次の問1は必須問題です。必ず解答してください。

問1　SSHによる通信に関する次の記述を読んで，設問1～4に答えよ。

SSH は遠隔ログインのための通信プロトコル及びソフトウェアであり，通信データの盗聴対策や，通信相手のなりすましを防ぐ仕組みを備えている。SSH では，サーバにログインしてデータをやり取りする通信（以下，ログインセッションという）に先立って，安全な通信経路の確立と利用者認証を行う必要がある。安全な通信経路の確立，利用者認証及びログインセッションを合わせて SSH セッションと呼ぶ。その流れを，図1に示す。

図1　SSHセッションの流れ

〔安全な通信経路の確立の概要〕

安全な通信経路の確立は，次のようにして行う。

(1) クライアントがサーバにアクセスする。

(2) サーバとクライアントが，SSH セッションで使用する暗号アルゴリズムについて合意する。

(3) サーバとクライアントが，通信データの暗号化に使用するセッション鍵と，他の SSH セッションと区別するためのセッション識別子について合意する。

(4) ①クライアントがサーバ認証を行う。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。

(5) 合意した暗号アルゴリズムとセッション鍵を用いて，②共通鍵暗号方式による通信データの暗号化を開始する。これ以降の通信は，全て暗号化される。

〔利用者認証の概要〕

クライアントからサーバへのログインでは，サーバは利用者認証を行う。SSH の利用者認証の方式には，ディジタル署名を用いる“公開鍵認証”とパスワードを用いる“パスワード認証”がある。

“公開鍵認証”では，クライアントの公開鍵を事前にサーバに登録しておき，この登録されている公開鍵に対応する秘密鍵をクライアントがもっていることをサーバが確認する。この確認では，クライアントがセッション識別子などに対するディジタル署名をサーバに送信し，サーバが［ b ］を用いてディジタル署名を検証する。

“パスワード認証”では，クライアントが利用者 ID とパスワードを送信し，サーバは受け取ったパスワードが当該利用者のパスワードと一致していることを検証する。

なお，③“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ている。

設問1　本文中の［　　］に入れる適切な答えを，解答群の中から選べ。

a，b に関する解答群

ア　安全な通信経路の確立時に合意したセッション鍵

イ　クライアントの公開鍵

ウ　クライアントの秘密鍵

エ　サーバの公開鍵

オ　サーバの秘密鍵

設問２　本文中の下線①によって防ぐことができる攻撃として適切な答えを，解答群の中から選べ。

解答群

ア　DoS攻撃　　イ　SQLインジェクション

ウ　クロスサイトスクリプティング　　エ　総当たり攻撃

オ　中間者攻撃

設問３　本文中の下線②について，通信データの暗号化に公開鍵暗号方式ではなく共通鍵暗号方式を用いる理由として適切な答えを，解答群の中から選べ。

解答群

ア　共通鍵暗号方式は，公開鍵暗号方式よりも暗号処理が高速である。

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。

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である。

設問４　本文中の下線③のように考えられている理由として適切な答えを，解答群の中から選べ。

解答群

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。

イ　“パスワード認証”では，正当なサーバとは異なるサーバに接続させられてしまっても利用者が気づけない。

ウ　“パスワード認証”では，パスワードだけを用いるが，“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。

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ので，盗聴されるとパスワードを取得されてしまう。