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。

Web サーバへアクセスする時のセキュリティとして SSL/TLS が使われる。SSL はネットスケープコミュニケーションズ社が開発したデータを暗号化して送受信するプロトコルであり，TLS は SSL3.0 を基に作られた。SSL と TLS の仕組みは同じだが互換性は無く，2014 年に発見された SSL の脆弱性から SSL の運用を停止して TLS のみで運用するサーバが増えている。SSL という名称が広く使われていることから，TLS であっても SSL と表記したり SSL/TLS と表記したりすることがある。

SSL/TLS は，公開かぎ暗号方式，共通かぎ暗号方式，ディジタル署名，ディジタル証明書の技術を利用して実現する。

＜設問１＞ 次のディジタル署名に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

ディジタル署名とは，公開かぎ暗号化方式を利用して文書の送信者が正当であることと文書が改ざんされていないことを保証するものである。ディジタル署名は次の図のようにやり取りされる。

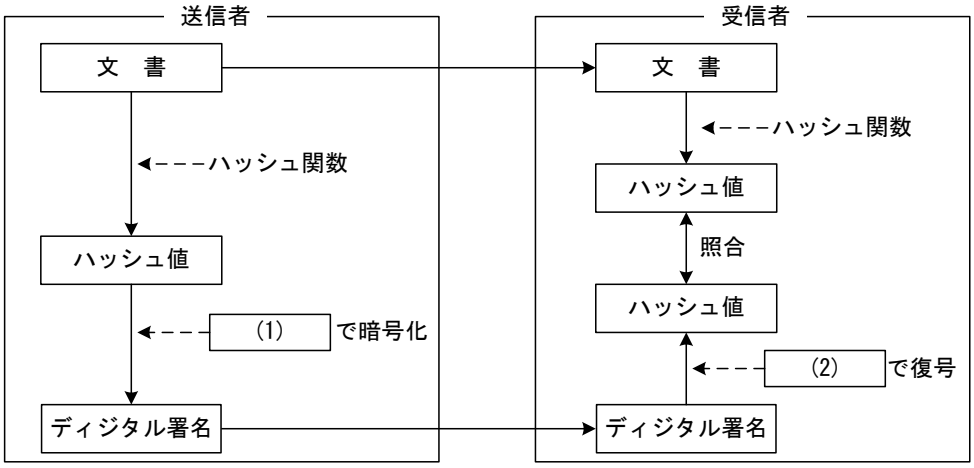

図１　ディジタル署名

送信者はハッシュ関数を使用して送信する文書からハッシュ値を生成し，［　(1)　］を使用して暗号化することでディジタル署名を作成する。

受信者は文書から送信者と同じハッシュ関数を使用してハッシュ値を生成する。また，ディジタル署名は［　(2)　］により復号され，受信者が文書から作成したハッシュ値と照合して正当なものか判断する。

(1)，(2) の解答群

ア．送信者の公開かぎ　　イ．送信者の秘密かぎ

ウ．受信者の公開かぎ　　エ．受信者の秘密かぎ

＜設問２＞ 次のディジタル証明書に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

公開かぎが「なりすまし」される可能性は十分考えられるので，ディジタル署名だけで「なりすまし」を完全に防ぐことはできない。

そこで，信頼できる第三者機関に公開かぎが正当であることを証明してもらうことで，公開かぎの「なりすまし」を防ぐことができる。第三者機関は認証局や［(3)］と呼ばれる。認証局が発行するのがディジタル証明書であり，認証局を通して送信者の正当性を証明することができる。

あるWebサーバがディジタル証明書の発行を依頼する流れは次のようになる。

① Webサーバ側でペアになる公開かぎと秘密かぎを生成する。

② Webサーバの公開かぎとサーバに関する情報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。

③ 認証局は Web サイトの公開かぎやサーバに関する情報からディジタル証明書を作成し［(4)］で暗号化しWebサーバに送信する。

④ ディジタル証明書を受け取ったWebサーバは，ディジタル証明書をWebサーバにインストールする。

(3) の解答群

ア．CA　　イ．DES　　ウ．PKI　　エ．SHA1

(4) 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

＜設問３＞ 次の SSL/TLS による通信に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

SSL/TLS によりクライアントと Web サーバ間で通信を始めるには，まず次のような処理をする。

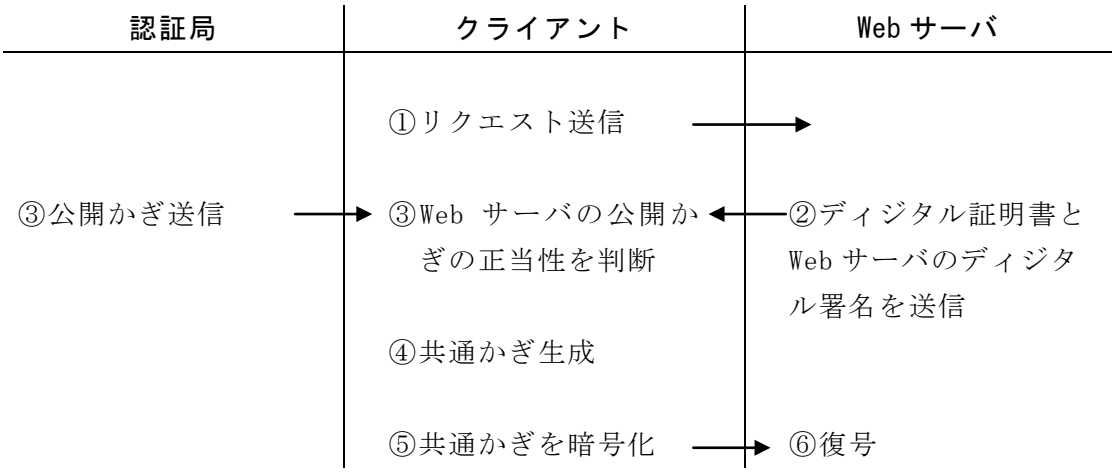

図２　SSL/TLS による通信開始までの流れ

① クライアントから Web サーバへリクエストを送信する。
② Web サーバのディジタル証明書をクライアントに送信する。
③ クライアントは，［(5)］を［(6)］で復号し，Web サーバの公開かぎを取得し，その正当を判断する。
④ クライアントは共通かぎを生成する。
⑤ ④で生成した共通かぎを［(7)］で暗号化して Web サーバへ送信する。
⑥ Web サーバは受信した情報を［(8)］で復号する。

この後は，［(9)］を使用した暗号化通信を行う。

(5) の解答群

ア．Web サーバのディジタル証明書　　イ．Web サーバの名称
ウ．認証局の秘密かぎ　　エ．認証局の名称

(6) ～ (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．共通かぎ

＜設問４＞ SSL3.0 の脆弱性はクライアントの Cookie 情報が盗まれる可能性である。Cookie 情報が盗まれた場合に発生する直接的な被害を解答群から選べ。

(10) の解答群

ア．USB メモリに保存してあるドキュメントファイルが盗まれる。

イ．インターネット上の会員制サイトへログインする時に使用する ID とパスワードが盗まれる。

ウ．ハードディスクに保存してある画像や音楽データが盗まれる。

エ．電子メールソフトで使っているアドレス帳から電子メールアドレスが盗まれる。