応用情報技術者

午後対策問題集

無料体験入学者用

TAC

はじめに

この問題集は,弊社刊「応用情報技術者試験対策テキストⅠ・Ⅱ・Ⅲ」の各学習項目に対応させて作成された問題集です。応用情報技術者試験の午後試験出題範囲である各分野(テクノロジ系，マネジメント系,ストラテジ系)の問題を，広く多数掲載しています。

本書は，過去の情報処理技術者試験において出題された午後問題で構成されています。実際の応用情報技術者試験の出題形式に合わせ,テーマごとに問題を集めて掲載しています(出典は目次の後)。

試験に合格するためには，テキストによる知識のインプットだけではなく,問題演習によるアウトプット(力試し)が非常に重要になります。問題を解き，間違えた問題のジャンルについては学習しなおして再度挑戦するという学習サイクルを身に付けましょう。

本書が，応用情報技術者試験の合格のお役に立てることを願ってやみません。

TAC情報処理講座

目　次

出典一覧

第1章　プログラミング

問1	平成29年秋期本試験　問3
問2	令和元年秋期本試験　問3
問3	平成26年秋期本試験　問3
問4	平成30年春期本試験　問3

第2章　システムアーキテクチャ

問1	平成26年春期本試験　問4
問2	平成27年春期本試験　問4
問3	平成25年秋期本試験　問3
問4	平成31年春期本試験　問4

第3章　データベース

問1	平成30年春期本試験　問6
問2	平成31年春期本試験　問6
問3	平成28年春期本試験　問6
問4	平成29年春期本試験　問6

第4章　ネットワーク

問1	平成30年春期本試験　問5
問2	平成25年秋期本試験　問4
問3	平成25年春期本試験　問5
問4	平成31年春期本試験　問5

第5章　情報セキュリティ

問1	平成29年秋期本試験　問1
問2	平成31年春期本試験　問1
問3	令和元年秋期本試験　問1
問4	平成25年春期本試験　問9
問5	平成25年秋期本試験　問8
問6	平成26年春期本試験　問1
問7	平成28年秋期本試験　問1
問8	令和2年本試験　問1

第6章　情報システム開発

問1	平成28年春期本試験　問8
問2	平成29年春期本試験　問8
問3	平成31年春期本試験　問8
問4	平成30年秋期本試験　問8

第7章　組込みシステム開発

問1	平成30年秋期本試験　問7
問2	平成31年春期本試験　問7
問3	令和元年秋期本試験　問7
問4	平成29年春期本試験　問7

第8章　プロジェクトマネジメント

問1	平成30年春期本試験　問9
問2	令和元年秋期本試験　問9
問3	平成28年春期本試験　問9
問4	平成29年秋期本試験　問9

第9章　サービスマネジメント

問1	平成29年春期本試験　問10
問2	平成26年秋期本試験　問10
問3	平成31年春期本試験　問10
問4	平成28年秋期本試験　問10

第10章　システム監査

問1	平成28年春期本試験　問11
問2	平成31年春期本試験　問11
問3	平成25年秋期本試験　問11
問4	平成29年春期本試験　問11

第11章　経営戦略と情報戦略

問1	平成28年秋期本試験　問2
問2	平成29年春期本試験　問2
問3	平成30年春期本試験　問2
問4	平成25年春期本試験　問1

第５章　情報セキュリティ

問1　個人情報保護の強化に関する次の記述を読んで，設問1，2に答えよ。

C 社は，服飾・雑貨のインターネット販売業者である。約 50,000 人の顧客が同社の会員制 Web サイトを利用している。会員制 Web サイトには HTTPS を使用してアクセスする必要がある。

