問題５　次の情報セキュリティに関する各設問に答えよ。

＜設問１＞ 次のマルウェアに関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

マルウェアは，利用者やコンピュータに有害で不正な動作を行わせるために，悪意を持って開発されたコンピュータプログラムの総称であり，次のようなものがある。

［(1)］は，ユーザに有用と見せかけて，実行させるように仕組まれたプログラムであり，ユーザが気付かない間にデータの消去やファイルの外部流出，他のコンピュータへの攻撃などを行う。

［(2)］は，コンピュータをロックして操作不能にすることや，データを暗号化してアクセス不能にするなどして，その解除のために金銭要求を行う。

［(3)］は，ユーザが通常利用している Web サイトにログインしている間に，罠の仕掛けられた Web サイトへのリンクをクリックすることで，この悪意のある Web サイトからログイン中の Web サイトへ意図しないリクエストが送られ，掲示板への書き込みや商品購入など正規のユーザでなければ出来ない処理を行う。

(1) ～ (3) の解答群

ア．クロスサイトリクエストフォージェリ
イ．サニタイジング
ウ．ソーシャルエンジニアリング
エ．トロイの木馬
オ．ボットネット
カ．ランサムウェア

＜設問２＞ 次のセキュリティ対策に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

Web サイトに接続されているデータベースに対して，データベースの改ざんや情報の不正入手を行う攻撃手法に，悪意のある SQL 文やその一部を入力する［(4)］がある。この攻撃への対策として［(5)］を利用するのが有効である。［(5)］は，パラメータとして与えられた部分に適切なエスケープ処理を自動で行うため，本来入力としては使われることが想定されていない SQL 文が挿入されても，その SQL 文の実行を防ぐことができる。

また，ネットワークシステムでは，送信者でも受信者でもない第三者が，ネットワーク上を流れるメッセージを勝手に読み取ってしまう「盗聴」，第三者がメッセージの内容を変更して，何事もなかったかのように送り付ける「改ざん」，送信者の名前を偽装してメッセージなどを送り付ける「なりすまし」といった脅威にさらされている。

「盗聴」への対策は，暗号化が有効である。暗号化方式としては，暗号化鍵と復号鍵が異なる公開鍵暗号方式，暗号化鍵と復号鍵が同一の［(6)］がある。それぞれの暗号方式には長所と短所があり，公開鍵暗号方式と［(6)］の長所を組み合わせた［(7)］も利用される。

「改ざん」への対策は，メッセージを［(8)］関数で短いビット列に変換したメッセージダイジェストを利用することが有効である。

「なりすまし」への対策は，確実なユーザ認証を行うことが有効である。ユーザ認証には様々な手法があるが，公開鍵暗号方式の［(9)］を用いて暗号化する手法もある。

(4) ～ (7) の解答群

ア．DNS キャッシュポイズニング　　イ．IP スプーフィング
ウ．RSA 暗号方式　　エ．SQL インジェクション
オ．共通鍵暗号方式　　カ．ハイブリッド暗号方式
キ．ファイアウォールアプライアンス　　ク．プリペアードステートメント

(8)，(9) の解答群

ア．公開鍵　　イ．チャレンジレスポンス
ウ．ハッシュ　　エ．バックドア
オ．秘密鍵