第４問 (80点)

次の文章について，以下の問いに答えよ。

情報セキュリティとは，情報の (ア) 機密性・(イ) 完全性・(ウ) 可用性の維持を指す。情報の機密性は，古くから軍事や政治の場面で常に求められている。この機密性を確保するための技術として暗号技術がある。もとの情報（平文）を暗号にすることを暗号化，暗号化された情報（暗号文）をもとの情報（平文）に戻すことを復号という。暗号化と復号で同じ鍵（共通鍵）を用いる暗号化方式のひとつである (エ) シーザー暗号は，各文字をアルファベット順で数文字分シフトして（ずらして）暗号文を作るものである。たとえば，“HAL”は “IBM”をアルファベット順で１文字前にずらした暗号文である。シーザー暗号では，アルファベット順でシフトする文字数が共通鍵となる。(オ) 共通鍵は送信者ごとに別々に必要となり，送信者と受信者がともに共通鍵を秘密に管理しなければならない。そこで，共通鍵を受け渡す過程での盗聴のリスクに加え管理が非常に煩雑になる。この問題を解決するために，暗号化のための鍵と復号のための鍵を別々にした公開鍵暗号が提案された。この公開鍵暗号は，送信者は受信者が公開した鍵（公開鍵）で平文を暗号化し，受信者は自分が秘密にもつ鍵（秘密鍵）で復号する暗号方式である。また，公開鍵暗号の一つである RSA 暗号は公開鍵と秘密鍵のどちらの鍵でも暗号化ができるという性質を有しているため，受け取った電子文書がなりすましにより改ざんされたものであるか否かを確認する (カ) 電子認証に応用されている。

学習指導要領（1）- 知・技 - イ
学習内容（1）- イ 法・情報セキュリティ・情報モラル

問１ 上の文章中にある (ア) 機密性，(イ) 完全性および (ウ) 可用性をそれぞれ説明せよ。

学習指導要領（4）- 知・技 - ア
学習内容（4）- ア ネットワークの仕組みと構成要素

問２ 上の文章中にある (エ) シーザー暗号について，“HIRO”をアルファベット順で３文字後ろにずらした暗号文を答えよ。

学習指導要領（4）- 思・判・表 - ア
学習内容（4）- ア ネットワークの仕組みと構成要素

問３ 上の文章中にある（オ）について，同じ人同士で送受信する際は同一の共通鍵を使うことにした場合，機密性を確保しつつ４人の間で相互に送受信するには６個の共通鍵が必要である。一般に，n $(n \geqq 2)$人の間では何個の共通鍵が必要か答えよ。なお，その答えの導出過程も述べること。

学習指導要領（4）- 思・判・表 - ア
学習内容（4）- ア ネットワークの仕組みと構成要素

問４ 図１は，上述の文章にある (カ) 電子認証のしくみを示している。図１中の認証局（CA）とは公開鍵を管理し正しい送信者であることを保証する機関である。電子証明書とは電子上の印鑑証明書である。また，要約文とはプログラムにより平文の特徴的な部分を生成した文である。そこで，図１中の①～⑥の説明として適切な語句を選択肢（a）～（j）から選べ。なお，選択肢中の電子署名とは電子上の印鑑である。また，同じ番号には同じ選択肢が対応するものとする。さらに，同じ選択肢が異なる番号に対応することもないものとする。

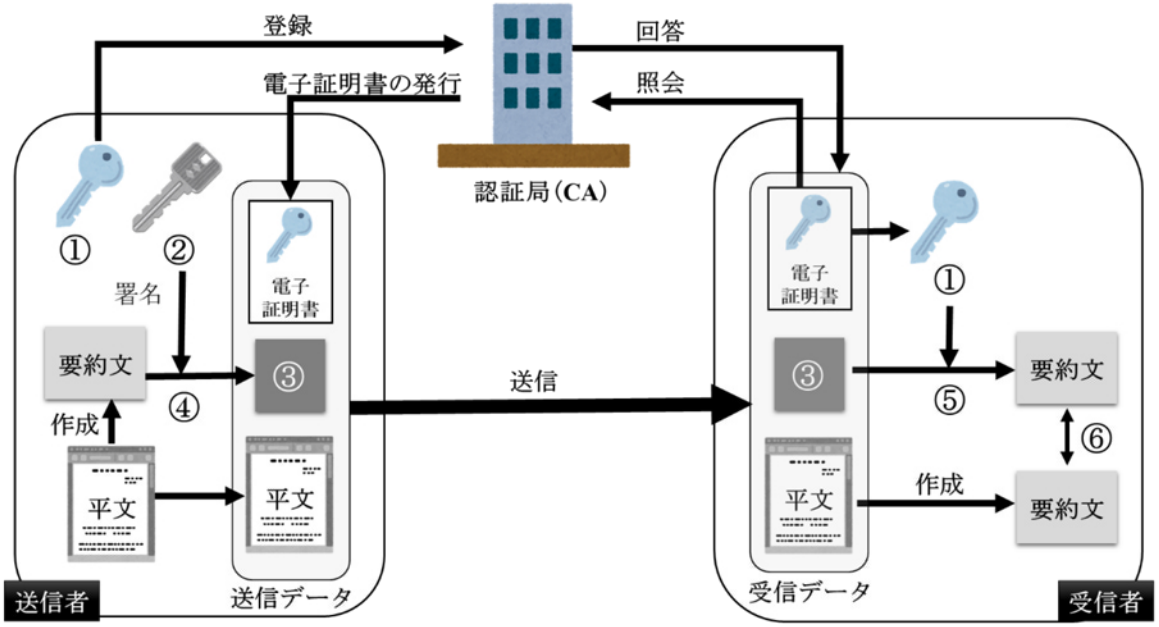

図１　電子認証のしくみ

選　択　肢

(a)	暗号化	(b)	復号	(c)	送信者の公開鍵	(d)	受信者の公開鍵
(e)	電子署名	(f)	電子文書	(g)	送信者の秘密鍵	(h)	受信者の秘密鍵
(i)	比較	(j)	複写				