問4　VPN（Virtual Private Network）（情報セキュリティ）（H25秋-FE 午後問4）

【解答】

［設問1］　エ
［設問2］　a－オ，b－ア，c－エ
［設問3］　d－エ，e－オ，f－カ

【解説】

問題のタイトルはVPN（Virtual Private Network）となっており，IPsecの基礎的な仕組みに関する問題となっている。IPsec の鍵交換方法や認証の仕組みは問題文に詳しく記述されているため，IPsec の詳細な知識がなくても，問題文を読み進めていけば解答できるようになっている。

設問1は，Diffie-Hellman鍵交換法（以下，DH法という）による鍵の作成の問題であり，図に記述された順番で計算すれば解答を導き出せる。

設問2は，公開鍵暗号方式の一つであるRSAアルゴリズムを用いたディジタル署名とデータの暗号化についての問題であり，公開鍵暗号方式と共通鍵暗号方式の仕組みが理解できていれば解答できる。

設問3は，IPsecのプロトコルの特徴と，暗号化通信，ディジタル署名の効果に関する知識を問う問題となっており，この部分については午前レベルの知識が必要となる。

［設問1］

IPsec では鍵交換方法や暗号化の方法を複数の候補から選択して利用することができる。DH 法は問題文に記述されているとおり，お互いに乱数を生成して，そこから計算された値を交換しあうことで，鍵を交換する方法である。DH 鍵の計算方法は図2に示されており，設問で与えられたZ＝11，X＝7，Y＝5を当てはめて計算すると求めることができる。

鍵A＝2^7 mod 11
　　＝128 mod 11
　　＝7
鍵B＝2^5 mod 11
　　＝32 mod 11
　　＝10

DH鍵は鍵A，鍵Bどちらを基に計算しても同じであるため，どちらを基にして計算してもよいが，両方で計算し結果が一致することを確認すると，計算間違えのチェックにもなり，より確実である。

鍵Aを基にした場合は，次のようになる。
DH鍵＝7^5 mod 11
　　＝16,807 mod 11
　　＝10

鍵Bを元にした場合は，以下のようになり計算結果が一致する。
DH鍵＝10^7 mod 11
　　＝10,000,000 mod 11
　　＝10

したがって，（エ）が正解となる。

［設問2］

図3中の空欄の穴埋め問題である。RSAアルゴリズムは素因数分解問題の困難性を利用した公開鍵暗号アルゴリズムの一つであり，問題文にあるようなディジタル署名に利用されている。

・空欄a：データから認証用ハッシュ値を算出し，RSAアルゴリズムを用いたディジタル署名を作成している。RSAアルゴリズムは公開鍵暗号方式であり，送信側しかもち得ない送信側の秘密鍵で署名を作成することで，ディジタル署名は送信側の正当性を示している。したがって，（オ）が正解である。
・空欄b：データは図3にあるように，共通鍵で暗号化して送られる。共通鍵で暗号化した暗号文は，共通鍵で復号する必要がある。したがって，（ア）が正解である。
・空欄c：署名を受信した側は送信元の正当性を確認するために，送信側の公開鍵で署名を復号する。したがって，（エ）が正解である。

一般的に公開鍵暗号方式は共通鍵暗号方式と比べて暗号化と復号に時間がかかるため，データ部分の暗号化と復号には共通鍵暗号方式を採用し，送信元の正当性確認の部分に限定して公開鍵暗号方式を採用することが多い。

［設問3］

IPsecを利用したVPNの導入効果に関する記述の穴埋め問題である。

・空欄d：IPsecがOSI参照モデルのどの層のプロトコルなのかを解答する。IPsecはネットワーク層のプロトコルである。したがって，（エ）が正解である。IPsecがどの層のプロトコルかを知らなくても，「IP」とあるように，IPパケットを暗号化して通信するためのプロトコルであるため，IPのプロトコルがネットワーク層のプロトコルであることを知っていれば解答できる。学習に当たっては，OSI参照モデルとプロトコルの関係を理解するようにしたい。
・空欄e：パケットを暗号化することで実現できることを解答する。データの中身が他者からは分からなくなるため，盗聴の対策になる。したがって，（オ）が正解である。
・空欄f：ディジタル署名を利用することで実現できることを解答する。設問2の解説でも記述したとおり，送信側の正当性を確認するためにディジタル署名を利用するので，なりすましの検知が可能になる。したがって，（カ）が正解である。

残りの解答群（ア）～（エ）は，いずれもIPsecとは関係ない技術であるため，誤りである。