顧客が会員制 Web サイトにログインするには会員番号が必要であり，会員登録時に，重複しない6桁の数字列をランダムに割り振っている。

C 社には，商品販売部門の他に，服飾類を扱う X 部門，生活雑貨を扱う Y 部門，そして輸入雑貨を扱う Z 部門の三つの商品開発部門がある。

〔C 社の現状〕

C 社の会員制 Web サイトは DMZ 内に設置してあり，セキュリティ専門会社に委託してインターネットからの不正アクセスの検知と対応を行っている。

C 社のネットワーク構成（抜粋）を図1に示す。

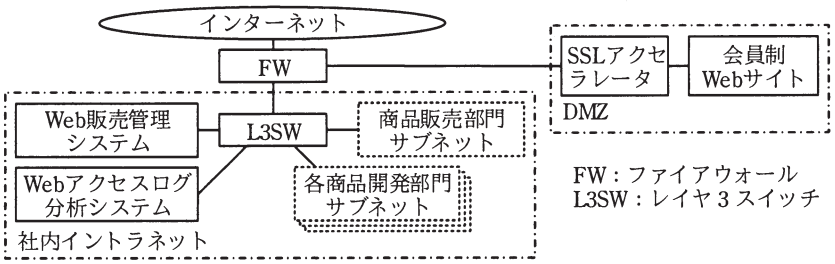

図1　C 社のネットワーク構成（抜粋）

C 社の会員制 Web サイトで扱う顧客情報や販売情報は，社内イントラネット内の Web 販売管理システムに蓄積されている。Web 販売管理システムの顧客情報データベースには，顧客の会員番号をキーとして，氏名，メールアドレス，電話番号，性別，年齢，住所などが格納されている。また，Web 販売管理システムの販売情報データベースには，顧客の会員番号をキーとして，該当顧客の販売情報が格納されている。二つのデータベースは磁気テープを用いて，月次でフルバックアップを行い，日次で増分バックアップを行っている。C 社の方針で過去1年間のバックアップデータを保管している。

C 社では，会員制 Web サイトの Web アプリケーションが出力する会員閲覧ログ（以下，Web サイト閲覧履歴という）を，毎日，社内イントラネット内の Web アクセスログ分析システムに転送して，その中に含まれる顧客の会員番号を基に，顧客ごとの閲覧履歴を分析している。

各商品開発部門は，Web サイト閲覧履歴や販売情報を参考にして，定期的に商品の品ぞろえを見直している。各商品開発部門では，有資格者だけが Web 販売管理システムにログインして，販売情報を PC で閲覧したり，CSV 形式のファイルで PC に出力したりすることができる。全顧客の Web サイト閲覧履歴も，有資格者だけが Web アクセスログ分析システムにログインして PC で閲覧したり，CSV 形式のファイルで PC に出力したりすることができる。有資格者が出力した Web サイト閲覧履歴や販売情報の CSV 形式のファイルは，分析完了後に PC から削除することになっている。

各商品開発部門の有資格者は有資格者リストで管理している。各商品開発部門からの申請に基づいて，システム部門が有資格者リストを更新するとともに，Web 販売管理システムや Web アクセスログ分析システムへのアクセス権限を設定する。

顧客情報データベースは，各商品開発部門には公開していない。各商品開発部門の有資格者が Web サイト閲覧履歴と販売情報を関連付け，閲覧した商品と売れ筋商品を分析する。その際，性別や地域，年齢などを必要とする場合，システム部門は，顧客情報から必要がない個人情報の箇所をマスクしたデータ（以下，加工個人情報という）を提供している。加工個人情報は，CSV 形式のファイルを暗号化して，電子メール（以下，メールという）に添付して有資格者に送付している。暗号化したファイルを復号するためのパスワードは別メールで送付することになっている。

〔個人情報保護の強化〕

システム部門の F 部長は，Web 販売管理システムのデータベースにある情報や，PC に保存されている Web サイト閲覧履歴や販売情報，加工個人情報について，社内からの不正アクセスや従業員の人的ミスによる漏えいのリスクが高いと考えた。会員番号を含めた個人情報が漏えいするおそれをできるだけ減らすためには，個人情報を含むデータの秘匿性を高める必要があると考え，社内で対策を協議した。

