問題５　次のセキュリティに関する各設問に答えよ。

＜設問１＞　次のWebサイトのセキュリティに関する記述を読み，各問に答えよ。

インターネットが普及している今日では，インターネットショッピングが日常の買い物手段として定着しつつある。

インターネット上のショッピングサイトで買い物をすると，個人情報がWeb サイトに送信される。この個人情報を不正に入手するために，偽装したWebサイトに利用者を誘導して個人情報を搾取する悪質なWebサイトも存在する。誘導する手口としては，(a)金融機関などを装ったメールからの誘導，SNSからの誘導などがある。

また，送信される情報が盗聴される恐れもある。そこで，(b) SSL（または TLS）を使用した通信を行い，送信する情報の保護を行う。

(1) 下線(a)に関係の深い字句を解答群から選べ。

(1) の解答群

ア．インジェクション　　イ．クラック
ウ．バックドア　　エ．フィッシング

(2) 下線(b)のSSLで処理する内容を解答群から選べ。

(2) の解答群

ア．ポップアップブロック　　イ．暗号化通信
ウ．スパイウェアからの保護　　エ．不正アクセスからの防御

(3) SSLを利用したWebサイトのURLで使用するスキームを解答群から選べ。

(3) の解答群

ア．http　　イ．https　　ウ．ssh　　エ．ftp

(4) ショッピングサイトでも商品紹介のように SSL を利用しないページが存在するが，その理由として適切なものを解答群から選べ。

(4) の解答群

ア．SSLを利用したページはレスポンスが悪いので表示に影響が出るから
イ．SSLが利用できるページ数はドメイン内で１ページに限定されるから
ウ．SSLを利用するページはコンピュータウイルスの検査が行えないから
エ．SSLは送信フォーム以外に利用することができないから

＜設問２＞　次の Web サイトの認証に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

認証局が発行する「ディジタル証明書」を持つことで，安全な Web サイトであることが保証される。このディジタル証明書を利用してインターネット上で通信相手を認証する仕組みを［　(5)　］という。ディジタル証明書には，証明書の正当性を保証するために「認証局のディジタル署名」が付加されており，ディジタル証明書が正規の手続きにより作成されたことを保証している。

Web サイトの認証では，ハッシュ関数と公開かぎ暗号方式の技術を用いる。

ハッシュ関数は一方向関数であり，入力されたメッセージからビット列（ハッシュ値）を生成するもので，メッセージが同じであれば生成されるハッシュ値は同じになる。また，ハッシュ値から元のメッセージに戻すことは不可能である。代表的なハッシュアルゴリズムに［　(6)　］がある。

公開かぎ暗号方式は，「公開かぎ」と「秘密かぎ」のペアでメッセージの暗号化と復号を行うものであり，公開かぎで暗号化したメッセージはペアの秘密かぎでのみ復号が可能であり，秘密かぎで暗号化したメッセージはペアの公開かぎでのみ復号が可能である。

ディジタル証明書を使った認証の流れは次のとおりである。

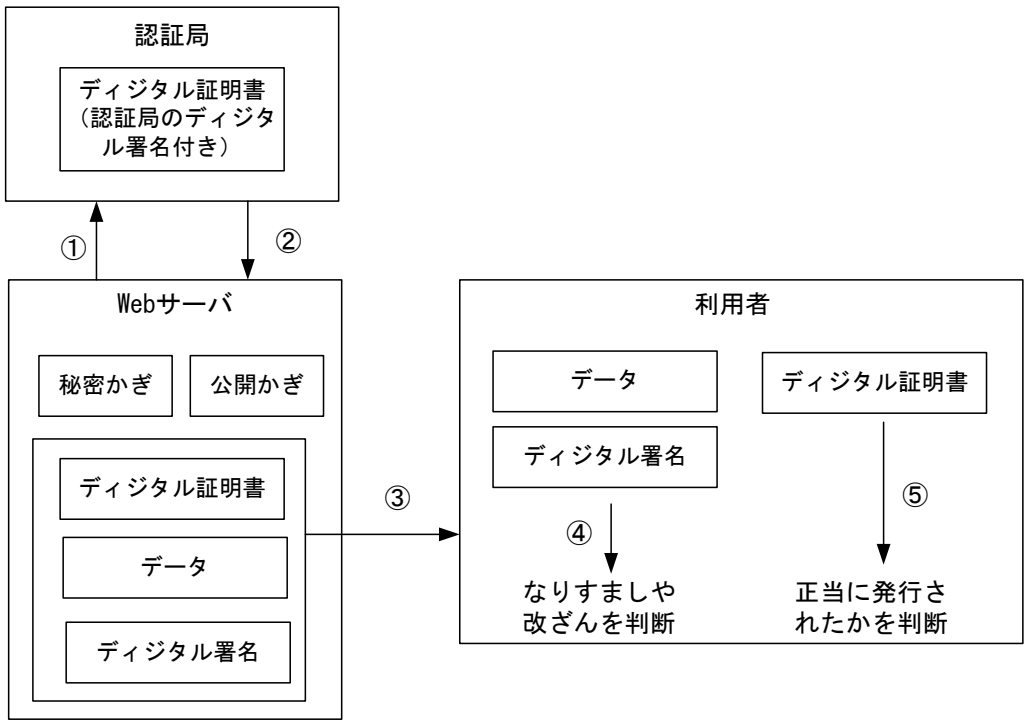

図　Web サイトの認証

［Webサイトがディジタル証明書を受け取るまでの流れ］

① Webサイトは，ペアとなる公開かぎと秘密かぎを作成し，公開かぎを認証局に送信してディジタル証明書の発行を依頼する。

② 認証局は，Webサイトの情報などから証明書を作成し，認証局のディジタル署名を付与してWebサイトに送信する。

［Webサイト認証の流れ］

③ Webサイトは，送信するデータから生成したハッシュ値を［ (7) ］で暗号化したディジタル署名とディジタル証明書をデータと一緒に利用者Xへ送信する。

④ 利用者Xは,ディジタル証明書に付与された認証局のディジタル署名を［ (8) ］で復号し，正当な手続きで発行されたディジタル証明書かどうかを確認する。

⑤ 利用者Xは,受信したディジタル署名を［ (9) ］で復号した値と,受信したデータから生成したハッシュ値を比較することで，なりすましや改ざんされていないことが確認できる。

(5) の解答群

ア．コールバック方式　　イ．チャレンジ・レスポンス
ウ．ワンタイムパスワード　　エ．公開かぎ基盤

(6) の解答群

ア．CA　　イ．PKI　　ウ．SHA-2　　エ．WPA2

(7) ～ (9) の解答群

ア．Webサーバの公開かぎ　　イ．Webサーバの秘密かぎ
ウ．認証局の公開かぎ　　エ．認証局の秘密かぎ
オ．利用者Xの公開かぎ　　カ．利用者Xの秘密かぎ

＜設問３＞　ディジタル証明書に含まれない情報を解答群から選べ。

(10) の解答群

ア．認証局の秘密かぎ　　イ．証明書の有効期限
ウ．認証局の名前　　エ．申請者の公開かぎ