次の問1は必須問題です。必ず解答してください。

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に関する次の記述を読んで，設問1～3に答えよ。

A社が提供するWebサービスを利用するには，利用者が決めた利用者IDとパスワードを，Webアプリケーションが動作するサーバに登録しておく必要がある。A社のWebアプリケーションでは，利用者がWebアプリケーションにログインするときに，Webブラウザから利用者IDとパスワードがサーバに送信される。サーバは，受信した利用者IDとパスワードを，照合することによって認証する。利用者が決めたパスワードは，パスワードファイルに平文で保存されている。

近年，パスワードファイルが漏えいし，不正ログインが発生したと考えられる事件が多数報道されている。そこで，A社に勤めるCさんは，自社のWebアプリケーションにおけるパスワードファイルが漏えいした際の不正ログインを防止するための対策について，上司から検討を命じられた。

Cさんは対策として，パスワードを平文で保存するのではなく，ハッシュ関数でパスワードのハッシュ値を計算（以下，ハッシュ化という）し，そのハッシュ値を保存する方式を提案することにした。この方式におけるログイン時の認証では，受信したパスワードから求めたハッシュ値を，パスワードファイルに保存されているハッシュ値と照合する。パスワードの保存の流れと，照合の流れを図1に示す。

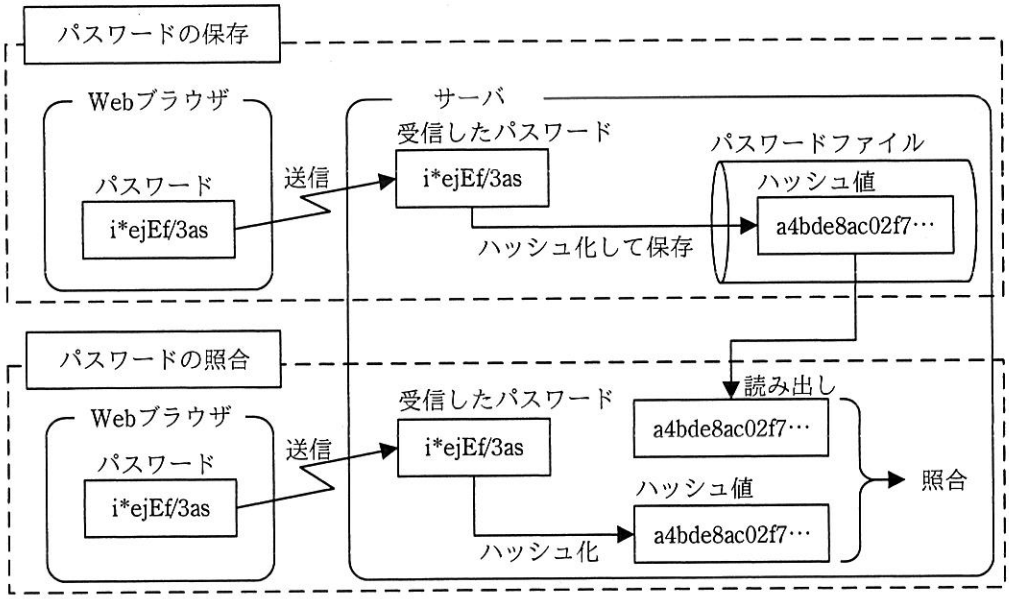

図１　パスワードの保存の流れと，照合の流れ

Ｃさんは，パスワードのハッシュ化には，ハッシュ関数の一つである［　a　］を用いることにした。ハッシュ化に用いるハッシュ関数は，一般的に次のような特徴を備えているので，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る。また，利用者のパスワードを平文で保存する場合と比べて，パスワードファイルが漏えいしても，より安全だと考えたからである。

〔ハッシュ化に用いるハッシュ関数の特徴〕

(1)　パスワードの長さに関係なく，ハッシュ値は固定長になる。

(2)　［　b　］

(3)　ハッシュ値からパスワードを推測することが非常に困難である。

(4)　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。

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に関する解答群

ア　AES　　イ　Diffie-Hellman　　ウ　RSA

エ　SHA-256　　オ　TLS

bに関する解答群

ア　異なるパスワードをハッシュ化したとき，同じハッシュ値になる可能性が高い。

イ　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。

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すると，元のパスワードになる。

エ　秘密鍵を使用してハッシュ値から元のパスワードを復元できる。

設問2　次の記述中の［　　］に入れる適切な答えを，解答群の中から選べ。

Cさんは，自身が提案する方式について，社内の情報セキュリティ責任者にレビューを依頼したところ，この方式は漏えいしたパスワードファイルを攻撃者に入手された場合，事前計算による辞書攻撃に弱いという指摘を受けた。この攻撃では，あらかじめ攻撃者は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。その後，攻撃者が漏えいしたパスワードファイルを入手したとき，この作成した一覧表からハッシュ値を検索する。ハッシュ値が一覧表に載っている場合は，元のパスワードを容易に知ることができる。

Cさんは，事前計算による辞書攻撃を難しくする方式を調査し，ソルトを用いる方式を提案することにした。ソルトとは，十分な長さをもつランダムな文字列である。

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。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　］。次に，ハッシュ化に使用したソルトと得られたハッシュ値をパスワードファイルに保存する。