その結果，個人情報保護を強化するために，次の(1)～(4)の対策を実施することと

し，具体的な実現方法をシステム部門のD課長が検討することになった。

(1) Web販売管理システムへのアクセスはHTTPSによるものに限定する。

(2) 顧客情報データベースと販売情報データベースは，暗号化鍵を用いて暗号化する。バックアップデータからの情報漏えいを防ぐために，暗号化されたデータのままバックアップを行う。

(3) Web サイト閲覧履歴は，その中に含まれる会員番号を，元に戻せない仮の ID（以下，仮 ID という）に変換してから，Web アクセスログ分析システムに転送する。

(4) 各商品開発部門の有資格者が Web 販売管理システムにログインした場合は，［ a ］情報に含まれる会員番号を同じ方法で仮 ID に変換して提供する。

D課長は検討した結果をF部長に報告した。

D課長：データベースの暗号化アルゴリズムには，共通鍵暗号方式の［ b ］を採用しようと考えています。暗号化鍵は四半期に 1 回変更します。新しい暗号化鍵でのデータベースの再暗号化が完了次第，古い暗号化鍵は削除する予定です。

F部長：①古い暗号化鍵を削除する運用だと問題があります。過去の暗号化鍵も含めて鍵を管理するように検討し直してください。

D課長：分かりました。それから，仮 ID に変換する際には，変換後の ID が衝突しないように，会員番号に［ c ］を適用した結果を採用しようと考えています。

F部長：仮 ID から直接元の会員番号に戻すことはできませんが，万一，採用した［ c ］が知られてしまった場合には，②間接的に仮 ID から元の会員番号を特定できてしまいます。これを防ぐために，公開しない文字列と会員番号を文字列連結した結果に対して，［ c ］による変換を行ってください。

〔加工個人情報の提供方法の改善〕

加工個人情報をメールに添付して送付する方法には，次のリスクが存在することが

分かった。

・パスワードを別メールで送付する運用だと，［　d　］に対して効果がない。

・間違って別のファイルや暗号化していないファイルを添付してメールを送付するおそれがある。

・間違って［　　e　　］にメールを送付するおそれがある。

D課長は，メールで送付する現状の受渡し方法ではリスクが高いと考え，加工個人情報をWeb販売管理システムに格納して，有資格者だけがアクセスできるように変更することにした。

設問1　〔個人情報保護の強化〕について，(1)～(4)に答えよ。

(1)　本文中の［　a　］に入れる適切な字句を4字以内で答えよ。

(2)　本文中の［　b　］，［　c　］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。

bに関する解答群

ア　AES　　イ　MAC　　ウ　RSA　　エ　SHA

cに関する解答群

ア　共通鍵暗号方式　　イ　公開鍵暗号方式

ウ　ディジタル署名　　エ　ハッシュ関数

(3)　本文中の下線①について，どのような問題があるか。40字以内で述べよ。

(4)　本文中の下線②について，仮IDから元の会員番号をどのようにして特定することが可能か。35字以内で述べよ。

設問2　〔加工個人情報の提供方法の改善〕について，(1)，(2)に答えよ。

(1)　本文中の［　d　］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　DoS攻撃　　イ　盗聴

ウ　パスワードリスト攻撃　　エ　ブルートフォース攻撃

(2)　本文中の［　e　］に入れる適切な字句を10字以内で述べよ。

問2　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。

第５章　情報セキュリティ　解答・解説

問1

解答

解答例

設問		解答例				備考
設問1	(1)	a	販売			
	(2)	b	ア	c	エ	
	(3)	削除された暗号化鍵で暗号化されたバックアップデータを復元できない。				
	(4)	会員番号となり得る全数字列を同じハッシュ関数で変換して突き合わせる。				
設問2	(1)	d	イ			
	(2)	e	意図しない宛先			

解説

設問1

(1)

aについて

空欄aの前で「各商品開発部門の有資格者がWeb販売管理システムにログインした場合」と述べられているので，まずはWeb販売管理システムへのログインに関する記述を本文から探す。〔C社の現状〕では，「各商品開発部門では，有資格者だけがWeb販売管理システムにログインして，販売情報をPCで閲覧したり，CSV形式のファイルでPCに出力したりする」と述べられており，Web販売管理システムにログインするのは販売情報を閲覧・出力するためであると判断できる。

