問題５　次の情報セキュリティに関する記述を読み，各設問に答えよ。

情報セキュリティは，コンピュータネットワークの飛躍的な進展がもたらした大きな社会的課題である。セキュリティ対策には物理的対策，技術的対策，人的対策がとられる。

＜設問１＞ 次のセキュリティ上の脅威の検出に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

セキュリティ上の脅威として，「盗聴」「改ざん」「なりすまし」などがある。

「盗聴」対策として暗号化がある。暗号化の一つである公開鍵暗号方式は，対となる公開鍵と秘密鍵からなり，一方の鍵で生成した暗号文は他方の鍵でしか復号できない。

「改ざん」を検知する方法として［(1)］がある。［(1)］は，送信するデータをハッシュ関数で一定長のビット列に変換したもので，データに付加して送信し，受信側も同じハッシュ関数を使い受信したデータからビット列を生成する。このビット列と，受信したビット列を比較し，同じであれば「改ざん」が行われていないことが確認できる。

「なりすまし」対策としてディジタル署名がある。ディジタル署名は，公開鍵暗号方式を利用するもので，送信者はデータを［(2)］で暗号化して送信し，受信者は［(3)］で復号することで相手の正当性を確認する認証方法である。しかし，鍵の信頼性まで確認できないので，送信者は第三者機関である認証局に公開鍵を登録して，［(4)］を発行してもらい，ディジタル署名に添付する。［(4)］は［(5)］で暗号化されており，受信者は［(6)］で復号することで，送信者の公開鍵の信頼性を確認できる。

ディジタル署名のデータに［(1)］を利用することで，「改ざん」と「なりすまし」の両方を検出できる。

(1)，(4) の解答群

ア．クライアント　　イ．サーバ
ウ．チェックディジット　　エ．チャレンジ／レスポンス
オ．ディジタル証明書　　カ．メッセージダイジェスト

(2)，(3)，(5)，(6) の解答群

ア．受信者の公開鍵　　イ．受信者の秘密鍵
ウ．送信者の公開鍵　　エ．送信者の秘密鍵
オ．認証局の公開鍵　　カ．認証局の秘密鍵

＜設問２＞ 次のDNS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。

DNSとは，ドメイン名をIPアドレスに変換する仕組みである。ドメイン名は３つの部分で構成され，www.jken.co.jpを例に部分名を図に示す。

jp	トップレベルドメイン
co	第２レベルドメイン
jken	第３レベルドメイン

図　ドメイン名の構成

ドメイン名からIPアドレスを求めることを名前解決と呼び，次の手順で処理する。なお，ここでは自社にDNSサーバを設置している。

【名前解決の手順】

① クライアントは自社の DNS サーバに問い合わせ,問い合わせたドメイン名をキャッシュに登録する。

以降の手順は自社のDNSサーバが行う。

② DNSサーバで管理されていないドメイン名であれば,ルートサーバに問い合わせ,トップレベルドメインのDNSサーバの情報を得る。

③ トップレベルドメインの DNS サーバに問い合わせ，第２レベルドメインの DNS サーバの情報を得るというように，再帰的問合せを繰り返す。

④ 自社のDNSサーバは，③で得たIPアドレスをクライアントに回答する。

このように，自社のDNSサーバは外部のDNSサーバに繰り返し問合せを行うため，この手順の間に攻撃者が自社のDNSサーバのキャッシュに偽の情報を書き込み，悪意のあるサイトに誘導する攻撃が［　(7)　］である。

この攻撃を受ける原因は，問い合わせたDNSサーバからの回答に認証を行わないことにある。ディジタル署名などを利用して正規のDNSサーバ以外のキャッシュへの書き込みを許可しない方法が有効な対策である。

(7) の解答群

ア．DNSキャッシュポイズニング　　イ．DNSリフレクター攻撃

ウ．クロスサイトスクリプティング　　エ．ソーシャルエンジニアリング