：拡張可能なマークアップ言語である。マークアップ言語とは文書の構造や見栄えの指定を記述する言語である。文書の構造や見栄えを記述する際に用いられる「タグ」をユーザ側で設定・追加できる。

問20　エ

解説　設問より，$r = 0.9$のときの高速化率（E）を$r = 0.3$のときの高速化率の3倍となるように式を構成する。

$$\frac{1}{1 - 0.9 + \frac{0.9}{n}} = 3 \times \frac{1}{1 - 0.3 + \frac{0.3}{n}}$$

$$\frac{n}{0.1n + 0.9} = \frac{3n}{0.7n + 0.3}$$

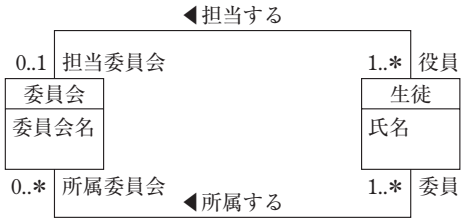
$$0.7n + 0.3 = 0.3n + 2.7$$

$$n = 6$$

したがって，必要となるプロセッサの台数は6台である。

問 21 正解 完璧 直前チェック

UMLを用いて表した図のデータモデルを基にして設計したテーブルのうち，適切なものはどれか。ここで，“担当委員会ID”と“所属委員会ID”は“委員会ID”を参照する外部キーである。“役員ID”と“委員ID”は“生徒ID”を参照する外部キーである。実線の下線は主キー，破線の下線は外部キーを表す。



ア　委員会（委員会ID，委員会名）
　　所属関連（所属委員会ID，委員ID）
　　生徒（生徒ID，氏名，担当委員会ID）

イ　委員会（委員会ID，委員会名）
　　役員関連（担当委員会ID，役員ID）
　　生徒（生徒ID，氏名，所属委員会ID）

ウ　委員会（委員会ID，委員会名，委員ID）
　　生徒（生徒ID，氏名，所属委員会ID，担当委員会ID）

エ　委員会（委員会ID，委員会名，役員ID）
　　生徒（生徒ID，氏名，所属委員会ID）

問21　ア

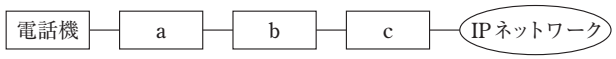
解説　設問の図より，生徒は複数の委員会に所属する可能性がある。選択肢イ，ウ，エの生徒テーブルには“生徒ID”を主キーとして“所属委員会ID”が含まれているが，これでは生徒は一つの委員会にしか所属できない。したがって，選択肢イ，ウ，エのテーブル構成はいずれも不適切である。

選択肢アのテーブルでは，生徒テーブルには“担当委員会ID”が含まれている。図より，生徒が役員として担当する委員会は一つ，もしくは担当なしであるから，このテーブルは正しい。

また，委員として複数の委員会に所属する状態は所属関連テーブルで表している。所属関連テーブルでは“所属委員会ID”と“委員ID”の組が主キーとなっているから，委員会と所属する生徒の全ての組をテーブルにすればよい。

問 22 正解 完璧 直前チェック

図は，既存の電話機とPBXを使用した企業内の内線網を，IPネットワークに統合する場合の接続構成を示している。図中のa～cに該当する装置の適切な組合せはどれか。



	a	b	c
ア	PBX	VoIPゲートウェイ	ルータ
イ	PBX	ルータ	VoIPゲートウェイ
ウ	VoIPゲートウェイ	PBX	ルータ
エ	VoIPゲートウェイ	ルータ	PBX

問 23 正解 完璧 直前チェック

署名されたソフトウェアを導入する前に，そのソフトウェアの開発元又は発行元を確認するために使用する証明書はどれか。

ア　EV SSL証明書　　イ　クライアント証明書
ウ　コードサイニング証明書　　エ　サーバ証明書

問 24 正解 完璧 直前チェック

米国NISTが制定した，AESにおける鍵長の条件はどれか。

ア　128ビット，192ビット，256ビットから選択する。
イ　256ビット未満で任意に指定する。
ウ　暗号化処理単位のブロック長よりも32ビット長くする。
エ　暗号化処理単位のブロック長よりも32ビット短くする。

問22　ア

解説　**PBX**（Private Branch eXchange：構内交換機）とは，企業などの構内に設置された内線電話の交換機である。PBXを介して電話機をIPネットワークに接続するためには，**VoIP**（Voice over Internet Protocol）**ゲートウェイ**を用いて音声データをIPパケットに変換する。変換された音声データは，**ルータ**を介してIPネットワークに接続される。よって選択肢アが正解である。

問23　ウ

解説

EV SSL証明書：SSL（Secure Sockets Layer）とはインターネット上で暗号化通信を行うプロトコルである。SSL証明書はWebサーバとWebクライアントの間の通信がSSL暗号化されていることを証明する証明書である。EV SSL証明書はこれをさらに厳格にしたもので，フィッシング詐欺などの対策などに利用されている。

クライアント証明書：PCやデバイスにインストールされて，その利用者が正しい利用者であることを証明する電子証明書。

コードサイニング証明書：ソフトウェアの開発元や配布者が正しいことを確認するための証明書である。インターネット経由でダウンロードするソフトウェアには改ざんされたものであったりウイルスに感染したものであったりする危険性があるので，コードサイニング証明書を確認することで危険性を回避できる。

サーバ証明書：SSL通信などの暗号化通信で使用するサーバ側の電子証明書。暗号化の鍵やサーバの所有者情報，署名などが含まれている。

問24　ア

解説　米国の**NIST**（National Institute of Standards and Technology：米国国立標準技術研究所）は，工業技術の標準化を支援する機関である。

AES（Advanced Encryption Standard）は，米国政府標準の共通鍵暗号方式である。共通鍵暗号方式では暗号化鍵と復号鍵に同じ鍵を使用するため，鍵を共有する手続きが必要である。鍵長は128ビット，192ビット，256ビットから選択可能なSPN型ブロック暗号である。ブロック長は128ビットとなっている。よって選択肢アが正解である。

問 25

正解 □ 完璧 □ 直前チェック □

スパムメール対策として，サブミッションポート（ポート番号587）を導入する目的はどれか。

ア　DNSサーバにSPFレコードを問い合わせる。
イ　DNSサーバに登録されている公開鍵を用いて署名を検証する。
ウ　POP before SMTPを使用して，メール送信者を認証する。
エ　SMTP-AUTHを使用して，メール送信者を認証する。

問25　エ

解説　スパムメール対策として**OP25B**（Outbound Port 25 Blocking）を行うと，25番のポート番号を使用するSMTPは外部のメールサーバに接続できなくなる。外部のメールサーバに接続するためには，ポート番号587で接続し，ユーザ認証機能をもつ**SMTP-AUTH**を使用する。このポートを**サブミッションポート**と呼ぶ。したがって選択肢エが正解である。

ア：**SPF**（Sender Policy Framework）は，電子メールの送信者詐称を防ぐ送信ドメイン認証技術である。DNSサーバに問い合わせて差出人アドレスに記載されたドメイン名を調べ，詐称していないかどうかを判断する。そのため差出人アドレスを詐称していない迷惑メールは検出できない。

イ：DNSサーバに公開鍵を用いて署名を検証するのは，DNSSECである。

ウ：**POP before SMTP**は，POP3で認証できたユーザと接続先のIPにのみSMTPメールを送信することを認可する。これによりSMTPにユーザ認証機能を付与するものである。