# 問題

## 問 1

正解 完璧 直前CHECK

UMLを使って図のクラスPを定義した．このクラスの操作のうち，公開可視性（public）をもつものはどれか．

| クラスP |
|---|
| + 操作A |
| − 操作B |
| # 操作C |

ア　全ての操作　　イ　操作A　　ウ　操作B　　エ　操作C

## 問 2

正解 完璧 直前CHECK

論理データモデル作成におけるトップダウンアプローチ，ボトムアップアプローチに関する記述のうち，適切なものはどれか．

ア　トップダウンアプローチでは，新規システムの利用者要求だけに基づいて論理データモデルを作成するので，現状業務の分析は行えない．
イ　トップダウンアプローチでもボトムアップアプローチでも，最終的な論理データモデルは正規化され，かつ，業務上の属性は全て備えていなければならない．
ウ　トップダウンアプローチでもボトムアップアプローチでも，利用者が使用する現状の画面や帳票を素材として分析を行うのは同じである．
エ　ボトムアップアプローチは現状業務の分析に用いるものであり，新規システムの設計ではトップダウンアプローチを使用する．

## 問 3

正解 完璧 直前CHECK

要件定義フェーズにおいてBPMN（Business Process Modeling Notation）を導入する効果として，適切なものはどれか．

ア　業務の実施状況や実績を定量的に把握できる．
イ　業務の流れを統一的な表記方法で表現できる．
ウ　定義された業務要件からデータモデルを自動生成できる．
エ　要件をE-R図によって明確に表現できる．

## 問1　イ

**UML**のクラス図は**クラス名**，**属性**，**操作**の要素から構成される．属性や操作の可視性と意味は以下の表の通りである．クラスPで公開可視性（public）を持つのは選択肢イの操作Aである．

クラス図

| クラス名 |
| --- |
| **属性**（省略可） |
| **操作**（省略可） |

**可視性　名前：型 = 初期値 ｛制約条件｝**
**可視性　名前（引数の名前：引数の型）：戻りの型**
※名前以外は省略可能

| 可視性 | 意味 |
| --- | --- |
| + | public：全てにおいて参照可能 |
| - | private：自クラスでのみ参照可能 |
| # | protected：自クラス及びその派生クラスにおいて参照可能 |
| ~ | package：同パッケージ内で参照可能 |

## 問2　イ

**トップダウンアプローチ**：経営者や組織のトップからの要求事項に基づいて論理データモデルを作成する．

**ボトムアップアプローチ**：利用者などとの接点から要求事項を集めて論理データモデルを作成する．

ア：利用者要求に基づいたアプローチはボトムアップアプローチである．

イ：正しい．トップダウンアプローチ，ボトムアップアプローチのどちらを利用しても良い．最終的には業務上の属性が必要になる．

ウ：利用者が使用する現状の画面や帳票は現場からの仕様であるため，ボトムアップアプローチである．

エ：新規システムの設計では，トップダウンアプローチ，ボトムアップアプローチのいずれでも良い．現場からの要求事項に基づいて新規システムを設計するケースもある．

## 問3　イ

**BPMN**（Business Process Modeling Notation）：ビジネスプロセス（業務手順）を図によって可視化するためのルールを定義したものである．図によって業務を容易に理解できるようになる．

# 問題

## 問 4

正解 完璧 直前CHECK

ソフトウェア方式設計時の“ソフトウェア構造とコンポーネントの方式設計”において，機能要求を実現するための各オブジェクトの作業分担を記述するのに適した図はどれか．

ア　コミュニケーション図　　イ　コンポーネント図
ウ　ステートマシン図　　エ　ユースケース図

## 問 5

正解 完璧 直前CHECK

モジュールの独立性を高めるには，モジュール結合度を弱くする必要がある．モジュール間の情報の受渡し方法のうち，モジュール結合度が最も弱いものはどれか．

ア　共通域に定義したデータを関係するモジュールが参照する．
イ　制御パラメタを引数として渡し，モジュールの実行順序を制御する．
ウ　入出力に必要なデータ項目だけをモジュール間の引数として渡す．
エ　必要なデータを外部宣言して共有する．

