次の問1は必須問題です。必ず解答してください。

問1　ECサイトの利用者認証に関する次の記述を読んで，設問1～4に答えよ。

M社は，社員数が200名の輸入化粧品の販売会社である。このたび，M社では販路拡大の一環として，インターネット経由の通信販売（以下，インターネット通販という）を行うことを決めた。インターネット通販の開始に当たり，情報システム課のN課長を責任者として，インターネット通販用のWebサイト（以下，M社ECサイトという）を構築することになった。

M社ECサイトへの外部からの不正アクセスが行われると，インターネット通販事業で甚大な損害を被るおそれがある。そこで，N課長は，部下のC主任に，不正アクセスを防止するための対策について検討を指示した。

〔利用者認証の方式の調査〕

N課長の指示を受けたC主任は，最初に，利用者認証の方式について調査した。

利用者認証の方式には，次の3種類がある。

（i）利用者の記憶，知識を基にしたもの

（ii）利用者の所有物を基にしたもの

（iii）利用者の生体の特徴を基にしたもの

（ii）には，［　a　］による認証があり，（iii）には，［　b　］による認証がある。（ii），（iii）の方式は，セキュリティ面の安全性が高いが，①多数の会員獲得を目指すM社ECサイトの利用者認証には適さないとC主任は考えた。他社のECサイトを調査したところ，ほとんど（i）の方式が採用されていることが分かった。そこで，M社ECサイトでは，（i）の方式の一つであるID，パスワードによる認証を行うことにし，ID，パスワード認証のリスクに関する調査結果を基に，対応策を検討することにした。

〔ID，パスワード認証のリスクの調査〕

ID，パスワード認証のリスクについて調査したところ，幾つかの攻撃手法が報告されていた。パスワードに対する主な攻撃を表1に示す。

表1　パスワードに対する主な攻撃

項番	攻撃名	説明
1	c 攻撃	ID を固定して，パスワードに可能性のある全ての文字を組み合わせてログインを試行する攻撃
2	逆 c 攻撃	パスワードを固定して，ID に可能性のある全ての文字を組み合わせてログインを試行する攻撃
3	類推攻撃	利用者の個人情報などからパスワードを類推してログインを試行する攻撃
4	辞書攻撃	辞書や人名録などに載っている単語や，それらを組み合わせた文字列などでログインを試行する攻撃
5	d 攻撃	セキュリティ強度の低い Web サイト又は EC サイトから，ID とパスワードが記録されたファイルを窃取して，解読した ID，パスワードのリストを作成し，リストを用いて，ほかのサイトへのログインを試行する攻撃

表 1 中の項番 1～4 の攻撃に対しては，パスワードとして設定する文字列を工夫することが重要である。項番 5 の攻撃に対しては，M 社 EC サイトでの認証情報の管理方法の工夫が必要である。しかし，他組織の Web サイトや EC サイト（以下，他サイトという）から流出した認証情報が悪用された場合は，M 社 EC サイトでは対処できない。そこで，C 主任は，M 社 EC サイトでのパスワード設定規則，パスワード管理策及び会員に求めるパスワードの設定方法の 3 点について，検討を進めることにした。

〔パスワード設定規則とパスワード管理策〕

最初に，C 主任は，表 1 中の項番 1，2 の攻撃への対策について検討した。検討の結果，パスワードの安全性を高めるために，M 社 EC サイトに，次のパスワード設定規則を導入することにした。

・パスワード長の範囲を 10～20 桁とする。
・パスワードについては，英大文字，英小文字，数字及び記号の 70 種類を使用可能とし，英大文字，英小文字，数字及び記号を必ず含める。

次に，C 主任は，M 社 EC サイトの ID，パスワードが窃取・解析され，表 1 中の項番 5 の攻撃で他サイトが攻撃されるのを防ぐために，M 社 EC サイトで実施するパスワードの管理方法について検討した。

一般に，Web サイトでは，②パスワードをハッシュ関数によってハッシュ値に変換（以下，ハッシュ化という）し，平文のパスワードの代わりにハッシュ値を秘密認証情報のデータベースに登録している。しかし，データベースに登録された認証情報が流出すると，レインボー攻撃と呼ばれる次の方法によって，ハッシュ値からパスワードが割り出されるおそれがある。

・攻撃者が，膨大な数のパスワード候補とそのハッシュ値の対応テーブル（以下，R テーブルという）をあらかじめ作成するか，又は作成された R テーブルを入手する。
・窃取したアカウント情報中のパスワードのハッシュ値をキーとして，R テーブルを検索する。一致したハッシュ値があればパスワードが割り出される。

レインボー攻撃はオフラインで行われ，時間や検索回数の制約がないので，パスワードが割り出される可能性が高い。そこで，C 主任は，レインボー攻撃によるパスワードの割出しをしにくくするために，③次の処理を実装することにした。

・会員が設定したパスワードのバイト列に，ソルトと呼ばれる，会員ごとに異なる十分な長さのバイト列を結合する。
・ソルトを結合した全体のバイト列をハッシュ化する。
・ID，ハッシュ値及びソルトを，秘密認証情報のデータベースに登録する。

〔会員に求めるパスワードの設定方法〕

次に，C 主任は，表 1 中の項番 3，4 及び 5 の攻撃への対策を検討し，次のルールに従うことを M 社 EC サイトの会員に求めることにした。

・会員自身の個人情報を基にしたパスワードを設定しないこと
・辞書や人名録に載っている単語を基にしたパスワードを設定しないこと
・④会員が利用する他サイトと M 社 EC サイトでは，同一のパスワードを使い回さないこと

C 主任は，これらの検討結果を N 課長に報告した。報告内容と対応策は N 課長に承認され，実施されることになった。

設問1　〔利用者認証の方式の調査〕について，(1)，(2)に答えよ。

(1) 本文中の［　a　］，［　b　］に入れる適切な字句を解答群の中から選び，記号で答えよ。

解答群

ア　虹彩　　イ　体温　　ウ　ディジタル証明書

エ　動脈　　オ　パスフレーズ　　カ　パソコンの製造番号

(2) 本文中の下線①について，（ii）又は（iii）の方式の適用が難しいと考えられる適切な理由を解答群の中から選び，記号で答えよ。

解答群

ア　インターネット経由では，利用者認証が行えないから

イ　スマートデバイスを利用した利用者認証が行えないから

ウ　利用者に認証デバイス又は認証情報を配付する必要があるから

エ　利用者のIPアドレスが変わると，利用者認証が行えなくなるから

設問2　〔ID，パスワード認証のリスクの調査〕について，(1)，(2)に答えよ。

(1) 表1中の［　c　］，［　d　］に入れる適切な字句を答えよ。

(2) 表1中の項番1の攻撃には有効であるが，項番2の攻撃には効果が期待できない対策を，“パスワード”という字句を用いて，20字以内で答えよ。

設問3　〔パスワード設定規則とパスワード管理策〕について，(1)，(2)に答えよ。

(1) 本文中の下線②について，ハッシュ化する理由を，ハッシュ化の特性を踏まえ25字以内で述べよ。

(2) 本文中の下線③の処理によって，パスワードの割出しがしにくくなる最も適切な理由を解答群の中から選び，記号で答えよ。

解答群

ア　Rテーブルの作成が難しくなるから

イ　アカウント情報が窃取されてもソルトの値が不明だから

ウ　高機能なハッシュ関数が利用できるようになるから

エ　ソルトの桁数に合わせてハッシュ値の桁数が大きくなるから

設問4　本文中の下線④について，パスワードの使い回しによってM社ECサイトで発生するリスクを，35字以内で述べよ。