また，〔C社の現状〕では，販売情報はWeb販売管理システムの販売情報データベースに格納されており，顧客の会員番号をキーとしていることが述べられている。ここから，販売情報に含まれる会員番号を仮IDに変換して提供すれば，個人情報の漏えいするおそれを減らすことができる。以上より，空欄aには，

販売

を入れればよい。

(2)

bについて

共通鍵暗号方式の規格には，AES，Camellia，DESなどがある。これらのうち，選択肢にあるのはAES（ア）のみである。

MAC（Message Authentication Code，メッセージ認証符号）：メッセージ（データ）の完全性を確認するためのデータ。共通鍵を利用して生成する

RSA：素因数分解の複雑さを利用した公開鍵暗号方式の一種

SHA（Secure Hash Algorithm）：ハッシュ関数の一種であり，SHA1やSHA2など，複数の種類がある

cについて

空欄cの前で「仮IDに変換する際には，変換後のIDが衝突しないように」と述べられており，〔個人情報保護の強化〕(3)では，「会員番号を，元に戻せない仮のID（以下，仮IDという）に変換して」と述べられている。ここから，空欄cには

・出力値（仮ID）から入力値（会員番号）が得られない

・衝突（異なる入力値から同じ出力値が得られる現象）が発生しない

という二つの特徴をもつものが入る。選択肢のうち，このような特徴をもつものは，ハッシュ関数（エ）だけである。ハッシュ関数は，

・入力値のサイズによらず，一定サイズの出力値を計算する

・出力値から入力値を求めることが困難である（一方向性）

・異なる入力値から同じ出力値が計算されない（衝突困難性）

といった性質をもつ。

(3)

下線①を含むF部長の発言の前で，データベースの暗号化アルゴリズムには，共通鍵暗号方式のAES（空欄b）を採用するとD課長が発言している。共通鍵暗号方式は，暗号化に用いる暗号化鍵と復号に用いる復号鍵が同一のため，暗号化鍵を削除するということは，暗号化されたデータを復号できなくなることを意味する。

また，D課長の発言では，データベースの暗号化に言及している。これに関する記述を探すと，〔個人情報保護の強化〕(2)で顧客情報データベースと販売情報データベースは暗号化鍵を用いて暗号化すること，及び暗号化されたデータもバックアップを行うことが述べられている。D課長の発言によれば，古い暗号化鍵を削除するのは新しい暗号化鍵での再暗号化が完了した後なので，古い暗号化鍵を削除してもデータベースそのものが復号できなくなることはない。よって，問題があるのはバックアップしたデータを復号する場合であると判断できる。

バックアップに関する記述を探すと，〔C社の現状〕では「C社の方針で過去1年間のバックアップデータを保管している」と述べられている。これに対し，D課長は，「暗号化鍵は四半期に1回変更する」と発言している。よって，古い暗号化鍵を削除して最新の鍵だけを残すような運用をすると，最大でも四半期前のバックアップデータしか復号することができず，1年前のバックアップデータは復号できなくなる。これを防ぐためには，F部長が発言しているように過去の暗号化鍵も含めて管理する必要がある。以上より，古い暗号化鍵を削除する運用だと起こりうる問題とは，

削除された暗号化鍵で暗号化されたバックアップデータを復元できない。

である。

(4)

下線②の後で，この問題の対策として「公開しない文字列と会員番号を文字列連結した結果に対して，ハッシュ関数による変換」を行えばよいことが述べられている。会員番号は6桁の数字列であるので，000000 ～ 999999 までの100万通りしかないが，公開しない文字列を連結することによって入力データの種類は大幅に増加し，推測が困難になる。すなわち，この問題は入力データが推測できることによって生じると判断できる。