## 問 6

正解 完璧 直前CHECK

ソフトウェア開発における分析・設計技法と，その技法における着目点の説明のうち，適切なものはどれか．

ア　DFDを用いた分析・設計技法では，データの流れに着目する．
イ　E-R図を用いた分析・設計技法では，事象と状態の変化に着目する．
ウ　HIPOを用いた分析・設計技法では，対象となるオブジェクトの関連に着目する．
エ　ペトリネットを用いた分析・設計技法では，処理機能に着目する．

## 問4　ア

機能要求を実現するための各オブジェクトの作業分担を記述する図法として適しているのは選択肢アの**コミュニケーション図**である．

**コミュニケーション図**：クラスやオブジェクト間の応答（相互作用）と関連の両方を表現する．

**コンポーネント図**：コンポーネントの内部構造ならびにコンポーネント間の依存関係を表現する．

**ステートマシン図**：イベントにより引き起こされるオブジェクトの状態遷移を表現する．

**ユースケース図**：ユーザなど外部からの要求に対するシステムの振る舞いを表現する．

## 問5　ウ

**モジュール結合度**の弱い順に列挙すると，データ結合，スタンプ結合，制御結合，外部結合，共通結合，内部結合となる．結合度は弱いほうが望ましい．

ア：**共有結合**である．

イ：**制御結合**である．

ウ：**データ結合**である．

エ：**外部結合**である．

なお，**スタンプ結合**はデータ構造（構造体，レコード）を含んだ引数を受け渡すもので，**内部結合**は外部変数宣言をしていないデータを他のモジュールが直接参照するものである．

## 問6　ア

ア：**DFD**を用いた分析・設計技法は，データの流れに着目する．

イ：**E-R**図を用いた分析・設計技法は，実体（エンティティ）とその関係（リレーション）に着目する．

ウ：**HIPO**図を用いた分析・設計技法は，処理機能に着目する．

エ：**ペトリネット図**を用いた分析・設計技法は，オブジェクトの関連に着目する．

# 問題

## 問 7

正解 完璧 直前CHECK

データ中心アプローチに関する記述のうち，最も適切なものはどれか．

ア　データ資源の重複だけでなく，データを更新するプロセスの重複も排除することを目的としている．

イ　データとその処理手順のカプセル化に見られるように，オブジェクト指向の方法論をデータベース設計に応用しようとする試みである．

ウ　データの流れに着目してシステム分析を行い，再利用可能なモジュールを抽出することによってソフトウェアの生産性を向上させることを目的としている．

エ　プログラム設計では，構造化設計技法を用いて業務システムを機能分割する必要がある．

## 問 8

正解 完璧 直前CHECK

出力帳票の1ページごとにヘッダと30件分のレコードを出力するプログラムをテストしたい．このプログラムを限界値分析によってテストするための最少のテストデータを用意するとき，レコード件数の組合せとして，適切なものはどれか．

ア　0，1，31　　イ　0，1，20，31

ウ　0，1，30，31　　エ　0，1，20，30，31

## 問7　ア

**データ中心アプローチ**：業務で扱うデータの構造や流れに着目し，システム設計を行う手法．業務で扱うデータ全体をERモデルによってモデル化し，それを正規化して関係データベース（RDB）を設計する．統一したデータベースによりデータの整合性・一貫性が保たれ，システム間のやりとりも容易になる．

## 問8　ウ

**限界値分析**とは，入力値の範囲などをチェックする際に利用されるテストデータの設計手法である．境界の前後の入力データをテストデータとする．つまり，テストデータには最小値の直前の値，最小値，最大値，最大値の直後の値を用意する．

出力帳票の1ページごとにヘッダと30件分のレコードを出力するプログラムをテストするための最少のテストデータは，「0，1，30，31」である．

# 問題

## 問 9

正解 完璧 直前CHECK

並列処理プログラミングの特徴を説明したものはどれか.

