問題５　次の利用者認証に関する各設問に答えよ。

クライアントからサーバへ接続する場合，セキュリティ上の必要性から利用者認証をする場合がある。利用者認証には様々な方法があるが，認証情報の盗聴や漏えいを防止するための方法も考えなければならない。

＜設問１＞　次の利用者 ID とパスワードによる認証方式に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

利用者はサーバに利用者 ID とパスワードを送信し，サーバ側で登録してある利用者 ID とパスワードかを判断して認証を行うものである。

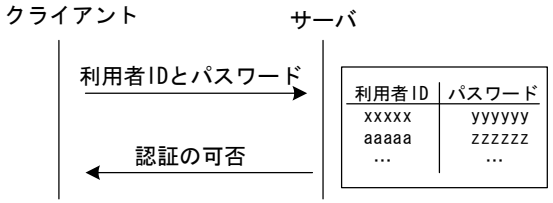

図１　利用者 ID とパスワードによる認証

パスワードには推測されにくい文字を利用し，桁数を増やすなどしてパスワードの強度を高める必要がある。

ここで，パスワードを発見するために，″aaa″，″aab″，″aac″，…，″zzz″のように，1 文字ずつ入れ替える総当たり方式で探索する場合を考える。

英小文字だけの 4 文字を使用して作成したパスワードを総当たり方式で発見するのにかかる時間が最大で T とした場合を考える。

英小文字と英大文字を使用した場合，1 文字当たりの選択肢は 2 倍になるので，4 文字で作成したパスワードは，発見に要する時間が最大で［　(1)　］となる。

なお，サーバ側では，［　(2)　］仕組みを導入して，総当たり方式によるパスワードの発見を防ぐ必要がある。

さらに，パスワードが盗聴されない工夫も必要である。パスワードが盗聴される要因として，パスワードを入力する現場を盗み見られる場合や，不正プログラムによりキーボードから入力した文字を外部に送信する［　(3)　］がある。

(1) の解答群

ア．2×T　　イ．8×T　　ウ．16×T　　エ．26×T

(2) の解答群

ア．暗号化通信を行う
イ．指定された IP アドレスからの接続だけを許可する
ウ．定期的にパスワードを変更する
エ．連続して認証に失敗した利用者 ID を使用不可にする

(3) の解答群

ア．キーロガー　　イ．ゼロディアタック
ウ．バックドア　　エ．ポートスキャン

＜設問２＞　次のワンタイムパスワードに関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

一度だけ有効なパスワードをワンタイムパスワードと呼ぶ。ワンタイムパスワードの生成にはいくつかの方法があるが，ここでは２つの方法について検証する。

［時刻同期方式］

トークンと呼ばれるパスワード生成器を利用するもので，トークンには時刻をもとに生成したパスワードが表示される。サーバにもトークンと同じ仕組みでパスワードを生成する仕組みが存在するので，利用者から送信されたパスワードとサーバで生成したパスワードを比較して認証の可否を判断する。

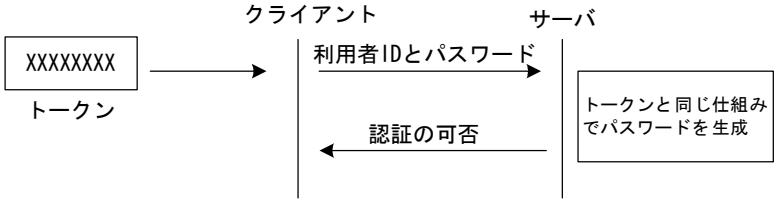

図２　時刻同期方式による認証

この方式の場合，［　(4)　］必要がある。

トークンは，おもに１分間隔でパスワードを生成するが，トークンとサーバでズレが生じる可能性がある。サーバでは，このズレに対して許容範囲を設定している。例えば,前後１分ずれた場合のパスワードと一致すれば認証を許可するようにしている。

(4) の解答群

ア．DHCP サーバから IP アドレスを再取得する
イ．あらかじめトークンとサーバの時刻を同期させる
ウ．トークンとサーバ間で自動認証を行う
エ．利用者 ID を登録しているテーブルの再構築する