この方式におけるパスワードの照合では，まず，サーバはパスワードファイルからソルトとハッシュ値を読み出す。次に，読み出したソルトと受信したパスワードを連結した文字列をハッシュ化し，得られたハッシュ値を，読み出したハッシュ値と照合する。ソルトを用いたパスワードの保存の流れと，照合の流れを図2に示す。

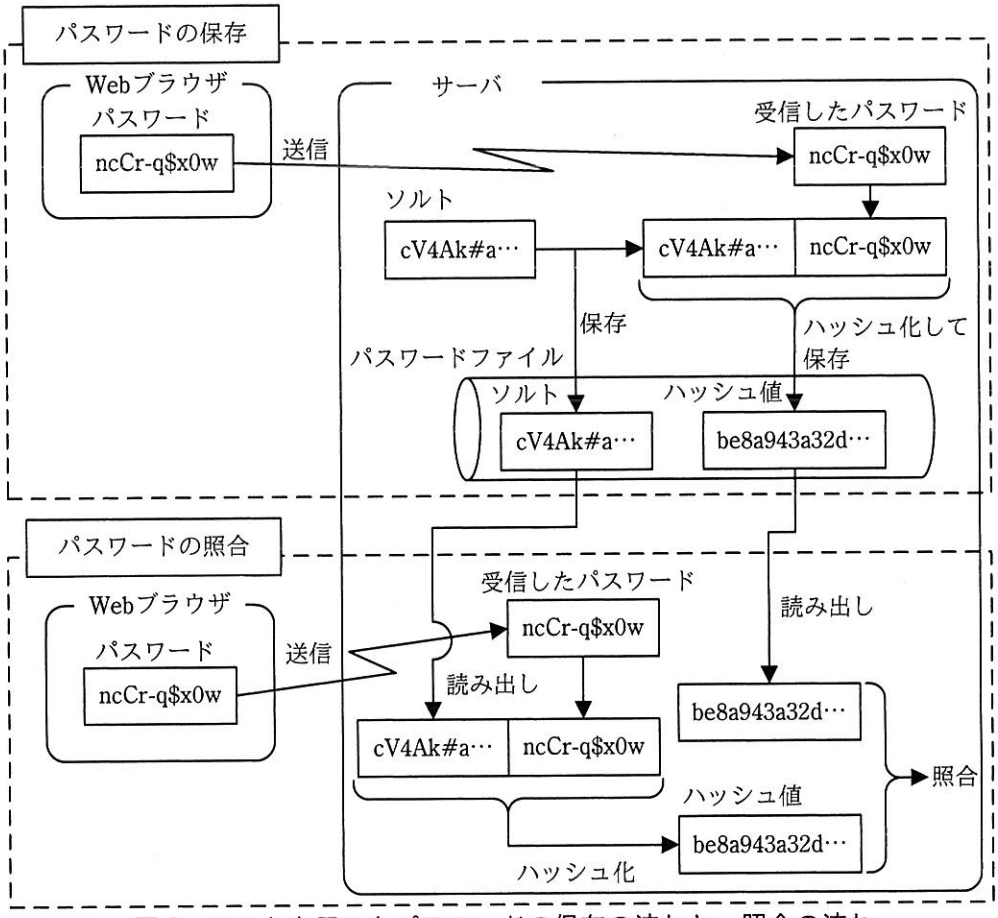

図２　ソルトを用いたパスワードの保存の流れと，照合の流れ

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。

c に関する解答群

ア　と同じ値になる　　イ　とは異なる値になる

ウ　よりも長さが長い　　エ　よりも長さが短い

d に関する解答群

ア　攻撃者が，ハッシュ値からではなくソルトから元のパスワードを検索するための一覧表を事前に作成しておく必要がある

イ　攻撃者がパスワードファイルからソルトを入手できない

ウ　攻撃者がパスワードファイルを入手するのが困難になる

エ　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

設問３　次の記述中の［　　］に入れる適切な答えを，解答群の中から選べ。

Ｃさんは，オフライン総当たり攻撃についても，対策を検討することにした。

漏えいしたパスワードファイルに対するオフライン総当たり攻撃とは，攻撃者が，パスワードファイルを入手した後，全てのパスワードの候補を逐次生成してはハッシュ化し，得られたハッシュ値がパスワードファイルに保存されているハッシュ値と一致するかどうか，しらみつぶしに確認することによって，ハッシュ値の元のパスワードを見つける攻撃方法である。

Ｃさんは，オフライン総当たり攻撃を難しくする方式として，ストレッチングという方式があることを知った。

この方式では，まず，ソルトとパスワードを連結した文字列をハッシュ化してハッシュ値を得る。次に，得られたハッシュ値の後にソルトとパスワードを連結し，その連結結果をハッシュ化する。この操作を指定した回数だけ繰り返すことによって，パスワードの照合に用いるハッシュ値を得る。パスワードファイルには，ソルト及びパスワードの照合に用いるハッシュ値に加えて，繰返し回数も保存する。この方式では，ハッシュ化の操作を１回だけ行う方式と比べると，攻撃者が，オフライン総当たり攻撃を行う際，［　　］。

解答群

ア　生成すべきパスワードの候補の最大文字列長が長くなる

イ　一つのパスワードの候補から求めたハッシュ値の長さが長くなる

ウ　一つのパスワードの候補から求めたハッシュ値を，パスワードファイルのハッシュ値と比較する回数が増える

エ　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