ア　複数のシステムを用いて，一方ではオンライン処理を実行し，他方ではバッチ処理などの優先度が低い処理を実行する．オンライン処理を実行しているシステムに障害が発生した際には，バッチ処理を実行していたシステムがオンライン処理を引き継ぐ．オンライン処理の可用性を高める．

イ　複数のシステムを用いて，同時に同じデータを用いて同じ処理を行う．処理結果を照合し，その結果が一致することを確認する．処理結果の信頼性を高める．

ウ　複数の処理装置を用いて，それぞれにネットワーク処理専用，演算処理専用，データベース処理専用などと役割を決めてお互いを接続する．各装置が役割に応じた処理をすることで，負荷を分散する．システム全体の処理性能を向上させる．

エ　複数の処理装置を用いて，一つのプログラムで行う処理内容を複数に分けて，それぞれの処理装置で実行する．各処理装置で得られた結果は，最終的に一つの結果にまとめる．単一の処理装置だけでは実現できない高速な処理を実現する．

## 問 10

正解 完璧 直前CHECK

アジャイルソフトウェア開発などで導入されている“ペアプログラミング”の説明はどれか.

ア　開発工程の初期段階に要求仕様を確認するために，プログラマと利用者がペアとなり，試作した画面や帳票を見て，相談しながらプログラムの開発を行う.

イ　効率よく開発するために，2人のプログラマがペアとなり，メインプログラムとサブプログラムを分担して開発を行う.

ウ　短期間で開発するために，2人のプログラマがペアとなり，作業と休憩を交代しながら長時間にわたって連続でプログラムの開発を行う.

エ　品質の向上や知識の共有を図るために，2人のプログラマがペアとなり，その場で相談したりレビューしたりしながら，一つのプログラムの開発を行う.

## 問9　エ

**並列処理プログラミング**：一つのプログラムで行う処理を複数に分けて，複数の処理装置を用いて実行する．単一の処理装置よりも高速な処理を実現し，各処理装置の結果は一つにまとめられる．

ア：**双方向スタンバイ型クラスタシステム**の説明である．

イ：**デュアルシステム**の説明である．

ウ：**機能分散**の説明である．

## 問10　エ

**アジャイルソフトウェア開発**：ソフトウェア要求仕様の変更に対して機敏に対応して，顧客に価値あるソフトウェアを迅速に提供することを目的とするソフトウェア開発方法論．

**ペアプログラミング**：二人のプログラマがペアになって，コーディング担当とチェックやアドバイスを担当する係りに分かれて相談したり，レビューをしたりしながら一つのプログラムの開発を行うこと．

# 問題

## 問 11

正解 完璧 直前CHECK

ソフトウェア開発手法の特徴に関する記述のうち，適切なものはどれか．

ア　ウォータフォールモデルは，要件定義，設計，プログラミング，テストの順に作業が流れていくので，エンドユーザプログラミングに最適である．

イ　スパイラルモデルは，要件定義，設計，プログラミング，テストを循環的に繰り返すので，未確定の要求があるシステムを開発する場合に有効である．

ウ　成長モデルは，実際に運用するシステムを作る前に評価モデルを作り，評価，改良を繰り返すので，システムの仕様や性能の早期確定に有効である．

エ　プロトタイピングは，スパイラルモデルを改良した方法であり，機能分割と段階的な機能追加を繰り返すので，大規模システム開発に最適である．

## 問 12

正解 完璧 直前CHECK

投資効果を現在価値法で評価するとき，最も投資効果の大きい（又は損失の小さい）シナリオはどれか．ここで，期間は3年間，割引率は5％とし，各シナリオのキャッシュフローは表のとおりとする．

