SG

平成29年度　春期
情報セキュリティマネジメント試験
午後　問題

試験時間	12:30 ～ 14:00（1時間30分）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. **答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。**
4. 問題は，次の表に従って解答してください。

問題番号	問1 ～ 問3
選択方法	全問必須

5. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) 答案用紙は光学式読取り装置で読み取った上で採点しますので，B 又は HB の黒鉛筆で答案用紙の**マークの記入方法**のとおりマークしてください。マークの濃度がうすいなど，**マークの記入方法**のとおり正しくマークされていない場合は読み取れません。特にシャープペンシルを使用する際には，マークの濃度に十分注意してください。訂正の場合は，あとが残らないように消しゴムできれいに消し，消しくずを残さないでください。
   (2) **受験番号欄**に**受験番号**を，**生年月日欄**に**受験票の生年月日**を記入及びマークしてください。答案用紙の**マークの記入方法**のとおり記入及びマークされていない場合は，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入及びマークしてください。
   (3) **解答**は，次の例題にならって，**解答欄**にマークしてください。答案用紙の**マークの記入方法**のとおりマークされていない場合は，採点されません。

〔例題〕　次の［　　］に入れる適切な字句を，解答群の中から選べ。

春の情報処理技術者試験は，［ a ］月に実施される。

解答群　ア 2　　イ 3　　ウ 4　　エ 5

適切な字句は“ウ 4”ですから，次のようにマークしてください。

例題	a	ア	イ	●	エ	オ	カ	キ	ク	ケ	コ

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

全問が必須問題です。必ず解答してください。

問1　マルウェア感染への対応に関する次の記述を読んで，設問1～3に答えよ。

T社は従業員数200名の建築資材商社であり，本社と二つの営業所の3拠点がある。このうち，Q営業所には，業務用PC（以下，PCという）30台と，NAS 1台がある。

PCは本社の情報システム課が管理しており，PCにインストールされているウイルス対策ソフトは定義ファイルを自動的に更新するように設定されている。

NASは，Q営業所の営業課と総務課が共用しており，課ごとにデータを共有しているフォルダ（以下，共有フォルダという）と，各個人に割り当てられたフォルダ（以下，個人フォルダという）がある。個人フォルダの利用方法についての明確な取決めはないが，PCのデータの一部を個人フォルダに複製して利用している者が多い。

Q営業所と本社はVPNで接続されており，営業所員は本社にある業務サーバ及びメールサーバにPCからアクセスして，受発注や出荷などの業務を行っている。

なお，本社には本社の従業員が利用できるファイルサーバが設置されているが，ディスクの容量に制約があり，各営業所からは利用できない。

T社には，本社の各部及び各課の責任者，並びに各営業所長をメンバとする情報セキュリティ委員会が設置されており，総務担当役員が最高情報セキュリティ責任者（以下，CISOという）に任命されている。また，情報セキュリティインシデント（以下，インシデントという）対応については，インシデント対応責任者として本社の情報システム課長が任命されている。さらに，本社と各営業所では，情報セキュリティ責任者と情報セキュリティリーダがそれぞれ任命されている。Q営業所の情報セキュリティ責任者はK所長，情報セキュリティリーダは，総務課のA課長である。

〔マルウェア感染〕

ある土曜日の午前10時過ぎ，自宅にいたA課長は，営業課のBさんからの電話を受けた。休日出勤していたBさんによると，Bさんの PC（以下，B-PCという）を起動して電子メール（以下，メールという）を確認するうちに，取引先からの出荷通知メールだと思ったメールの添付ファイルをクリックしたという。ところが，その後，画面に見慣れないメッセージが表示され，B-PCの中のファイルや，Bさんの個人フォルダ内のファイルの拡張子が変更されてしまい，普段利用しているソフトウェアで開くことができなくなったという。これらのファイルには，Bさんが手掛けている重

要プロジェクトに関する，顧客から送付された図面，関連社内資料，建築現場を撮影した静止画データなどが含まれていた。そこで，B さんは図 1 に示す T 社の情報セキュリティポリシ（以下，ポリシという）に従って A 課長に連絡したとのことであった。

