1-1 利用者認証

問 1-1-1

次の各設問に答えよ。

設問１　認証技術を，所有物による認証，身体的特徴による認証及び知識による認証の三つに分類したとき，分類と実現例①～③の適切な組合せはどれか。

① ICカードを用いた認証
② ID，パスワードによる認証
③ 指紋による認証

	①	②	③
ア	所有物による認証	身体的特徴による認証	知識による認証
イ	所有物による認証	知識による認証	身体的特徴による認証
ウ	知識による認証	所有物による認証	身体的特徴による認証
エ	知識による認証	身体的特徴による認証	所有物による認証

設問２　アクセス制御に用いる認証デバイスの特徴に関する記述のうち，適切なものはどれか。

ア　USBメモリにディジタル証明書を組み込み，認証デバイスとする場合は，利用するPCのMACアドレスを組み込む必要がある。
イ　成人には虹彩(こう)の経年変化がなく，虹彩認証では，認証デバイスでのパターン更新がほとんど不要である。
ウ　静電容量方式の指紋認証デバイスでは，LED照明を設置した室内において正常に認証できなくなる可能性がある。
エ　認証に利用する接触型ICカードは，カード内のコイルの誘導起電力を利用している。

設問３　リバースブルートフォース攻撃に該当するものはどれか。

ア　攻撃者が何らかの方法で事前に入手した利用者IDとパスワードの組みのリストを使用して，ログインを試行する。
イ　パスワードを一つ選び，利用者IDとして次々に文字列を用意して総当たりにログインを試行する。
ウ　利用者ID，及びその利用者IDと同一の文字列であるパスワードの組みを次々に生成してログインを試行する。
エ　利用者IDを一つ選び，パスワードとして次々に文字列を用意して総当たりにログインを試行する。

設問４　Webサーバの認証において，同じ利用者IDに対してパスワードの誤りがあらかじめ定められた回数連続して発生した場合に，その利用者IDを自動的に一定期間利用停止にするセキュリティ対策を行った。この対策によって，最も防御の効果が期待できる攻撃はどれか。

ア　ゼロデイ攻撃　　イ　パスワードリスト攻撃
ウ　バッファオーバフロー攻撃　　エ　ブルートフォース攻撃

設問５　パスワードクラック手法の一種であるレインボー攻撃に該当するものはどれか。

ア　何らかの方法で事前に利用者IDと平文のパスワードのリストを入手しておき，複数のシステム間で使い回されている利用者IDとパスワードの組みを狙って，ログインを試行する。
イ　パスワードに成り得る文字列の全てを用いて，総当たりでログインを試行する。
ウ　平文のパスワードとハッシュ値をチェーンによって管理するテーブルを準備しておき，それを用いて，不正に入手したハッシュ値からパスワードを解読する。
エ　利用者の誕生日や電話番号などの個人情報を言葉巧みに聞き出して，パスワードを類推する。

設問６　入力パスワードと登録パスワードを用いて利用者を認証する方法において，パスワードファイルへの不正アクセスによる登録パスワードの盗用防止策はどれか。

ア　パスワードに対応する利用者IDのハッシュ値を登録しておき，認証時に入力された利用者IDをハッシュ関数で変換して参照した登録パスワードと入力パスワードを比較する。
イ　パスワードをそのまま登録したファイルを圧縮しておき，認証時に復元して，入力されたパスワードと比較する。
ウ　パスワードをそのまま登録しておき，認証時に入力されたパスワードと登録内容をともにハッシュ関数で変換して比較する。
エ　パスワードをハッシュ値に変換して登録しておき，認証時に入力されたパスワードをハッシュ関数で変換して比較する。

設問７　パスワード管理に関する記述のうち，適切なものはどれか。

ア　業務システムで使用しているパスワードを，私的なインターネットサービスの利用では使用しない。
イ　初期パスワードは，システムのログイン操作に慣れるまで変更しない。
ウ　数個のパスワードを用意しておき，それを使い回す。
エ　パスワードは，平文のファイルに格納してPCへ保存しておく。

問 1-1-2

生体認証システムの導入に関する次の記述を読んで，設問１～３に答えよ。

Ｓ社は，個人投資家を対象とした，従業員約200人の証券会社である。事務所では従業員に一人１台のPCが割り当てられている。社内ではディジタル証明書による認証は利用しておらず，全ての業務システムは従業員ID（以下，IDという）とパスワードでログインできるようになっている。Ｓ社では，システム管理者がIDを一括管理できるようにするために，ID管理システムを導入している。 ID管理システムは，氏名などの個人情報とIDを関連付けており，認証サーバとしての役割も兼ねている。

業務システムには，出張手配や勤怠管理を行う総務システム，顧客との取引情報を管理する顧客管理システムなどがある。個別の顧客との取引情報は，その顧客を担当している従業員と直属の上司だけが閲覧することを許されている。

〔セキュリティインシデントの発生〕

ある従業員が担当している顧客の取引情報を，別の従業員が不正に入手して利用するというセキュリティインシデントが発生した。調査の結果，IDとパスワードの不適切な管理によって，IDとパスワードを不正利用されてしまったことが分かった。この事態を重く見たＳ社は，業務システムへの不正アクセスを防ぐために，セキュリティの強化を図ることにした。