単位　万円

| シナリオ | 投資額 | 回収額 | | |
|---|---|---|---|---|
| | | 1年目 | 2年目 | 3年目 |
| A | 220 | 40 | 80 | 120 |
| B | 220 | 120 | 80 | 40 |
| C | 220 | 80 | 80 | 80 |
| 投資をしない | 0 | 0 | 0 | 0 |

ア　A　　イ　B　　ウ　C　　エ　投資をしない

## 問11　イ

ア：**ウォータフォールモデル**はエンドユーザプログラミングには不適である．

ウ：**成長モデル**はウォータフォールモデルを改良した方法である．システムの仕様の変更があるたびにソフトウェア開発工程を繰り返す．

エ：**プロトタイピング**は，システムを試作して要求仕様の確認・評価，ユーザインタフェースの確定や性能確認を行い，後続段階での仕様変更による後戻りを防ぐ手法である．スパイラルモデルを改良したものではない．

## 問12　イ

**現在価値法**：投資の適否を判断するときの基準の一つ．将来のキャッシュフローを現在価値に直して，それをすべて合計することで算出する．一般的には**現在価値＞資本コスト**となる場合に投資すべきだと判断する．

現在価値 = 将来価値 ／ 利回り年数

問題のシナリオA～Cは，いずれも投資額220万円に対して3年間の回収額は240万円となっており，20万円の利益がある．投資をしないというシナリオはなくなる．回収額についてはシナリオB＞シナリオC＞シナリオAの順に早期に回収できることから，割引率を考慮し，最も投資効果が大きいのはシナリオBである．

## 問 13

正解 完璧 直前CHECK

BABOKの説明はどれか.

ア　ソフトウェア品質の基本概念，ソフトウェア品質マネジメント，ソフトウェア品質技術の三つのカテゴリからなる知識体系

イ　ソフトウェア要求，ソフトウェア設計，ソフトウェア構築，ソフトウェアテスティング，ソフトウェア保守など10の知識エリアからなる知識体系

ウ　ビジネスアナリシスの計画とモニタリング，引き出し，要求アナリシス，基礎コンピテンシなど七つの知識エリアからなる知識体系

エ　プロジェクトマネジメントに関して，スコープ，時間，コスト，品質，人的資源，コミュニケーション，リスク管理など九つの知識エリアからなる知識体系

## 問 14

正解 完璧 直前CHECK

システムの非機能要件となるものはどれか.

ア　システム化を実現する業務の範囲

イ　システム内での情報（データ）の流れ

ウ　システムの操作性

エ　他システムとのインタフェースのレイアウト

## 問13　ウ

**BABOK**（Business Analysis Body of Knowledge）：ビジネス分析のための知識体系．次の七つの知識エリアの知識体系からなる．

(1) ビジネスアナリシスの計画とモニタリング
(2) 要求の管理と伝達
(3) エンタープライズ分析
(4) 要求の引き出し
(5) 要求の分析
(6) ソリューションの評価と妥当性確認
(7) コンピテンシ

## 問14　ウ

**機能要件**：システムがユーザに提供する機能の観点から，インタフェース，プロセス，データ項目等を定義したもの．

**非機能要件**：性能や信頼性，拡張性，セキュリティなど，機能要件以外のもの全般．

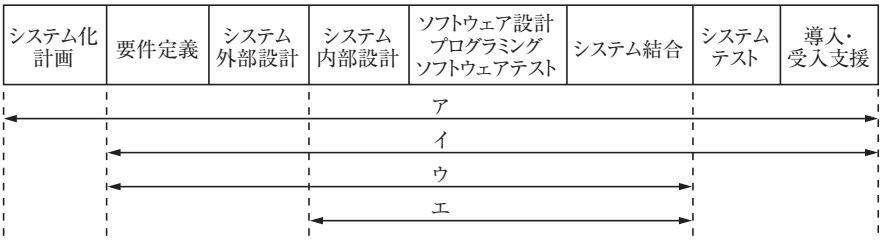
ア，イ，エはいずれも機能要件である．

# 問題

## 問 15

正解 □ 完璧 □ 直前CHECK □

経済産業省の“情報システム・モデル取引・契約書”によれば，ユーザとベンダ間で請負型の契約を推奨しているフェーズはどれか．




ア　システム化計画フェーズから導入・受入支援フェーズまで
イ　要件定義フェーズから導入・受入支援フェーズまで
ウ　要件定義フェーズからシステム結合フェーズまで
エ　システム内部設計フェーズからシステム結合フェーズまで

