

【問題 4】 以下の文章を読み、問に答えなさい。

解答欄	4 ア～コ
-----	-------

1990年代以降、(あ)使いやすいインタフェースを備えたパーソナルコンピュータ用基本ソフトウェアの普及やインターネット接続事業者のサービスが拡大したことにより、一般家庭においてもインターネットの利用が増えていった。その後、光ファイバ等を利用した [A] 接続が低廉な価格で提供されるようになり、一般家庭におけるインターネット利用は常時接続の形態をとるようになる。

また、2000年代に入ると、電気通信事業者等が公共のスペースで [B] 規格の公衆無線 LAN サービスを開始したり、その後、携帯電話が「ガラケー」と呼ばれるフィーチャーフォンからスマートフォンへ進化したりするなど、さまざまな条件が整うことで、(い)自宅においてのみならず、自宅外においてもインターネットに接続できる環境が整えられていった。

インターネットが情報インフラストラクチャーとして確立したことによって、一般の消費者もインターネットを通じて商品やデジタルコンテンツを購入するようになった。インターネットを通じ、種々の個人情報や取引情報がやりとりされるうえで、通信の暗号化技術は非常に重要なものである。

デジタル情報の暗号化においては、当初、情報を発信する側と受信する側が暗号化のための鍵を共有する [C] が一般的だった。両者があらかじめ特定の鍵を共有しておく、あるいは、インターネットを通じて情報を発信した後、電話等、別の手段を用いて第三者に知られないかたちで鍵を伝達するというものである。ワープロソフトや表計算ソフトでは、作成したファイルにパスワードを設定することで、第三者の閲覧を防止することができるが、[C] はこのようなケースで使用されている。

しかし、インターネットを通じて多数の人々が暗号化通信を行う場合、[C] は鍵の共有に大きな手間がかかる。これを解消するものが [D] である。

[D] の利用は、ユーザがそれぞれ一対の鍵を持つところから始まる。[E] と [F] である。情報の送信者は、受信者があらかじめ公表している [E] を用いて暗号化を行う。受信者は受信した情報をみずからの [F] で復号化する。[E] と [F] は数学的な計算によって相手を導きだすことができないところに特徴がある。

通信の暗号化に加え、電子的にやりとりされるみずからの署名を [F] で暗号化して送付することで、(う)なりすましを防止することができる。受信者が送

信者の [E] を利用して署名を正しく復号化できた場合、情報の送信者の身元が真正であると証明される。これを [G] と呼ぶ。

[D] は、ウェブブラウザの暗号化通信のプロトコルである [H] などに利用されており、(え)インターネットを通じた各種経済活動の基盤となっている。

問1～問3 { 学習指導要領 (4) - 知・技 - ア
学習内容 (4) - ア ネットワークの仕組みと構成要素

問1 文中の空欄 [A] にあてはまる語句としてもっとも適切なものを選び。

解答欄 4 ア

- | | |
|----------|-----------|
| ① ADSL | ② ISDN |
| ③ ナローバンド | ④ ブロードバンド |

問2 文中の空欄 [B] にあてはまる語句としてもっとも適切なものを選び。

解答欄 4 イ

- | | |
|---------|----------|
| ① IrDA | ② LTE |
| ③ Wi-Fi | ④ モバイル通信 |

問3 文中の空欄 [C]・[D] にあてはまる語句の組み合わせとしてもっとも適切なものを選び。

解答欄 4 ウ

- | | |
|------------|----------|
| ① C: 共通鍵暗号 | D: 公開鍵暗号 |
| ② C: 共通鍵暗号 | D: 同一鍵暗号 |
| ③ C: 共通鍵暗号 | D: 複合鍵暗号 |
| ④ C: 公開鍵暗号 | D: 同一鍵暗号 |
| ⑤ C: 公開鍵暗号 | D: 複合鍵暗号 |
| ⑥ C: 公開鍵暗号 | D: 共通鍵暗号 |
| ⑦ C: 同一鍵暗号 | D: 公開鍵暗号 |
| ⑧ C: 同一鍵暗号 | D: 複合鍵暗号 |
| ⑨ C: 同一鍵暗号 | D: 共通鍵暗号 |