ハッシュ関数は，入力データが等しければ出力されるハッシュ値も必ず等しく，入力データが異なれば出力されるハッシュ値も異なる。このため，100万通りの会員番号と会員から求めたハッシュ値（生成される仮ID）の組をあらかじめ用意し，それを目的の仮IDと照合することによって，元の会員番号を特定することが可能となる。

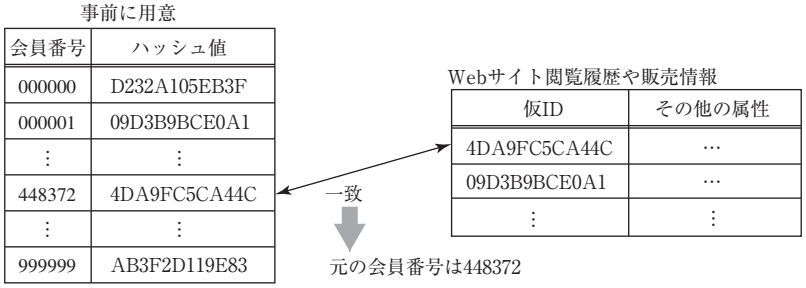

図2　元の会員番号の特定

設問2

(1)

dについて

空欄dの後に「効果がない」と述べられている。暗号化の効果がないということは，暗号化したファイルが容易に復号できてしまうと考えられる。そこで，暗号化したファイルとパスワードの両方が入手される可能性について考える。「パスワードを別メールで送付する」ということは，暗号化した加工個人情報と，それを復号するためのパスワードの両方がメールで送付されることになる。これらを不正に入手するためには，通信経路の途中で通信内容を，

盗聴

すればよい。

DoS攻撃：サーバに不要な負荷をかけて，本来提供するべきサービスの提供を妨害する攻撃
パスワードリスト攻撃：他のサイトで流出したユーザIDとパスワードをそのまま利用してログインを試みる攻撃
ブルートフォース攻撃：パスワードを総当たりで調べる攻撃

(2)

eについて

「間違って［ e ］にメールを送付」ということは，メールの送付先が問われていると判断できる。問題文の末尾で述べられている対策で，「有資格者だけがアクセスできるようにした」と述べられているように，加工個人情報を含むメールやパスワードを記載したメールは有資格者のみに送付すべきものである。これが間違いによって送付されるのであるから，有資格者ではない社員や外部の人間といった，本来送付すべきではない宛先にメールを送付する可能性が考えられる。これを10字以内で答えればよい。

問2

解答

設問		解答例				備考
設問1	(1)	a	ウ	b	ア	
	(2)	ウ				
設問2	(1)	c	総当たり　　又は　　ブルートフォース			
		d	パスワードリスト			
	(2)	パスワード入力試行回数の上限値の設定				
設問3	(1)	ハッシュ値からパスワードの割出しは難しいから				
	(2)	ア				
設問4		他サイトから流出したパスワードによって，不正ログインされる。				

解説

設問1

aについて

(ⅱ)の所有物を基にした認証ではICカードやセキュリティトークンなどが利用されるが，このような“物”に該当するような選択肢はない。そこで，所有物の中に格納される情報に注目する。所有物によって利用者を認証するということは，所有物の中には利用者ごとに固有であり，かつ偽造が困難な情報が格納されているはずである。このような特性をもつ情報の一つとして，ディジタル証明書が挙げられる。

ディジタル証明書に含まれる公開鍵にはペアとなる秘密鍵が存在し，その秘密鍵はディジタル証明書の所有者本人しかもたないことが前提となる。このため，秘密鍵をもつことが証明できれば，ディジタル証明書の正当な所有者であることを証明できる。鍵ペア（ディジタル証明書と秘密鍵）を格納したICカードを利用して，利用者を認証する例を図1に示す。