## 問 16

正解 □ 完璧 □ 直前CHECK □

エンタープライズアーキテクチャにおいて，ビジネスアーキテクチャの成果物である機能情報関連図（DFD）を説明したものはどれか．

ア　業務・システムの処理過程において，情報システム間でやりとりされる情報の種類及び方向を図式化したものである．
イ　業務を構成する各種機能を，階層化した３行３列の格子様式に分類して整理し，業務・システムの対象範囲を明確化したものである．
ウ　最適化計画に基づき決定された業務対象領域の全情報（伝票，帳票，文書など）を整理し，各情報間の関連及び構造を明確化したものである．
エ　対象の業務機能に対して，情報の発生源と到達点，処理，保管，それらの間を流れる情報を，統一記述規則に基づいて表現したものである．

## 問15　エ

経済産業省の**情報システム・モデル取引・契約書**は，情報システムの信頼性向上・取引の可視化に向けた取引・契約のあり方等の議論及びパブリックコメントを集約したものである．

請負型の契約を推奨しているのは，システム内部設計からソフトウェア設計，プログラミング，ソフトウェアテスト，システム結合までである．ユーザによるフェーズやユーザと共同で行うフェーズは請負型にすべきではない．

ユーザとベンダとの間の取引形態については，推奨では「モデル取引・契約のポイント」に記載されている．

<table>
<tr><th>取引・契約にモデル<br>におけるフェーズ分け</th><th>モデル契約書雛形における<br>個別業務と契約類型</th></tr>
<tr><td>システム化計画</td><td>対象外</td></tr>
<tr><td>要件定義</td><td>準委任型</td></tr>
<tr><td>システム外部設計</td><td>準委任型もしくは請負型の選択</td></tr>
<tr><td>システム内部設計</td><td rowspan="4">請負型</td></tr>
<tr><td>ソフトウェア設計<br>プログラミング<br>ソフトウェアテスト</td></tr>
<tr><td>システム結合</td></tr>
<tr><td>システムテスト</td><td>準委任型もしくは請負型の選択</td></tr>
<tr><td>導入・受入支援</td><td>準委任型</td></tr>
</table>

## 問16　エ

**エンタープライズアーキテクチャ**：政府機関や大企業における業務手順や情報システムの標準化，組織の最適化を進め，効率よい組織の運営を図るための方法論．

ア：**情報システム関連図**の説明である．

イ：**機能構成図**の説明である．

ウ：**情報体系整理図**の説明である．

## 問 17

正解 完璧 直前CHECK

BCP策定に際して，目標復旧時間となるものはどれか．

ア　災害時に代替手段で運用していた業務が完全に元の状態に戻るまでの時間
イ　災害による業務の停止が深刻な被害とならないために許容される時間
ウ　障害発生後のシステムの縮退運用を継続することが許容される時間
エ　対策本部の立上げや判定会議の時間を除く，待機系への切替えに要する時間

## 問 18

正解 完璧 直前CHECK

グリッドコンピューテイングの説明はどれか．

ア　OSを実行するプロセッサ，アプリケーションを実行するプロセッサというように，それぞれの役割が決定されている複数のプロセッサによって処理を分散する方式である．
イ　PCから大型コンピュータまで，ネットワーク上にある複数のプロセッサに処理を分散して，大規模な一つの処理を行う方式である．
ウ　カーネルプロセスとユーザプロセスを区別せずに，基本的に同等な役割の複数のプロセッサに処理を分散する方式である．
エ　プロセッサ上でスレッド（プログラムの実行単位）レベルの並列化を実現し，プロセッサの利用効率を高める方式である．

