問040001解説

◆解答

設問１　ａ　カ　　ｂ　エ

設問２　ｃ　ア　　ｄ　エ　　ｅ　ア

◆解説

利用者認証に関する問題である。

パスワードとは

パスワードはコンピュータで利用者の認証を行うために利用される数字や文字列である。利用制限を行っているコンピュータや共有資源では、ユーザＩＤとパスワードによって利用者であることを認証する。ユーザＩＤの保有者自身が実際にアクセスしているかどうかを確認するために利用する。正当な利用者以外にパスワードを漏洩したり、推測しやすいパスワードを設定すると、悪意ある第三者による不正利用の恐れがある。パスワードの発行はユーザＩＤの発行手続きと同様な方法をとる。

パスワード設定上の留意点

① パスワード入力の際にパスワード自体の表示や印字を抑止する。
② パスワードの有効期限を設定する。
③ 利用者が自分のパスワードをいつでも自由に変更できるようにする。
④ パスワードを暗号化してファイル上に格納する。
⑤ パスワードを保存するパスワードファイルのアクセスを制限する。
⑥ 高度パスワードを適用し、類推できるようなパスワードの使用を制限する。
⑦ 初期パスワードの設定をする。
⑧ 初期パスワードは、初回だけ仮パスワードで情報処理システムへアクセスを許し、ファイルアクセス前にユーザ側で正式のパスワードに変更しなければならない方法にする。
⑨ パスワードは数字と文字列の組合せで作成し、８桁～１４桁以上が望ましい。

パスワードの強度を高める方法

① パスワードの桁数を多くする。通常は８桁以上、可能ならば１４桁以上が望ましい。
② １桁の文字数を多くする。アルファベットと数字、または、アルファベットの大文字、小文字、数字の組合せなどを用いる。

パスワードの種類の場合の数の計算法（強度）

１桁の文字数の種類をＸ、パスワードの桁数をＮとすると、パスワードの種類の数Ｙは次の式で与えられる。

$$Y = X^N$$

０～９の数字を使用し、８桁のパスワード場合、10^8種類

０～９の数字を使用し、１４桁のパスワード場合、10^{14}種類

アルファベット２６文字、数字１０文字の８桁のパスワードの場合、36^8種類
大文字、小文字、数字の８桁のパスワードの場合、62^8種類

リプレイアタック

クライアントとサーバ間で暗号鍵を共有し、パスワードを送る場合、毎回暗号化された同じデータで通信すると、そのデータを盗聴し、正当なユーザと偽ってサービスを要求すると、サーバは正当なユーザと認証してしまう。不正者は正しいパスワードを知らないまま正当なユーザになりすますことができる。これをリプレイアタックと呼ぶ。

ワンタイムパスワード

リプレイアタックを考慮すると、認証のためのデータは毎回異なるものにする。パスワードと現在時刻を組み合わせて情報を暗号化する。時刻が変化するため、認証に用いるデータも変化する。

チャレンジレスポンス方式

利用者からの依頼があると、その都度ランダムにチャレンジを生成し、利用者の入力したパスワードとチャレンジを組み合わせてハッシュ関数を利用して、レスポンスを送信する。ハッシュ関数は公知のものであるから、パスワードとチャレンジを盗聴されるとレスポンスを生成することができる。

トークン方式

利用者ＩＤとトークンを利用して、時刻によって変化するパスワードを使用する方式である。時刻が変化するため、認証に用いるデータも変化する。

設問１

aは、１桁２６文字、８桁の場合の種類の数は26^8種類になる。桁数が１０桁になると種類の数は26^{10}種類になる。従って、その比率は$(26^{10})/(26^8)=26^2=676$となる。求める答えはカとなる。

bは、英文字の大文字、小文字を使用する場合は$52^8=(26\times2)^8$となり、小文字のみの場合との比率は$((26\times2)^8)/(26^8)=2^8=256$となり、求める答えはエとなる。

設問２

利用者ＩＤとパスワードが不正な方法によって入手される場合について考える。

cは、通信経路上で利用者ＩＤとパスワードが盗聴された場合であるから、方式１の場合は不正利用者がそのまま入力すれば、サーバは正しい利用者と判断する。方式２では、ユーザＩＤ、チャレンジ、レスポンス、パスワードの連続した一連の処理の結果で認証するため、ユーザＩＤ、チャレンジ、レスポンスが盗聴されても、パスワードが盗まれない限り不正アクセスにはならない。方式３は刻々パスワードが時間と共に変化するため、トークンが盗まれない限り問題は発生しない。求める答えはアとなる。

dは、キーボード入力時に利用者ＩＤとパスワードが盗まれる場合である。方式１は不正アクセス可能である。方式２はパスワードが盗まれるため、チャレンジからレスポンスが作成可能になり、不正アクセスが可能になる。方式３はトークンが盗まれない限り、パスワードが刻々変化するため不正アクセスにはならない。求める答えはエとなる。

eは、不正サーバ内の情報である利用者ＩＤとパスワードが盗まれる場合である。方式１は利用者ＩＤとパスワードを入力すれば不正アクセス可能である。方式２の場合は通常のログイン操作では接続されない。方式３ではトークンがないため操作できない。求める答えはアとなる。