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＞　図１の SSL の仕組みに関する記述中の［　　］に入れるべき最も適切な字句を解答群から選べ。

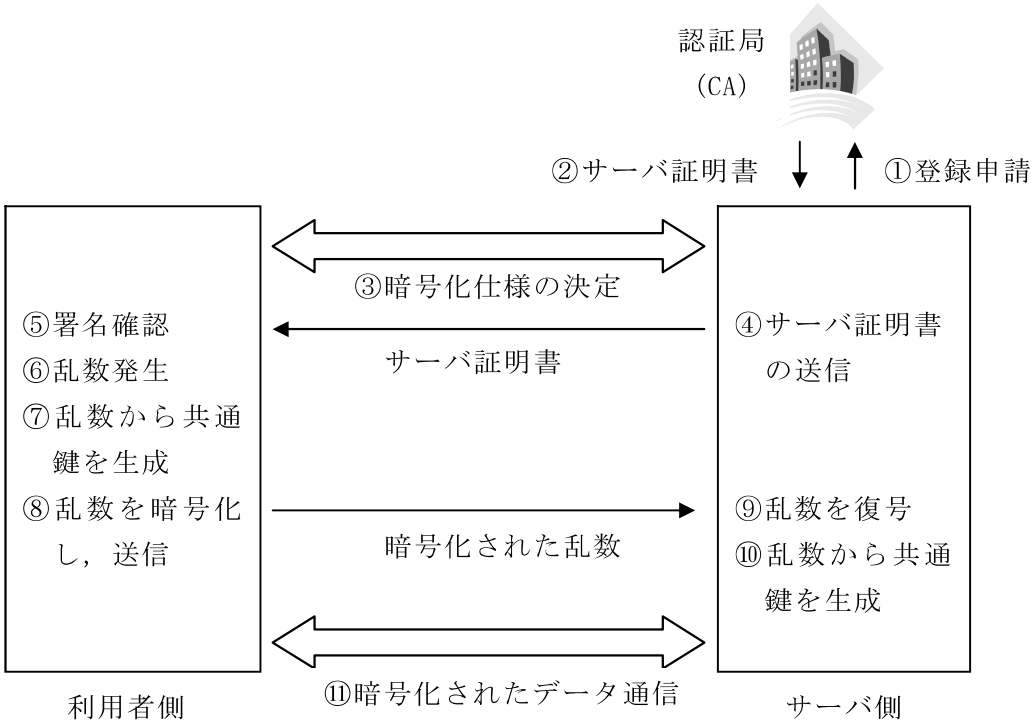

図１　SSL の仕組み

①サーバを運用している会社(サーバ側)は，認証局(CA)にサーバ証明書の交付を申請する。
②認証局は申請された会社の実在性を確認し，サーバ証明書を発行する。サーバ証明書には［　(1)　］など含まれている。
③利用者側が利用できる暗号化の仕様リストから暗号化仕様を決定する。
④認証局から送られてきたサーバ証明書を利用者に送る。
⑤利用者は送られてきたサーバ証明書の署名を［　(2)　］で復号し，［　(3)　］の署名を確認する。
⑥利用者側で乱数を発生させる。
⑦乱数から共通鍵を生成する。
⑧乱数を［　(4)　］で暗号化し，送信する。
⑨暗号化された乱数を［　(5)　］で復号する。
⑩乱数から共通鍵を生成する。
⑪通信文を［　(6)　］で暗号化し，送受信する。

(1) の解答群

ア．サーバの公開鍵，サーバ運営会社の財務状況，認証局の署名
イ．サーバの公開鍵，サーバ運営会社の名称と所在，認証局の署名
ウ．サーバの秘密鍵，サーバ運営会社の取引先，認証局の公開鍵
エ．サーバの秘密鍵，サーバ運営会社の名称と所在，認証局の秘密鍵

(2) ～ (6) の解答群

ア．サーバ　　イ．サーバの公開鍵　　ウ．サーバの秘密鍵
エ．認証局　　オ．認証局の公開鍵　　カ．認証局の秘密鍵
キ．利用者　　ク．利用者の公開鍵　　ケ．利用者の秘密鍵
コ．共通鍵

＜設問２＞　次の ID,パスワード管理に関する記述に関係の深い字句を解答群から選べ。

(7) 他人になり済まして不正アクセスを行うため，会社のごみ箱などをあさり，他人の ID やパスワードなどのメモを見つけ出す行為。
(8) クレジットカードやキャッシュカードなどの利用者認証カードと一緒に使用される個人識別番号。

(7)，(8) の解答群

ア．スキャベンジング　　イ．スパム　　ウ．トロイの木馬
エ．PGP　　オ．PIN　　カ．SNS

＜設問３＞　次のパスワードに関する記述中の［　　］に入れるべき適切な数値を解答群から選べ。

10 進数だけを用いて 6 桁でパスワードを作成する場合，［ (9) ］通りのパスワードを作成できる。これに対し，10 進数値に加え英小文字も使用できる場合は 10 進数値のみを使用する場合に比べて，［ (10) ］倍の種類のパスワードを作成することができる。

(9) ～ (10) の解答群

ア．3.6^6　　イ．3.6^{26}　　ウ．6^{36}　　エ．10^6　　オ．10^{26}　　カ．10^{36}