## 問 19

正解 完璧 直前CHECK

光源からの光を微小な鏡に反射させ，その反射光を拡大投影する動作方式をとるプロジェクタはどれか．

ア　CRT　　イ　DLP　　ウ　LCD　　エ　PDP

## 問17　イ

**BCP**（Business Continuity Plan，事業継続計画）**策定**：自然災害，伝染病，停電などによる都市機能のマヒや情報セキュリティインシデント等が発生した際に，事業継続できるように必要な組織体制・対策などをあらかじめ決めておくこと．

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では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停止が許されると考えられる目標時間が定義されている．よって，BCP策定の目標復旧時間の正解は，災害による業務停止が深刻な被害とならないために許容される時間である．

## 問18　イ

**グリッドコンピューティング**：ネットワーク上にある複数のコンピュータのプロセッサに処理を分散して，仮想的に高性能なコンピュータを構成したりメモリやストレージなどの資源配分を行ったりして，大規模な一つの処理を行う方式のこと．

ア：**非対称型マルチプロセッサ**の説明である．

ウ：**対称型マルチプロセッサ**の説明．2個のプロセッサを用いる場合にはデュアルプロセッシングと呼ぶことがある．

エ：**ハードウェアマルチスレッド**の説明．インテル社のプロセッサではハイパースレッディングと呼んでいる．

## 問19　イ

**CRT**：ブラウン管を利用した表示装置．液晶ディスプレイ（LCD）が主流になるまでパソコンやテレビとして多く利用されていた．装置の奥に備えられた電子ビームから前面の蛍光幕に照射することにより像を発生させる．

**DLP**：光半導体に実装された極めて小さな鏡（マイクロミラー）を電気信号で制御して光源からの光を反射し，その反射光をプロジェクションレンズに通して映像を発生させる装置．

**LCD**：液晶を利用した表示装置．2枚のガラス板の間に封入した液晶に電圧をかけることによって液晶分子の向きを変化させ，光源からの光の透過率を増減させて映像を発生させる．光源にはLEDやCCFL（冷陰極管）が用いられる．

**PDP**：ガラス板に封入した高圧の希ガスに高い電圧をかけて，ガスを発光させることによって映像を発生させる装置．

## 問 20

正解 完璧 直前CHECK

キャパシティプランニングで行うことはどれか.

ア　コンピュータシステムで，操作ミスや設計上の不具合などの障害が発生することをあらかじめ想定し，被害が最小限になるように対策を検討する.

イ　コンピュータシステムに効率よく投資するために，性能，経済性及び拡張性を考えてシステムの構成を決定する.

ウ　コンピュータシステムのデータを適切に保護する観点から，誰にデータのアクセスを許可するか，データを暗号化して格納するか否かなどを決める.

エ　コンピュータシステムを複数台の機器で構成し，機器のうちの1台が故障しても処理を続行したままで修理や故障した機器の交換ができるようにする.

## 問 21

正解 完璧 直前CHECK

次数がnの関係Rには，属性なし（φ）も含めて異なる射影は幾つあるか.

ア　n　　イ　2n　　ウ　$n^2$　　エ　$2^n$

## 問 22

正解 完璧 直前CHECK

磁気ディスク装置や磁気テープ装置などのストレージ（補助記憶装置）を，通常のLANとは別の高速な専用ネットワークで構成する方式はどれか.

