問1　SSHによる通信（情報セキュリティ）　(H29秋-FE 午後問1)

【解答】

［設問1］　a－ア，b－イ
［設問2］　オ
［設問3］　ア
［設問4］　ア

【解説】

SSHによる通信を題材とした，公開鍵暗号方式と共通鍵暗号方式に関する出題である。公開鍵暗号方式と共通鍵暗号方式の違いや，ディジタル署名における署名鍵が問われている。暗号技術や認証技術の基本をしっかりと理解していれば，確実に正答できる問題である。

また，サイバー攻撃に関する内容が設問2で問われており，正解の選択肢だけではなく，解答群にある全ての攻撃内容についても，どういう攻撃であるかを理解してほしい。

［設問1］

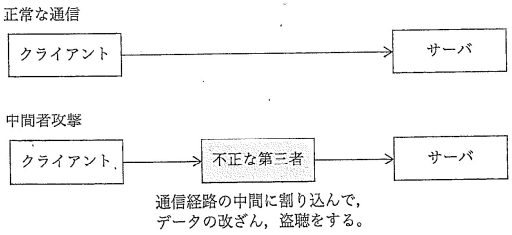
・空欄a：〔安全な通信経路の確立の概要〕(4)には「サーバ認証では，クライアントがあらかじめ入手して正当性を確認しておいた［　a　］を用い，サーバによるセッション識別子へのディジタル署名が正しいかどうかを検証する」とある。ポイントは，「サーバ認証」という記述である。サーバを認証するには，そのサーバしかもち得ない情報を確認することである。その情報とは「サーバの秘密鍵」であり，その「サーバの秘密鍵」が正しいかどうかを確認するには，「サーバの公開鍵」が必要になる。したがって，（エ）が正解である。

・空欄b：〔利用者認証の概要〕には「サーバが［　b　］を用いてディジタル署名を検証する」とある。空欄aとは逆に，「利用者認証」，つまりクライアントを認証する。クライアントを認証するには，そのクライアントしかもち得ない情報を確認することである。その情報とは「クライアントの秘密鍵」であり，その「クライアントの秘密鍵」が正しいかどうかを確認するには，「クライアントの公開鍵」が必要になる。したがって，（イ）が正解である。

［設問2］

下線①は「クライアントがサーバ認証を行う」とある。この認証によって防ぐことができる攻撃を答える。結論から先に述べると，正解は（オ）の「中間者攻撃」である。なぜこれが正解になるのか，中間者攻撃について解説する。

中間者攻撃は，通信を行う二者の間に不正な第三者が割り込んで，両者が交換する情報を改ざんしたり盗聴したりする攻撃である。



この攻撃を防ぐためには通信相手を認証する必要がある。問題文の例では，ディジタル署名を用いて通信相手を認証することで，中間者攻撃を防ぐ。

（ア）～（エ）の攻撃は，攻撃者側からサーバや別のクライアントが一方的に攻撃されるもので，サーバ認証によって防げる攻撃ではない。

ア：DoS攻撃……サーバのOSやWebアプリケーションのセキュリティホールを突いてソフトウェアを異常停止，誤動作させたり，大量の通信パケットを送り付けたりしてサーバをダウンさせる攻撃である。

イ：SQLインジェクション……データベースへの問合せを行うWebアプリケーションの入力欄に，悪意のある問合せや操作を入力し，破壊を引き起こす攻撃である。

ウ：クロスサイトスクリプティング……攻撃者は，訪問者の入力データをそのまま画面に表示するWebサイトに対して，悪意のあるスクリプトを埋め込み，訪問者のブラウザで実行させる攻撃である。

エ：総当たり攻撃……ブルートフォース攻撃とも呼ばれ，特定のアカウントを標的に，パスワードの全ての組合せを試行する攻撃である。

［設問3］

通信相手を認証する際は，公開鍵暗号方式を利用する。しかし，実際のデータ通信では，下線②に「共通鍵暗号方式による通信データの暗号化」とあるように，共通鍵暗号方式を利用する。この理由が問われている。

同じ暗号強度を求める場合，共通鍵暗号方式の方が公開鍵暗号方式よりも高速に暗号化，復号ができる。したがって，正解は（ア）である。

なお，このように，認証時と実際のデータ通信時で暗号方式を組み合わせる方法を，ハイブリッド暗号方式という。鍵の安全な配布においては公開鍵暗号方式を使い，データの送受信時には高速な共通鍵暗号方式を使うことによって，両者の長所を活かし，短所を補っている。

イ：「共通鍵暗号方式は，公開鍵暗号方式よりも解読に時間が掛かる」とあるが，同じ暗号鍵のサイズであれば，公開鍵暗号方式の方が，共通鍵暗号方式よりも解読に時間が掛かる。

ウ：「共通鍵暗号方式は，公開鍵暗号方式よりも鍵の再利用が容易」とあるが，鍵を再利用することは，第三者に解読されるリスクにつながる。このため，鍵を再利用することが，そもそも不適切である。

エ：「共通鍵暗号方式は，公開鍵暗号方式よりも鍵の配布が容易」とあるが，記述が逆であり，公開鍵暗号方式の方が鍵の配布が容易である。それは，公開鍵暗号方式の場合，相手に渡す鍵を公開してよいからである。一方，共通鍵暗号方式の場合は，第三者に秘匿のまま渡す必要があり，遠く離れた通信相手であればなおさら容易ではない。

［設問4］

下線③にある“パスワード認証”は“公開鍵認証”に比べて，安全性が低いと考えられる理由を答える。選択肢を順に見ていこう。

ア：「“パスワード認証”では，サーバが攻撃者に乗っ取られていた場合，送信したパスワードを攻撃者に取得されてしまう」リスクがある。一方，公開鍵認証の場合，サーバには秘密鍵は存在しない。盗まれても困らない公開鍵しかないので，このようなリスクは存在しない。したがって，（ア）が正解である。

イ：「正当なサーバとは異なるサーバに接続させられて」とあるが，これはサーバ認証の内容である。下線③ではクライアント認証が論点なので，関係のない記述である。

ウ：問題文には，「“公開鍵認証”では，パスワードの他にディジタル署名も用いる」という記述はなく，実際にSSHでは公開鍵認証を利用する場合，パスワードは利用しない。

エ：「“パスワード認証”では，利用者のパスワードが平文でネットワーク上を流れる」とあるが，平文ではなく暗号化されている。その根拠は，図1の「安全な通信経路の確立」と〔安全な通信経路の確立の概要〕(5)の「これ以降の通信は，全て暗号化される」であり，利用者認証の通信が暗号化されていることが分かる。