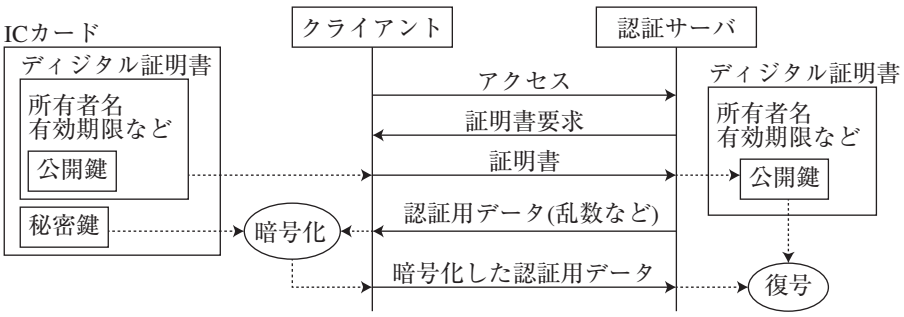

図1　ICカードを利用した認証の流れ

この例では，利用者がICカード中に格納された秘密鍵で認証用データを暗号化し，認証するサーバが暗号化された認証用データをディジタル証明書に含まれる公開鍵で復号する。両者が一致すれば，利用者は鍵ペアが格納されたICカードを所有しており，正当な利用者であるとみなすことができる。

bについて

(ⅲ)の生体の特徴を基にした認証方式(生体認証)では，指紋，虹彩，手のひらの静脈などのパターンが広く利用されている。これらのうち，選択肢にあるものは虹彩のみである。なお，動脈は静脈よりも体の内側に位置するために読み取りにくいなどの理由により，生体認証には用いられないことが一般的である。

(2)

下線①では「多数の会員獲得を目指す」と述べられているので，利用者が増えるとどのような弊害が生じるのかを考える。

(ⅱ)によって利用者認証を行うためには，ディジタル証明書などを格納したICカードやセキュリティトークンを，全会員に配布しなければならない。この場合，M社にとって手間やコストが生じるだけでなく，利用者にとっても利用できるまでに時間がかかったり，登録作業や操作が煩雑になったりするため，利便性は低下する。この結果，インターネット通販で顧客が獲得できない結果が予想される。

同様に，(ⅲ)によって利用者認証を行うためには，虹彩センサなどの生体情報を読み取るための認証デバイスが必要になる。この場合も，多数の会員獲得を目指すことを考えると，認証デバイスを配布するための手間やコストの増加，利用者の利便性の低下を引き起こす。以上より，(ⅱ)，(ⅲ)の方式の適用が難しいと考えられる理由はウの「利用者に認証デバイス又は認証情報を配布する必要があるから」と判断できる。

設問2

(1)

cについて

項番1の説明にあるような「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」ような攻撃を総当たり攻撃又はブルートフォース攻撃という。

dについて

項番5の説明では，セキュリティ強度が低いサイトからIDとパスワードを窃取してリスト化し，そのIDとパスワードの組合せをほかのサイトでそのまま利用する旨が述べられている。このようなリスト化したIDとパスワードによって行う攻撃をパスワードリスト攻撃という。

近年，様々なWebサイトで会員登録を求められるが，その際に，ユーザIDは利用者のメールアドレスとすることが多い。この結果，利用者IDが様々なサイトで共通となっている。一方，利用者もパスワードを忘れないようにするために，各サイトで同じパスワードを設定していることが多い。すると，同じID，パスワードで様々なサイトにアクセス可能となる。パスワードリスト攻撃は，こういった背景を巧みに利用している。

(2)

ここでは，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が問われているので，まずはブルートフォース攻撃に対する対策を考える。ブルートフォース攻撃は，特定のIDに対して全ての文字の組み合わせをパスワードとして試行する攻撃である。この攻撃では，攻撃が成功するまで一つのIDに対して認証の失敗が連続するので，パスワードの入力試行回数に上限値を設定し，これを超えた場合はそのIDを一時的に無効とする対策が有効となる。これをアカウント(ID)のロックアウトという。

一方，項番2の逆ブルートフォース攻撃(リバースブルートフォース攻撃)は，パスワードをよく利用されているもの（password，123456，qwertyなど）に固定して，IDを変化させる攻撃である。この場合，1回だけ認証に失敗したIDが多数発生することになるので，特定のIDに対してパスワードの入力試行回数に上限値を設定する対策は有効に機能しない。よって，

