問4　利用者認証（情報セキュリティ）　(H21秋-FE 午後問4)

【解答】
［設問1］　a－カ，b－エ
［設問2］　c－ア，d－エ，e－ア

【解説】
利用者認証として，〔利用者IDとパスワード方式〕，〔チャレンジレスポンス方式〕，〔トークン（パスワード生成器）方式〕の三つの方式に関し，クライアントとサーバ間での通信内容を比較して，各方式のパスワードの強度と安全性やリスクを検証する問題である。ランダムに生成されるチャレンジや，これを基に計算されるハッシュ値，レスポンスなど認証技術のキーとなる用語を盗聴のリスクと対比させて理解しておくことが大切である。また，実際にトークンを利用した経験がない場合は，トークンとサーバの同期や認証に必要な一定時間の許容値が存在することをトークン方式の基礎知識として，それらの意味を把握しておくことも必要である。設問1は，パスワードの文字数による組合せ総数の計算方法と強度に関する問題である。設問2では，各方式において端末から入力されたデータや，端末とサーバ間でやり取りされるデータの盗聴のリスクを(1)平文のパスワード，(2)キーロガーによる入力データの盗聴，及びフィッシング等によって(3)不正なサーバに誘導された場合の情報の盗聴や漏えいを想定し，解答する問題である。問題文の記述は，特別高度な内容ではなく，盗聴のリスクによって不正ログインが可能になるケースについての理解を試すものである。

［設問1］
・空欄a：任意の1文字からなる文字列を1文字のパスワードと比較して等しいことを確認するのに必要な最大時間をtとすると，英小文字26文字だけからなる8文字のパスワードに対する組合せ総数は26の8乗（26^8）であるため，総当たり方式による発見に必要な最大時間は，$26^8 \times t$となる。同様にパスワードの長さが10文字の場合の総当たり方式による発見に必要な最大時間は，$26^{10} \times t$であるが，これは$26^{10} \times t = 26^2 \times 26^8 \times t$と展開できる。$26^8 \times t = 1$とすれば，$26^{10} \times t = 26^2 = 676$となる。したがって，（カ）が正解である。
・空欄b：英大文字も使用すると合計52文字から8文字のパスワードを生成することになるため，パスワードの組合せの総数は，52の8乗（52^8）であるから必要な最大時間は，$52^8 \times t = 2^8 \times 26^8 \times t$となる。$26^8 \times t = 1$とすれば，$2^8 \times 26^8 \times t = 2^8 = 256$となる。したがって，（エ）が正解である。

［設問2］
三つの方式の特徴について最初に確認すると，方式1では，IDとパスワードは暗号化されず平文（ひらぶん）のままサーバに送信されるため，これらが盗聴された場合には，サーバへの不正ログインが可能となる。
方式2では，パスワードpが平文でサーバに送信されることはなく，パスワードpとサーバから受信した乱数であるチャレンジcから計算されたハッシュ値$h(p,c)$がレスポンス値としてサーバに送信される。ハッシュ関数の一方向性によって，ハッシュ値から元の値を求めることができないため，通信を盗聴された場合でもパスワードを知ることは事実上不可能とされている。
方式3では，パスワードは利用者IDと時刻から関数gを使ってトークンで生成され，サーバに送信される。サーバとトークンの時刻の同期は保証されており，同じ関数を使ってサーバ側で生成したパスワードと比較され，一致した場合にログインができる仕組みである。パスワードの有効期間が許容された時間内に限定されるため，通信経路からパスワードを盗んで不正ログインすることが困難となっている。
・空欄c：盗聴に対して問題があるのは，通信経路が暗号化されておらず，利用者IDとパスワードが平文のまま送信される場合である。盗聴後も利用者がパスワードを変更していない場合は，盗んだIDとパスワードをそのまま利用してサーバへ不正ログインすることが可能となる。方式1はこれに該当する。方式2では，通信経路上にはハッシュ値$h(p,c)$が送信されて平文のパスワードpをそのまま盗聴することができず，不正ログインをすることができない。方式3では，通信経路上にはパスワード$g(u,t)$が送信されるが，このパスワードは一定の許容時間内だけに有効であるため，「利用者がパスワードを変更しない限り」に当てはまらない。したがって，方式1だけ不正ログインがいつでも可能となる。したがって，（ア）が正解である。
・空欄d：これはキーボードからの入力を監視して記録するキーロガーのプログラムが動作している場合を想定したものであり，リモートログインの端末上で悪意のある第三者によって仕掛けられた場合は，IDとパスワード情報を盗むことができる。キーロガーでは，入力情報がキーボードから直接読み取られるので，利用者がパスワードを変更していない場合には，通信経路の暗号化とは無関係にサーバへの不正ログインがいつでも可能であり，方式1と方式2が該当する。方式3では，キーボード入力で読み取った情報から生成されたパスワード$g(u,t)$と利用者IDがサーバに送信されるが，上記で述べたとおり，このパスワードは一定の許容時間内だけに有効であることから，不正ログインがいつでも可能となるのは，方式1，2だけとなる。したがって，（エ）が正解である。
・空欄e：利用者が気付かないうちに不正なサーバに誘導されるフィッシングのような場合では，不正なサーバで入力してしまった正しい利用者IDやパスワードが，正式なサーバでそのまま悪用された場合には，利用者がパスワードを変更していない限り，不正ログインがいつまでも可能となる。平文が送信される方式1は，このケースに該当する。方式2では，不正なサーバには，正しいパスワード情報p'が存在しないため，ログインが行われたように詐称することはできたとしても，正規のパスワードを取得することはできない。方式3では，通信経路上にはパスワード$g(u,t)$が送信されるが，不正なサーバ側で関数gが分かっていない場合や時刻が同期していない場合は，パスワードを正しく生成することができず，照合が不可能なため不正ログインすることができない。したがって，方式1だけ不正ログインがいつでも可能で，（ア）が正解となる。

なお，本問にも出てくるハッシュ関数として実際には，MD5（Message Digest 5）やSHA-1（Secure Hash Algorithm 1），SHA-2（Secure Hash Algorithm 2）などが実装レベルで使用される。MD5やSHA-1では，ハッシュ値の衝突や攻撃が報告されており，必ずしも安全とは言えなくなってきている。