問 3　パスワードへの攻撃に関する次の記述を読んで，設問 1～4 に答えよ。

Z 社は，従業員数 300 名の衣料品販売企業であり，インターネット上で衣料品を購入できるショッピングサイト（以下，Z サイトという）を 7 年前から運営している。Z サイトは，携帯電話，スマートフォン及び PC を対象としたサイトであり，オンライン決済にはクレジットカードを採用している。クレジットカード情報は会員情報として保存せずに，決済の都度入力してもらう方式にしている。利用者は，会員登録をすれば，購入金額に応じたポイントをためて，購入代金への充当や，他社のギフト券への交換ができる。Z サイトの現在の会員数は約 400 万人である。

Z サイトの会員の利用者 ID は，会員のメールアドレスであり，パスワードは，携帯電話での利便性を考慮し，数字 6 桁の固定長となっている。同じ日の 0 時から 24 時の間に連続 5 回認証に失敗した利用者 ID は，アカウントロック状態となり，翌日にその状態が解除される仕組みとなっている。

〔不正アクセスの発生〕

ある日，Z サイトの問合せ窓口の担当者から，Z サイトの運用を担当しているシステム運用部の A 主任に連絡があり，ポイントが勝手にギフト券に交換されたという被害の連絡を，会員 11 名から受けたことが報告された。報告を受けた A 主任がログサーバを調査したところ，特定の IP アドレスから，Z サイトの会員ページへのログイン試行が，短時間のうちに大量に発生していたことが分かった。A 主任は，上司である B 部長の指示の下，全会員に事象を告知するとともに，経営陣の承認を経て Z サイトを緊急閉鎖し，以前にセキュリティ診断を依頼したことがある Y 社に，この不正アクセスの調査を依頼した。大量のログイン試行のログを表 1 に示す。

表 1　大量のログイン試行のログ（抜粋）

日時	接続元 IP アドレス	利用者 ID	パスワード
2014/9/18 19:21:10	x.y.1.12	abcde@aaaaa.ne.jp	123456
2014/9/18 19:21:10	x.y.1.12	agikaen@bbbbb.com	123456
2014/9/18 19:21:11	x.y.1.12	12ko3k3@bbbbb.com	123456
2014/9/18 19:21:12	x.y.1.12	k323t4t34@ccccc.ne.jp	123456
2014/9/18 19:21:13	x.y.1.12	93adfasga@ddddd.ne.jp	123456
2014/9/18 19:21:13	x.y.1.12	192slsoso@aaaaa.ne.jp	123456

〔不正アクセスの調査結果〕

3 日後，Y 社による，不正アクセスの詳細な調査が終了した。次は，A 主任が B 部長に調査結果を報告した際の会話である。

A 主任：Y 社の調査によると，パスワードを固定した上で，約 70 万個の文字列を次々に利用者 ID として入力し，ログインを試行するという攻撃があったとのことでした。試行された利用者 ID のうち，7 万個については，利用者 ID として実在していました。また，実際に 560 件の利用者 ID については，不正ログインまで成功しており，さらに，130 件については，ポイントが不正に交換されていました。

B 部長：ポイントが不正交換された会員への連絡は済んでいるのかね。

A 主任：はい，不正交換された会員を含め，不正ログインされた会員への個別連絡と，全会員への注意喚起は完了しています。

B 部長：分かった。経営陣には私から報告しておく。

A 主任：不正ログインされた会員に対して，パスワードリセットを実施したいのですが，よろしいでしょうか。

B 部長：Z サイトの再開までにはパスワードリセットも必須だが，それよりも，今回のような攻撃は今後も繰り返される可能性があるので，Y 社に依頼して，現在の Z サイトのアカウント管理の問題点を調査してもらってくれ。パスワードリセットと Z サイトの再開時期については，問題点の調査結果を見た上で考えることにする。

A 主任：分かりました。それでは再度 Y 社に調査を依頼します。

A 主任は，早速 Y 社に調査を依頼し，当日中に Y 社による調査が開始された。

〔問題点の調査結果と改善案〕

調査開始から 4 日後，Z サイトのアカウント管理における問題点の調査結果の報告が Y 社からあり，複数の問題点が存在することが分かった。Y 社が報告した Z サイトのアカウント管理の主要な問題点を図 1 に示す。