パスワード入力試行回数の上限値の設定

などのように答えればよい。

設問3

(1)

設問で「ハッシュ関数の特性を踏まえ」て答えるよう要求されているので，まずはハッシュ関数の特性について整理する。情報セキュリティの分野で利用されるハッシュ関数には，次のような特性がある。

表2　ハッシュ関数の主な特性

衝突困難性	衝突（異なる入力値から同じ出力値が得られる現象）が発生する確率が極めて低い。
一方向性	出力値（ハッシュ値）から入力値を逆算することが困難である。

下線②ではパスワードをハッシュ値に変換する旨が述べられているので，入力値はパスワードである。一方向性を考慮すると，パスワードファイルを不正に入手しても記録されたハッシュ値から元のパスワードを逆算することができないので，パスワードリスト攻撃を防げることになる。以上を制限字数内にまとめ，

ハッシュ値からパスワードの割出しは難しいから

などのように表現すればよい。

(2)

下線③の前では，「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」と述べられているので，まずはレインボー攻撃の概要を問題文から確認する。すると，その前の文章で攻撃者がパスワード候補とハッシュ値の対応関係を記録したRテーブルを用意し，Rテーブルから攻撃対象となるパスワードのハッシュ値を探すことがわかる。このパスワード候補とハッシュ値の対応関係を表3に示す。表3からもわかるように，Rテーブルに攻撃対象のハッシュ値と同じものがあれば，それに対応するパスワードは容易に得られることになる。

表3　パスワード候補とハッシュ値の対応関係

パスワード候補	対応するハッシュ値
password	5f4dcc3b5aa765d61d8327deb882cf99
admin	21232f297a57a5a743894a0e4a801fc3
12345	827ccb0eea8a706c4c34a16891f84e7b
⋮	⋮

注記：この対応関係は膨大な量になるため，実際のレインボー攻撃では“チェーン”とよばれる概念で複数の対応関係を関連づけて管理することによってテーブルの大きさを削減している。

続いて下線③の処理を確認する。下線③の直後の文章を読むと，パスワードにソルトとよばれるバイト列(文字列)を連結してハッシュ値を求めること，ソルトとなる文字列は会員ごとに異なることがわかる。ソルトが会員ごとに異なるということは，仮に同じパスワードを設定していても登録されるハッシュは会員ごとに異なる結果となる。

表4　パスワード候補とソルト及びハッシュ値の対応関係

ID	ソルト	パスワード	ハッシュ値
user1	AX	admin	8a0e92eca8efdf3687aafee975b34241
user2	fU	admin	e993504cc80b05d891abdf37ab87b1b8
user3	MZ	admin	1284c6b98f2d749b54156845f693ce7f

このため，認証を行う場合は入力されたパスワードに登録されているソルトを連結した結果をハッシュ関数に入力するだけでよいが，攻撃者はソルトごとにRテーブルを用意する必要が生じてしまう。よって，アの「Rテーブルの作成が難しくなるから」を選べばよい。

イ　ソルトは秘密認証情報のデータベースに登録されているので，アカウント情報が窃取されればソルトの値は判明する。

ウ　ソルトの使用に関わらず，利用するハッシュ関数は同じである。

エ　ハッシュ関数は，いかなる入力値であっても固定長(256ビットなど)のハッシュ値を出力する。

設問4

表1項番5の説明文に注目して考えればよい。表1項番5では，パスワードリスト攻撃について説明している。パスワードリスト攻撃は，他のサイトから流出したID，パスワードをそのまま利用して不正にアクセス攻撃である。ここでは「M社ECサイトで発生するリスク」が問われているので，M社ECサイトが不正アクセスされることを考えればよい。すなわち，会員が利用する他のサイトとM社のECサイトで同一のパスワードを利用していた場合，他のサイトからIDとパスワードの組合せが流出した際に，

他サイトから流出したパスワードによって，不正ログインされる。

というリスクが考えられる。