ア　DAFS　　イ　DAS　　ウ　NAS　　エ　SAN

## 問20　イ

**キャパシティプランニング**：システムに求められる処理能力（ピーク時性能，同時利用ユーザ数など），サービスレベル（トランザクション量やネットワークトラフィック），システム数，システム増強や再配置を考えて最適なシステム構成を計画すること．

ア：**フールプルーフ**についての説明である．

ウ：**データ保護**についての説明である．

エ：障害が発生したときに性能を落としたり機能を制限したりして，限定的ながら稼働を続行する**縮退運転**（フォールバック）の説明である．

## 問21　エ

**射影**とは，関係データベースにおいて元表からいくつかの属性（列）を取り出す演算である．属性Rの次数がnの場合，射影の組合せは次のようになる．

取り出す属性が0個の場合　→　${}_nC_0$通り
取り出す属性が1個の場合　→　${}_nC_1$通り
取り出す属性が2個の場合　→　${}_nC_2$通り
…　…
取り出す属性がn個の場合　→　${}_nC_n$通り

となる．したがって，異なる射影の総数は次のように求められる．

${}_nC_0 + {}_nC_1 + {}_nC_2 + \cdots + {}_nC_n = (1+1)^n$通り$= 2^n$通り

## 問22　エ

**DAFS**（Direct Access File System．OSを介さずにネットワーク越のファイルの読み書きを高速に行えるようにした方式．高速アクセス，低遅延が特徴．

**DAS**（Direct Attached Storage）：一つのサーバと一つ以上のストレージ装置が接続された形態．

**NAS**（Network Attached Storage）：ネットワークによりストレージ装置が接続された形態．

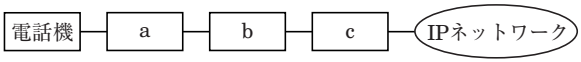
**SAN**（Storage Area Network）：ストレージ装置間とコンピュータの間を接続する専用の高速なネットワーク．

# 問題

## 問 23

正解 完璧 直前CHECK

図は，既存の電話機とPBXを使用した企業内の内練網を，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 24

正解 完璧 直前CHECK

暗号方式のうち，共通鍵暗号方式はどれか．

ア　AES　　イ　ElGamal　　ウ　RSA　　エ　楕円曲線暗号

## 問 25

正解 完璧 直前CHECK

何らかの理由で有効期間中に失効となっ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23　ア

**PBX**：企業などで内線電話同士の接続や，加入者電話網やISDN回線などの公衆回線への接続を行う機器．構内交換機．

**VoIPゲートウェイ**：電話網とIPネットワークの間の中継を行う機器．

本問は，既存の電話機とPBXを使用した企業内の内線網をIP化する接続構成のうち，電話機とIPネットワークの間の三つの装置の接続順が問われている．既存の電話機が接続できるのはPBXであり，次に接続するのは電話をIP化するVoIPゲートウェイで，次にルータを介してIPネットワークに接続する．

## 問24　ア

米国政府標準暗号方式の**AES**（Advanced Encryption Standard）は，共通鍵暗号方式である．一方，選択肢イ～エはいずれも公開鍵暗号方式である．

イ：ElGamalが開発した公開鍵暗号方式．離散対数問題とよばれる数学の問題を応用したもの．平文と乱数と公開鍵から暗号文を生成し，秘密鍵で復号する．

ウ：**RSA**は，3名の発案者（R.Rivest, A.Shamir, L.Adleman）の頭文字から名付けられた公開鍵暗号方式であり，解読するには大きな二つの素数から成る整数を素因数分解する必要がある．この暗号の効率の良い解読方法はいまだ発見されていない．

エ：楕円曲線と呼ばれる数式によって定義される特殊な加算法に基づいて暗号化・復号を行う暗号方式．RSAよりも短い鍵で安全性が確保できる．

## 問25　エ

**CA**（Certificate Authority）：電子証明書を発行，管理する機関．認証局．

**CP**（Certificate Policy）：証明書ポリシー．電子証明書に関して，利用目的，適用範囲，セキュリティ基準，電子証明書の発行等に係る審査基準などの規則を定めるもの．

**CPS**（Certification Practice Statement）：認証局（CA）を運用する際に証明書の利用目的を定める証明書ポリシー（CP：Certificate Policy）と，CAの運用方法を定める認証実施規定のこと．

**CRL**（Certificate Revocation List）：有効期間内に無効（取消）になった公開鍵証明書のシリアル番号の一覧．証明書失効リスト．