

問題1 次の（１）～（２０）の記述について、正しいものには○、間違っているものには×を解答欄に記入しなさい。

- （１）ブラックボックステストとは、内部構造は意識せず、アプリケーションの機能がシステム要件定義書通りに動作しているか確認するテストである。
- （２）CSS とは Web ページの論理構造を指定する言語である。
- （３）システム構成においてデュアルシステムとは、メインで動作するコンピュータと、障害発生時に対処するため待機しているコンピュータの２つのコンピュータからなるシステム構成のことである。
- （４）MTBF とは、システムが故障せずに正常動作していた時間の平均値である。
- （５）SSL/TLS は、ハイブリッド暗号方式である。
- （６）PKI とは、公開鍵の持ち主を保証するための社会的基盤である。
- （７）Open Source Software は著作権が放棄されている。
- （８）アジャイル開発とは、ソフトウェアの開発とリリースを繰り返し、ビジネス環境の変化やユーザーの仕様変更に対応する開発モデルのことである。
- （９）オンプレミスとは、他社のデータセンター内に自社のサーバを置くサービスのことである。
- （１０）個人情報のうち、犯罪の経歴は要配慮個人情報だが、病歴は要配慮個人情報ではない。
- （１１）不正アクセス禁止法は、他人のコンピュータを直接操作し、そのコンピュータにログインすることも対象として扱われる。
- （１２）マーケティングミックスにおける 4P とは、「Process」、「Price」、「Place」、「Promotion」である。
- （１３）コンピュータプログラムのアルゴリズムは著作権法の保護の対象である。

- (14) Society5.0 とは、サイバー空間とフィジカル空間を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する人間中心の社会のことである。
- (15) サービスレベル管理とは、サービスの提供者と利用者が事前に合意し、維持・改善するための活動である。
- (16) RAID 1 は別名「ストライピング」とも呼ばれる。
- (17) JAN コードはメーカーコード、商品アイテムコード、チェックディジットで構成される仕様の商品識別番号である。
- (18) ISO27001 は、情報セキュリティマネジメントシステムに関する国際的な規格である。
- (19) 生成 AI においてハルシネーションが起こる原因として、モデルの学習データが十分な量ではなかったり、学習データが間違っていたりすることがあげられる。
- (20) SNS の広まりにより、従来よりもレピュテーションリスクは低くなっている。

問題2 次の【A】～【C】の設問のうち、2問を選択し答えなさい。

なお、選択した2問について、解答用紙にレ点を入れなさい。

【A】 次の文章はチャレンジ・レスポンス認証に関するものである。(1)～(5)にあてはまる最も適切な語句を(ア)～(カ)から選択し、それぞれ解答欄に記入しなさい。

ネットワーク上での□(1)の脆弱性を補うための方法がチャレンジ・レスポンス認証です。認証の流れは、以下の通りです。

1. クライアントから□(2)を送信する。
2. サーバでは□(3)を生成し、クライアントに返信する。
3. クライアントとサーバは、互いに保存しているパスワードとこの□(3)から□(4)を生成する。
4. クライアントがサーバに□(4)を返信する。
5. サーバでは、自分が計算した□(4)とクライアントから送られた□(4)を突合することでユーザ認証を行う。

チャレンジ・レスポンス認証を採用した実装技術として□(5)があります。

選択肢

- | | | |
|--------------|---------------|-----------|
| (ア) チャレンジコード | (イ) CHAP | (ウ) ハッシュ値 |
| (エ) ユーザ ID | (オ) クリアテキスト認証 | (カ) なりすまし |

【B】 次の（１）～（５）の論理式を簡単にした結果をそれぞれ解答欄に記入しなさい。ここで、 $+$ は論理和、 $\cdot$ は論理積、 $\bar{X}$ は X の否定を表す。

（１） $A \cdot (\bar{A} + B)$

（２） $A \cdot B + A \cdot \bar{B}$

（３） $\overline{(\bar{A} + B) \cdot (A + \bar{C})}$

（４） $(A + \bar{B} + C) \cdot (\bar{A} + C)$

（５） $(A + B \cdot C) \cdot (B + A \cdot \bar{C})$

【C】 次の文章は無線 LAN に関するものである。（１）～（４）にあてはまる数字を、それぞれ解答欄に記入しなさい。

IEEE （１）n は ISM バンドと呼ばれる （２）GHz 帯と （３）G Hz 帯を使用し、規格上の最大伝送速度は （４）Mbps である。（２）GHz 帯は電子レンジなどの家電製品も利用されていることが多く、電波の干渉が起こりやすくなっている。

問題3 次の[A]、[B]の設問に答えなさい。

[A] 配列とリストの違いについて、以下の問いに答えなさい。

- (1) 配列のデータ構造について、「メモリアドレス」という言葉を用いて説明しなさい。
- (2) リストのデータ構造について、「メモリアドレス」という言葉を用いて説明しなさい。
- (3) n 番目の要素へのアクセスが速いのはどちらか、理由とともに答えなさい。
- (4) データサイズが異なる要素を扱うのに適しているのはどちらか、理由とともに答えなさい。
- (5) 要素の追加・削除がしやすいのはどちらか、理由とともに答えなさい。

[B] 次の5つのプロトコルの役割について簡単に説明しなさい。

- (1) ARP
- (2) NAT
- (3) DNS
- (4) DHCP
- (5) FTP