問題点(ア)　パスワード強度が不十分である
　パスワードに使用できる文字種が数字だけであり，かつ，パスワード長が短い。
問題点(イ)　パスワード保存方法が不適切
　パスワードをハッシュ化しただけで保存しているので，パスワードファイルが窃取された際に，パスワードを推測されるおそれがある。

図1　アカウント管理の主要な問題点

また，Y社は，これらの問題点についてそれぞれ図2の改善案を提示した。

改善案(ア)　パスワード強度の変更
・パスワードに使用できる文字種を，英大文字，英小文字，数字及び記号の80種とする。
・パスワードの最小文字数を8文字，最大文字数を64文字とする。
改善案(イ)　パスワード保存方法の変更
・①アカウントごとにソルトを設定し，ソルトとパスワードを結合したものをSHA-256ハッシュ関数でハッシュ化して保存する。

図2　改善案

A主任は，これらの改善案を実施するためのシステム改修の見積作業に取り掛かった。

〔暫定再開の検討〕

見積りの結果，ハッシュ値の保存に必要な領域が，1アカウント当たり16バイトから［　a　］バイトに変更されるのに加え，ソルトの保存領域の追加などの改修やディスクの増設が必要となり，再開まで3か月掛かることが分かった。A主任は，そのことをB部長に相談したところ，3か月間のZサイト閉鎖は，経営上の影響が非常に大きいので，何らかの対応を行った上で暫定再開する方法をY社と検討するよう指示を受けた。次はその時の，A主任とY社のC氏との会話である。

A主任：システム改修の3か月間，Zサイトを閉鎖することは，当社にとって影響が非常に大きいことから，何らかの対応を行った上で暫定再開させたいのですが，良い方法はないでしょうか。

C氏　：経営上の影響を考えると暫定再開はやむを得ないですね。図3のようなパスワードに対する攻撃（以下，パスワード攻撃という）を検知し対応する仕組みを導入し，攻撃を検知した場合は都度対応する運用とした上で，暫定再開

する方法はいかがでしょうか。ただし，暫定再開に当たっては，不正ログインされた会員のパスワードリセットを忘れずに実施してください。また，ポイントの交換については，システム改修が完了するまで停止した方が良いと思います。

方法(ア)
単位時間当たりのアカウントロックされた会員の数のしきい値を設定し，そのしきい値を超えた場合には，システム運用部に通知する。
方法(イ)
方法(ア)で検知されない場合に対処するために，[b] のしきい値を設定し，そのしきい値を超えた場合には，システム運用部に通知する。システム運用部は，当該 IP アドレスからの接続をファイアウォールのルール設定で遮断する。
方法(ウ)
方法(ア)でも方法(イ)でも検知されない場合に対処するために，単位時間当たりのログイン失敗数のしきい値を設定し，そのしきい値を超えた場合には，システム運用部に通知する。システム運用部は，Z サイトを緊急に閉鎖する必要があるかどうかを検討し，必要がある場合，経営陣の承認を経て閉鎖する。

図3　パスワード攻撃を検知し対応する方法

A 主任：分かりました。ところで，三つの方法は，それぞれどのようなパスワード攻撃を検知することができるのですか。

C 氏　：方法(ア)では，パスワード総当たり攻撃や辞書攻撃を検知します。方法(イ)では，今回の攻撃のように，同一 IP アドレスからのリバースブルートフォース攻撃を検知します。方法(ウ)では，[c] から行われるパスワード攻撃を検知します。ただし，どの方法も，攻撃を 100％検知できるというわけではありません。

