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。

契約書などの書面に，当事者本人であることを証明するために署名や捺印することと同様に，ディジタル化された文書に添付するのがディジタル署名である。これは，公開かぎ暗号方式を利用したもので，署名者の正当性を保証する仕組みである。署名者は［(1)］で署名を暗号化して送信し，受信者は［(2)］で復号することで，署名者(送信者)の正当性を確認できる。しかし，ディジタル署名だけではかぎの信頼性まで確認できない。

そこで，署名者は第三者機関である認証局に自分の作成した公開かぎを登録して，ディジタル証明書を発行してもらい，ディジタル署名に添付する。ディジタル証明書は［(3)］で暗号化されており，受信者は［(4)］で復号することで，送信者の公開かぎの信頼性を確認できる。

(1) ～ (4) の解答群

ア．受信者の公開かぎ　　イ．受信者の秘密かぎ
ウ．署名者の公開かぎ　　エ．署名者の秘密かぎ
オ．認証局の公開かぎ　　カ．認証局の秘密かぎ

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

認証局は，大きくは登録局と発行局という二つの機関に分けられる。登録局は申請を受け付け，申請者を審査する機関で，申請者に問題が無ければ発行局に伝達し，発行局が申請者にディジタル証明書を発行すると共に，ディジタル証明書を保管するデータベースにも登録する。ディジタル証明書には，申請者情報，［(5)］，有効期限，認証局情報などが含まれている。有効期限内であっても申請者の秘密かぎが盗まれてしまった場合などで，ディジタル証明書を廃棄する場合がある。この場合も発行局が［(6)］として公開する。

(5)，(6) の解答群

ア．クライアント証明書　　イ．クライアントの機種情報
ウ．証明書失効リスト　　エ．証明書署名要求
オ．申請者の公開かぎ　　カ．申請者の秘密かぎ

＜設問３＞ 次の暗号化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。

インターネットで情報を暗号化してやり取りする際のプロトコルが TLS である。SSL3.0 を基に規格化され，SSL の脆弱性が発見されてから TLS で運用されているが，SSL の名称が広く普及していたこともあり，現在も SSL や SSL/TLS と併記する名称が使われている。

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。

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，まず次のような手順で処理する。

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 サーバは，ディジタル証明書，ディジタル署名，Web サーバの公開かぎなどが含まれたサーバ証明書をクライアントに送信する。
③ クライアントは，受け取ったディジタル証明書を基に，Web サーバの公開かぎが正当であるかを確認する。
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。

(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．共通かぎ　　エ．認証局の公開かぎ
オ．認証局の秘密かぎ