［S/Key 方式］

回数を示す番号（シーケンス番号）やシードと呼ばれる値などをもとに一方向ハッシュ関数に入力した結果をパスワードとして用いる方式である。

S/Key 方式は，次のような手順で行う。

＜事前準備＞

① 利用者は利用者 ID とパスフレーズをサーバに登録する。

② サーバはランダムに生成したシードとパスフレーズを一方向ハッシュ関数に入力して 1 回目のワンタイムパスワードを生成する。2 回目以降は，1 回前のワンタイムパスワードをシードとして一方向ハッシュ関数に入力して生成する。

一方向ハッシュ関数を H，パスフレーズを p，ランダムに生成したシードを r とすれば，n 回目のワンタイムパスワードは次のように表現できる。

$$\text{n 回目のワンタイムパスワード} = \underbrace{H(p,\ H(p,\ H(\cdots,\ H(p,\ H(p,\ r))\cdots)))}_{\text{n 回}}$$

生成したワンタイムパスワードは，シーケンス番号とともに記録する。

＜認証の手順＞

① クライアントからサーバへ利用者 ID を送信する。

② サーバからシーケンス番号（n-1）とシードをクライアントに送信する。なお，シーケンス番号はアクセスするたびに 1 ずつ増加されてサーバに記録される。

③ クライアントは，一方向ハッシュ関数にパスフレーズとサーバから送られてきたシードを入力してワンタイムパスワードを生成し，サーバへ送る。

④ クライアントから受け取ったワンタイムパスワードとパスフレーズを一方向ハッシュ関数に入力して n 回目のワンタイムパスワードを生成し，登録してある n 回目のワンタイムパスワードと比較して認証の可否を判断する。

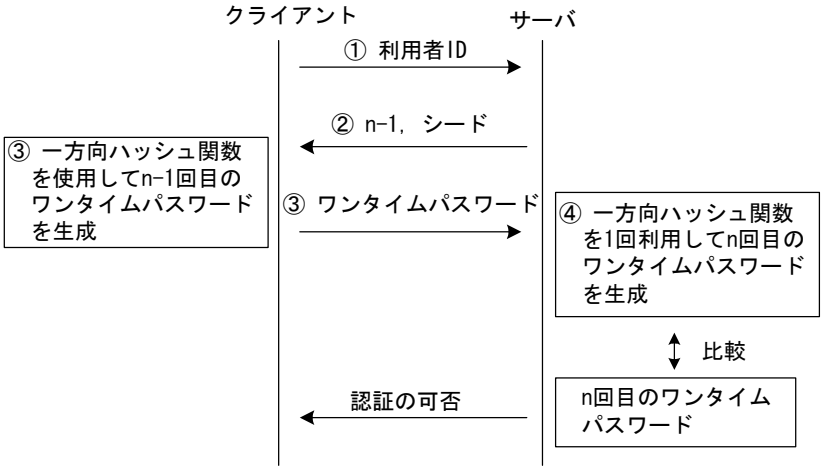

図３　S/Key による認証

ここで，認証の手順②～④を検証する。

なお，サーバ側で記録しているワンタイムパスワードとパスフレーズおよびシードは，図４のようになっているものとする。また，サーバとクライアントで同じハッシュ関数を用いる。

パスフレーズ 0000

シード 1111

シーケンス番号	ワンタイムパスワード
⋮	⋮
29	2222
30	3333
31	4444
⋮	⋮

図４　サーバに登録されている情報

認証手順	検証内容
②	30 回目の認証を行う場合，認証手順②でサーバからクライアントに送信されるシーケンス番号は 29 である。
③	クライアントの一方向ハッシュ関数で生成するワンタイムパスワードのもとになる値は 0000 と［　(5)　］であり，一方向ハッシュ関数を 29 回利用してワンタイムパスワードを生成する。正しい一方向ハッシュ関数を用いていれば，サーバに送信される値は［　(6)　］である。
④	サーバが受け取ったワンタイムパスワードとパスフレーズを一方向ハッシュ関数に入力して返された値が［　(7)　］であれば，認証が許可される。

この方法では，クライアントとサーバ間でやりとりされる利用者 ID，パスフレーズ，シーケンス番号，シードが盗聴されたとしても［　(8)　］が漏えいしない限り第三者が認証されることはない。

(5) ～ (7) の解答群

ア．29　　イ．30　　ウ．31　　エ．0000

オ．1111　　カ．2222　　キ．3333　　ク．4444

(8) の解答群

ア．n-1 回目のワンタイムパスワード

イ．n 回目のワンタイムパスワード

ウ．一方向ハッシュ関数

エ．サーバに登録しているワンタイムパスワードの数