〔不正アクセス予防策の実施〕

Ｓ社では，IDとパスワードのクラッキングや業務システムへの不正アクセスの対策として，予想される不正アクセスに対応する予防策を実施した。予防策は，実施されたことが確実に確認できるものに限定した。その抜粋を表１に示す。

表１　予想される不正アクセスとその予防策（抜粋）

予想される不正アクセス	予防策
他の従業員が，ログインが成功するまでパスワードを変えて試行する。	a
他の従業員がパスワードを類推してIDを使用する。	b
他の従業員がパスワードを入手して，長期間にわたって業務システムを不正利用する。	３か月に１回のパスワード変更を強制し，過去４回分のパスワードを使用できないように設定する。

対策を導入してから６か月経過した時点でセキュリティ監査を実施し，次の問題を確認した。

・パスワードを書いたメモ用紙をディスプレイに貼っている従業員がいる。
・パスワードを忘れた従業員に対する，システム管理者によるパスワード再発行業務の負荷が高まっている。

〔生体認証システムの導入〕

Ｓ社では，業務システムへの不正アクセスを防止するために，IDとパスワードによる認証以外の手段を用いた，新たな認証システムの導入を検討することにした。総務部では，新たな認証システムの導入に当たって，認証に必要な情報をシステム管理者側で一括管理できることと，導入コストが安価であることを基本方針とした。

導入担当となった総務部システム課のＴ君は，新たな認証システムの方式として，ICカード方式と生体認証方式を検討した。

基本方針に基づきＴ君が検討した認証方式を表２に示す。

表２　Ｔ君が検討した認証方式

認証方式	概要	導入時の注意事項
ICカード方式	ICカードに埋め込んだ利用者の秘密鍵とPINコードで認証する。	・新たに［ c ］の導入が必要となる。 ・使用するPCごとにICカードリーダが必要となる。 ・ICカードの盗難や紛失時に，対象のICカードの利用停止と新たなICカードの発行が必要である。
生体認証方式	生体情報をセンサで読み取り，あらかじめ登録しておいた生体情報との類似度が高いことで認証する。導入コストが安価なものとして指紋認証方式がある。	・使用するPCごとにセンサが必要となる。 ・誤って他人を本人と認識する確率（以下，他人受入率という）と，誤って本人を拒否する確率（以下，本人拒否率という）は，いずれもできるだけ低いことが望ましい。 ・他人受入率が低い製品を選ぶと，本人拒否率は高くなる傾向にあるので，両者のバランスを考慮する必要がある。

Ｔ君は，導入コスト，新たな認証システムの運用に掛かる業務負荷の軽減，及びセキュリティ強化の契機となったセキュリティインシデントへの対応の観点から，指紋認証方式を採用することにした。

この方式の採用に当たり，氏名などの個人情報と指紋情報が同時に漏えいしないように，個人情報と指紋情報を物理的に分けた上で，一括管理を行う方針とする。

〔導入製品の決定〕

指紋認証には，次の２種類の方式がある。

・マニューシャ方式

皮膚が線状に隆起した隆線の分岐や終端部分の位置・種類・方向などの指紋特徴点（マニューシャ）を登録する。指紋特徴点だけでは元の指紋全体を再現できない。

・パターンマッチング方式

指紋全体をスキャンしてデータ化し，パターンマッチングする。

Ｔ君は，他社における指紋認証システム導入の事例を調査した。その結果，登録された指紋情報が漏えいすることや，他の目的で利用されることへの従業員の不安が大きいことが分かった。

Ｔ君は，万が一指紋情報が漏えいした場合でも①実害が少ないと考えて，マニューシャ方式を採用している製品を調査した上で導入製品を選択し，上司に報告した。

設問１　〔不正アクセス予防策の実施〕について，(1)，(2)に答えよ。

(1) 表１中の［ a ］に入れる最も適切な予防策を解答群の中から選び，記号で答えよ。

解答群

ア　業務システムとPCとの通信を暗号化する。
イ　直前のログイン記録を次回ログイン時に表示する。
ウ　パスワードを３回続けて間違えると，アカウントをロックする。
エ　ログインエラーが発生した日時を本人にメールで後日通知する。

(2) 表１中の［ b ］に入れる適切な予防策を解答群の中から二つ選び，記号で答えよ。

解答群

ア　IDと同じ文字列をパスワードに含めることを禁止する。
イ　英字，数字，記号が混在する８字以上のパスワードを設定させる。
ウ　他人とのパスワードの共有を禁止する。
エ　パスワードのヒントを設定して，自分だけが知っている答えをパスワードの一部に使用させる。

解答欄	(1)	a		
	(2)	b		

設問２　表２中の［ 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。

解答群

ア　LDAP　　イ　PKI
ウ　TLS　　エ　リバースプロキシ

解答欄	c		

設問３　〔導入製品の決定〕について，本文中の下線①で，マニューシャ方式は実害が少ないとＴ君が考えた理由を，その特徴に着目して25字以内で述べよ。

解答欄																

問 1-1-3 【2019年春期 応用 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

解答欄	(1)	a		b		
	(2)					

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。

解答欄	(1)	c		d	
	(2)				

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

解答欄	(1)	
	(2)	

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。

解答欄	