問題は全部で４題あります。
［問１］、［問２］については、計算などの過程も記載してください。
解答用紙の表面に書ききれない場合は、解答用紙の裏面を使用してください。

［問１］ 次の（１）から（４）の問いに答えよ。

（１） $a_n = 2n$であるとき、
$\sum_{n=1}^{100} a_n$
の値を答えよ。

（２） ６進数が好きなＡさんは、大阪府警察の採用試験の受験番号を６進数に変換したところ、“12345”になった。Ａさんの受験番号を 10 進数で答えよ。

（３） 袋の中に赤色の球が３個、白色の球が６個入っている。袋から球を２個同時に取り出した時、少なくとも１つは白色の球である確率を分数で答えよ。

（４） Ａ、Ｂ、Ｃの３人は、１から６の六つの目が同じ確率で出るサイコロをそれぞれ１回振って、出た目の大きい方を勝ちとするゲームをしていた。勝負が終わった後の３人の言葉から、３人が出したそれぞれのサイコロの目を答えよ。なお、サイコロを振ったのは同時ではなく、Ａ、Ｂ、Ｃの順番とする。
Ａ：３人とも出た目は違う数であった。
Ｂ：自分がＡに勝つ確率は 50％だったが、勝てなかった。
Ｃ：自分はＡに負けたが、自分のサイコロの出た目は１ではない。

［問２］ 次の（１）、（２）の問いに答えよ。

（１） サンプリング周波数を 20kHz、量子化ビット数を 16 ビットで 10 秒間サンプリングした音声データを作成した場合について、(ア）から（ウ）の問いに答えよ。ただし、１k バイトは 1,000 バイトとする。

（ア） 作成時のサンプリング回数を答えよ。

（イ） 作成した音声データのデータ量は何 k バイトか答えよ。

（ウ） 作成した音声データを圧縮率 1/4 の ADPCM によって圧縮した場合、データ量は何 k バイトになるか答えよ。

（２） 検索処理の平均応答時間が、ヒットした場合には 0.4 秒、ヒットしなかった場合には 4.0 秒を要するキャッシュサーバーについて、(ア)、(イ）の問いに答えよ。ただし、解答が割り切れない場合は、小数第二位を四捨五入し、小数第一位までで答えよ。

（ア） 平均検索応答時間が 2.2 秒のとき、ヒット率を答えよ。

（イ） このキャッシュサーバーの５年後のヒット率は検索量増加により現在の半分になると予測されている。５年後の平均検索応答時間は何秒になるか答えよ。ここで、その他のオーバーヘッドは考慮しないものとする。

［問３］ 以下の文中の空欄（ａ）から（ｈ）に当てはまる言葉を語群から選択し答えよ。

・セキュリティホールが発見されてから、メーカーなどがその穴を塞ぐための修正プログラムを提供するまでの期間に行われる攻撃のことを（　ａ　）という。この期間に攻撃を受けると、防ぐ手段はないため、利用者自身が「避ける手段」を講じる必要がある。
・総当たり攻撃は、攻撃者が「ログインパスワード」や「暗号キー」を破るために、すべての文字などの組合せを試す攻撃のことをいい、（　ｂ　）ともいう。
・攻撃者が目的とする相手（個人または企業の社員など）を、マルウェアに感染させるために、あらかじめ訪問しそうなウェブサイトにマルウェアを仕込んで待つことを（　ｃ　）という。
・攻撃者などが不正に操作した多数のパソコンなどから、攻撃目標に一斉に多量の問合せなどを行い、攻撃対象の反応が追いつかず利用できない状況にする攻撃を（　ｄ　）という。
・生成 AI（Artificial Intelligence：人工知能）は過去のデータ等を基に入力情報を学習し、新たなデータを生成する。テキスト、画像、動画、音声等、様々なコンテンツを出力することができる。より具体的な出力を求めたい場合は、質問や命令文の内容である（　ｅ　）を具体的にすることが重要である。
・生成 AI で入力した情報は、AI の再学習で利用される可能性があり、（　ｆ　）の懸念も考えられる。機密情報や顧客情報等については入力しない、もしくは組織内のみで利用できる生成 AI ツールを利用するなどして、機密情報や顧客情報等が外部に流出しないように対策を行うことが重要である。
・生成 AI で入力する情報が学習データとして利用される際に、不正確な内容や、偏り（バイアス）を含んでいた場合、AI が誤った回答を提供する（　ｇ　）が発生するおそれがある。
・生成 AI から正しい回答を受け取るためには、情報を提供するユーザー側も（　ｈ　）を身に付ける必要がある。AI が誤った情報を基に学習をしないように、日頃から正しい情報をインターネットで発信することを心がける。

語群

ワーム	サイドチャネル攻撃	トロイの木馬	ダークネット
情報リテラシー	フォールトマスキング	エントロピー	情報漏えい
インタプリタ	ブルートフォース攻撃	プロンプト	チューリングマシン
インジェクション	フィッシング	水飲み場攻撃	Emotet
ゼロデイ攻撃	サプライチェーン攻撃	DDoS 攻撃	ランサムウェア
標的型メール	ハルシネーション	オートマトン	情報クリッピング

［問４］ 以下の認証局を利用した電子証明書の仕組みについて述べた文を読んで（１）、（２）の問いに答えよ。

・送信者は認証局に対し、自身の（　①　）を送付し、電子証明書の発行を申請する。
・認証局は申請に基づき送信者の本人確認を行い、送信者名義の（　②　）を発行する。
・送信者は自身の（　③　）で暗号化し、認証局より発行された（　④　）とともに受信者へ送信する。
・受信者は同封されている送信者の（　⑤　）を用いて復号を行えるか検証する。

（１） 文中の空欄（①）から（⑤）に入る言葉を答えよ。ただし、それぞれ、「公開鍵」、「秘密鍵」、「証明書」のいずれかが入り、複数回同じ言葉を使用してもよいものとする。

（２） 認証局を利用した電子証明書はインターネットが抱える特有の問題への対策として用いられている。認証局を利用した電子証明書を用いることで情報の受け手が確認できることを、インターネットが不特定多数の相手との通信を行うオープンなネットワークであることに着目した上で「・・・を確認できる。」の形式で２点、それぞれ 20 字程度で答えよ。なお、認証局は完全に信頼できるものとする。