●平成30年度春期

午後問題 解答・解説

問1　Webサービスを利用するためのパスワードを安全に保存する方法（情報セキュリティ）　(H30春-FE 午後問1)

【解答】

［設問1］　a－エ，b－イ
［設問2］　c－イ，d－エ
［設問3］　エ

【解説】

Webサービスにおけるパスワードの安全な保存を題材に，ハッシュ関数の特性や技術的な仕組みに焦点を当てた問題である。ソルトやストレッチングといった専門的な知識が詳しく解説されており，その知識を理解した上で問題を解く必要がある。簡単な問題とは言えないが，問題文の記述をよく読み込むことで，正解が導けるようになっている。正答が分からない場合でも，関連知識を駆使することで，消去法で正解を導き出すこともできるであろう。

［設問1］

・空欄a：空欄aに入れる用語を答える。問題文には「ハッシュ関数の一つである［ a ］を用いる」とある。五つの選択肢の中から，ハッシュ関数を選べば正解になる。

（エ）の「SHA-256」は，SHA-2（Secure Hash Algorithm 2）の一つで，ハッシュ値として256ビットの値を出力するハッシュ関数である。したがって，正解である。

ア：AES（Advanced Encryption Standard）は，共通鍵暗号方式である。
イ：Diffe-Hellmanは，共通鍵暗号を使う際に，情報の送り手と受け手が安全に鍵を共有する方法である。DHとも呼ばれる。
ウ：RSA（発明者のRivest，Shamir，Adlemanの頭文字）は，アルゴリズムに「大きな桁数の素数を掛け合わせた数値から，それを素因数分解して元となった素数を求めることは困難である」という数学的性質を利用した代表的な公開鍵暗号方式である。
オ：TLS（Transport Layer Security）は，HTTPSなどで利用される通信プロトコルで，認証や暗号，改ざん検知の仕組みをもつ。

・空欄b：空欄bに入るハッシュ関数の特徴を答える。ハッシュ関数の特徴を理解していれば，難しくない問題である。また，ハッシュ関数の特徴を理解していなかったとしても，空欄bの前の記述にある「パスワードが一致していることの確認に用いる」という要件を理解すれば，正解を導くことができる。（イ）の記述にあるような「同一のパスワードをハッシュ化すると，同じハッシュ値になる」という特性がないと，「パスワードが一致していることの確認に用いる」ことができない。図1ではパスワードが一致しているかどうかを，ハッシュ値が同じかどうかで照合している。したがって，（イ）が正解である。

ア：異なるパスワードから生成したハッシュ値が一致することも稀にあるが，その確率は非常に低い。このように，たまたまハッシュ値が一致するデータをシノニムという。
ウ：「パスワードをハッシュ化した結果のハッシュ値を再度ハッシュ化」しても，元のパスワードにはならない。
エ：秘密鍵を使用しても，ハッシュ値から元のパスワードを復元することはできない。

［設問2］

・空欄c：設問文には，「このとき得られるハッシュ値は，パスワードだけをハッシュ化した場合のハッシュ値［ c ］」とある。〔ハッシュ化に用いるハッシュ関数の特徴〕の(4)に「パスワードが1文字でも異なれば，ハッシュ値は大きく異なる」とあるように，元の値が違えばハッシュ値は異なる。ソルトとパスワードを連結した文字列をハッシュ化した場合は，元になるパスワードが同じであっても生成されるハッシュ値は異なる。したがって，（イ）の「とは異なる値になる」が正解である。

ア：「と同じ値になる」とあるが，(4)にあるように，パスワードが1文字でも異なればハッシュ値は異なる。
ウ：「よりも長さが長い」とあるが，(1)にあるように，ハッシュ値は固定長である。
エ：「よりも長さが短い」とあるが，(1)にあるように，ハッシュ値は固定長である。

・空欄d：設問文には，「ソルトを用いる方式が，事前計算による辞書攻撃の対策として効果があるのは，［ d ］からである」とある。

攻撃者が「パスワードとしてよく使われる文字列を，よく使われているハッシュ関数でハッシュ化し，ハッシュ値から元のパスワードが検索可能な一覧表を作成しておく」ことに対し，「十分な長さをもつランダムな文字列である」ソルトを用いる方式を提案することにした。「この方式におけるパスワードの保存では，まず，サーバは新しいパスワードの保存の都度，新しいソルトを生成し，ソルトとパスワードを連結した文字列をハッシュ化する」。

つまり，「ソルトがどのような値になるか分からない」ので，「ソルトとパスワードを連結した文字列」の組合せは，ソルトを使わない場合に比べて圧倒的に多くなる。このため，「攻撃者が一つのパスワードに対して事前に求めるハッシュ値の数が膨大になる」という（エ）が正解である。

ア：攻撃者は「ソルトから元のパスワードを検索する」ことはしない。というのも，図2を見ると，ソルトからパスワードを作成したわけでもなく，ソルトとパスワードは無関係だからである。
イ：図2を見ると，パスワードファイルには「ソルト」と「ハッシュ値」が入っていることが分かる。したがって，攻撃者がパスワードファイルを入手すると，ソルトも入手できる。
ウ：ソルトを用いた場合も，攻撃者がパスワードファイルを入手する困難さは同じである。

［設問3］

ストレッチングの方式を図にすると，次のようになる。つまり，パスワードからハッシュ値を求めるのに，連結結果をハッシュ化する処理を指定した回数だけ繰り返している。したがって，繰り返す分だけ，（エ）にあるように「一つのパスワードの候補からハッシュ値を求める時間が増加する」。したがって，（エ）が正解である。

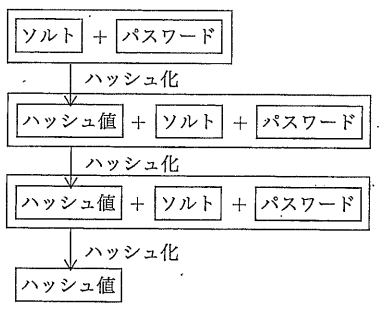

図　ストレッチングの方式

ア：パスワードの文字列長は変わらない。
イ：ハッシュ値の長さは，〔ハッシュ化に用いるハッシュ関数の特徴〕の(1)にあるように，固定長である。長くなるようなことはない。
ウ：「パスワードの候補から求めたハッシュ値」と「パスワードファイルのハッシュ値」を比較しても意味がない。ストレッチングの図にあるように，ソルトが付与されているからである。