問4 文中の空欄 [E]・[F] にあてはまる語句の組み合わせとしてもっとも適切なものを選び。

解答欄 4 エ

- | | |
|----------|--------|
| ① E: 共通鍵 | F: 開錠鍵 |
| ② E: 共通鍵 | F: 公開鍵 |
| ③ E: 共通鍵 | F: 秘密鍵 |
| ④ E: 公開鍵 | F: 開錠鍵 |
| ⑤ E: 公開鍵 | F: 施錠鍵 |
| ⑥ E: 公開鍵 | F: 秘密鍵 |
| ⑦ E: 施錠鍵 | F: 開錠鍵 |
| ⑧ E: 施錠鍵 | F: 公開鍵 |
| ⑨ E: 施錠鍵 | F: 秘密鍵 |

問5 文中の空欄 [G] にあてはまる語句としてもっとも適切なものを選び。

解答欄 4 オ

- | | |
|----------|-------------|
| ① IDカード | ② 電子署名 |
| ③ デジタル名刺 | ④ ハイパーシグネチャ |

問6 文中の空欄 [H] にあてはまる語句としてもっとも適切なものを選び。

解答欄 4 カ

- | | |
|--------|------------|
| ① JAVA | ② SSL |
| ③ WEP | ④ ブロックチェーン |

学習指導要領 (1) - 知・技 - ウ
学習内容 (2) - イ 情報デザインと役割

問7 文中の下線部 (あ) に関する記述としてもっとも適切なものを選び。 解答欄 4 キ

- ① 液晶画面に表示されたオブジェクトを指でタップして開くことができる直感的なインタフェースとなった。
- ② キーボードからコマンドを入力する CUI から、マウスも使用できる GUI に変化した。
- ③ それまでの基本ソフトウェアはすべて英語表示だったものが、日本語で操作できるようになった。
- ④ 複数のウィンドウを開いて操作を行うインタフェースが初心者に分かりにくかったため、シングルタスク、シングルウィンドウのインタフェースとなった。

学習指導要領 (1) - 知・技 - ウ
学習内容 (1) - ウ 情報技術と情報社会

問8 文中の下線部 (い) に関連し、国民がいつでもどこでもインターネットに接続できる環境の整備を目的とした政府施策 u-Japan が想定した社会像の名称としてもっとも適切なものを選び。 解答欄 4 ケ

- ① Society 5.0 ② 超スマート社会
- ③ マルチメディア社会 ④ ユビキタス社会

学習指導要領 (4) - 知・技 - ア
学習内容 (4) - ア ネットワークの仕組みと構成要素

問9 文中の下線部 (う) に関連し、既存の機関・企業などのウェブサイトを巧妙にまね、なりすましのサイトをつくり、メール等で誘導したうえで、各種サービスの ID・パスワードやクレジットカード情報などを詐取するサイバー犯罪の手口の名称としてもっとも適切なものを選び。 解答欄 4 ケ

- ① ソーシャルエンジニアリング ② ハッキング
- ③ フィッシング ④ ブルートフォース攻撃

学習指導要領 (4) - 知・技 - ア

学習指導要領 (1) - 思・判・表 - ウ

学習内容 (4) - ア ネットワークの仕組みと構成要素

問 10 文中の下線部 (え) に関連し、現在、インターネット上にオンラインモールを開設して他者にビジネスの場を提供したり、SNS・メールサービス等を無償提供したりして、膨大な個人情報を蓄積・活用する事業者がある。これら事業者に関しては、優越的な地位を利用し、出店者に不利な契約を行うなど、問題が指摘されている。また、蓄積した個人情報をみずからのビジネスに活用することで大きな利益をあげていることについても批判がなされている。これら事業者の呼称としてもっとも適切なものを選べ。

解答欄 4 コ

- ① キャリア ② コンテンツプロバイダー
③ 重要社会基盤事業者 ④ デジタルプラットフォーマー