A 主任：分かりました。それらの対応であれば1週間でできそうです。

A 主任は，暫定再開に向けた作業を行い，1週間後，Z サイトを暫定再開した。

〔本格再開の検討〕

A 主任は，本格再開に向けた作業を確認するために，再び C 氏に相談した。次はその時の A 主任と C 氏との会話である。

A 主任：パスワード攻撃の監視と対応を継続すれば，システム改修にもう少し時間を掛けてもよいのではないかと考えているのですが。

C 氏　：それは危険です。実は問題が幾つかあります。例えば，パスワード攻撃には，方法(ア)～(ウ)を組み合わせても検知できないものがあります。現行のパスワード強度と改善後のパスワード強度を比較評価するため，その攻撃が行われた場合に，どのくらいの時間で攻撃が成功するかを計算してみましょう。

C 氏は，方法(ア)～(ウ)を組み合わせても検知されずに行われるパスワード攻撃が成功するまでの所要時間を，図 4 のように説明した。

【前提条件】

(A)　会員によるログイン失敗が，1 日当たり 7,000 件あるとする。

(B)　方法(ウ)中の単位時間当たりのログイン失敗数のしきい値を(A)の 2 倍，つまり，1 日当たり 14,000 件とする。

(C)　攻撃方法の前提条件

(i) 何らかの方法で n 人分の利用者 ID（会員メールアドレス）のリストを取得済み
なお，n > 5,000 とする。

(ii) 方法(ア)で検知されないよう，利用者 ID ごとに 1 日 4 回を上限に攻撃

(iii) 方法(イ)で検知されないよう，[c] から攻撃

(iv) 方法(ウ)で検知されないよう，パスワード攻撃の試行回数の上限は，(A)と合わせても(B)より少ない 1 日当たり 5,000 件

【攻撃成功時間の計算】

(あ)　数字 6 桁のパスワードの場合，パスワードの全組合せは，[d] 通りである。上記の前提条件に沿って，試行の都度パスワードと利用者 ID を変えながらパスワードの全組合せを試行すると，少なくとも [e] 日掛かる。また，一つのパスワードで，取得済みの全ての利用者 ID に対して試行した後，別のパスワードで，取得済みの全ての利用者 ID に対して試行する。これをパスワードを変えながら繰り返すと，どれか一つの利用者 ID のログインに成功するために要する平均日数は，n によって異なるが，[e] 日の半分よりも大きく，[e] 日以下である。

(い)　文字種が 80 種で 8 桁のパスワードの場合，パスワードの全組合せは，[f] 通りである。全てのパスワードを試行するためには，3,355 億 4,432 万日掛かる。また，(あ)と同様に試行した場合，どれか一つの利用者 ID のログインに成功するために要する平均日数は，n によって異なり，3,355 億 4,432 万日の半分よりも大きく，3,355 億 4,432 万日以下である。

図 4　パスワード攻撃が成功するまでの所要時間の計算

A 主任：なるほど，暫定期間を延ばすと，検知を擦り抜けて不正ログインされる可能性が十分に現実的になるということですね。それでは，パスワード強度の変更とパスワード保存方法の変更が完了したことを条件として本格再開の時期

を設定します。他に気をつけることはありますか。

C 氏　：会員には②他のサイトで使っていないパスワードを設定してもらうよう注意喚起した方がいいですね。

A 主任：分かりました。

A 主任は，Z サイトの本格再開に向けたシステム改修計画をまとめ，B 部長とともに経営陣の承認を取り，3 か月後に本格再開を果たした。

設問 1　図 2 中の下線①は，ハッシュ値が保存されているファイルが漏えいした場合に，そのファイルに保存されたハッシュ値からパスワードが推測されることを防ぐための方法である。ソルトを用いることによって防ぐことができる攻撃方法を，60 字以内で具体的に述べよ。

設問 2　〔暫定再開の検討〕について，(1)～(3)に答えよ。

(1)　本文中の [a] に入れる適切な数値を答えよ。

(2)　図 3 中の [b] に入れる適切な字句を，30 字以内で述べよ。

(3)　本文中及び図 4 中の [c] に入れる適切な字句を，15 字以内で答えよ。

設問 3　図 4 中の [d] ～ [f] に入れる適切な数式又は実際の値を答えよ。

設問 4　本文中の下線②は，どのような攻撃による被害を避けるための注意喚起か。攻撃方法を 45 字以内で具体的に述べよ。