A 課長は，B-PC にそれ以上触らずそのままにしておくよう B さんに伝え，取り急ぎ出社することにした。

8. インシデントへの対応
(1) 事象の発見と報告
当社の情報資産についてマルウェア感染，情報漏えいなどが疑われる事象を発見した従業員は，所属する拠点の情報セキュリティリーダに速やかに事象を報告する。報告を受けた情報セキュリティリーダは，速やかに事象を確認し，事象を当該拠点の情報セキュリティ責任者及びインシデント対応責任者（不在時は情報システム課員）に報告する。情報セキュリティ責任者は，情報資産の機密性，完全性，可用性に関する重大な被害が発生する可能性があると判断した場合には，インシデントの発生を宣言する。
(2) 被害拡大の防止
情報セキュリティリーダは，当該インシデントに係る被害の拡大を防止するための対策を当該拠点の従業員に指示する。
(3) 被害状況の把握，原因の特定及び影響範囲の調査
情報セキュリティリーダは，インシデント対応責任者と協力して，被害状況の把握，原因の特定及び影響範囲の調査を行う。
(4) システムの復旧
情報セキュリティリーダは，インシデント対応責任者と協力して，特定された原因の除去と，システムの復旧に努める。
(5) 再発防止策の実施
情報セキュリティリーダは，インシデント対応責任者とともにインシデントの再発防止策を検討し，実施する。

図 1　ポリシ（抜粋）

A 課長が Q 営業所に到着して B-PC を確認したところ，画面にはファイルを復元するための金銭を要求するメッセージと，支払の手順が表示されていた。A 課長は，B-PC がマルウェアに感染したと判断し，K 所長に連絡して，状況を報告した。この報告を受けた K 所長は，インシデントの発生を宣言した。また，B さんは，A 課長の指示に従って B-PC と NAS から LAN ケーブルを抜いた。

さらに，A 課長が B さんに，他に連絡した先があるかを尋ねたところ，A 課長以外にはまだ連絡していないとのことであった。そこで，A 課長はインシデント対応責任者である情報システム課長に連絡したところ，情報システム課で情報セキュリティ

を主に担当している S 係長に対応させると言われた。そこで，A 課長は S 係長に連絡し，現在の状況を説明した。

S 係長によると，状況から見て［ a ］と呼ばれる種類のマルウェアに感染した可能性が高く，①この種類のマルウェアがもつ二つの特徴が現れているとのことであった。A 課長は S 係長に，今後の対応への協力と当該マルウェアに関する情報収集を依頼し，S 係長は了承した。その後，A 課長が状況の調査を更に進めていたところ，昼過ぎに K 所長が Q 営業所に到着したので，A 課長はその時点までの調査結果を K 所長に説明した。調査結果を図 2 に示す。

・B-PC 上のファイルと，B-PC から個人フォルダに複製したファイルがマルウェアによって暗号化されており，開くことができない状態になっていた。一方，B さんは，顧客から送付されたデータを営業課の共有フォルダに複製していたが，そのデータに異常は見られなかった。
・B-PC に表示されたメッセージによると，B さんのファイルは AES と RSA の二つの暗号アルゴリズムを用いて暗号化されており，これが事実だとすると，復号することは極めて困難である。
・［ a ］によっては，暗号化されたデータを復号できるツールがウイルス対策ソフトベンダなどから提供されている場合もあるが，今回のマルウェアに対応しているツールはない。また，［ a ］によっては OS の機能を用いると暗号化される前のデータが OS の復元領域から復元できる場合もあるが，今回のマルウェアは，OS の復元領域を削除していた。
・今回のマルウェアは，金銭の受渡しに際して，②攻撃者の身元を特定できなくするための技術を利用している。
・B-PC 以外の Q 営業所の PC は全てシャットダウンされていた。

図 2　調査結果

〔感染後の対応〕

K 所長と A 課長は，金銭の支払に応じるべきか否かは Q 営業所だけで判断できることではないが，それぞれの場合に想定される被害及び費用の項目は一応把握しておきたいと考えた。そこで，“支払った場合にはデータを確実に復元できるが，支払わなかった場合にはデータを復元できない可能性が高い”という前提の下で想定される被害及び費用の項目を，表 1 の Ⅰ～Ⅲに分けてリストアップした。

表１　想定される被害及び費用の項目

Ⅰ．支払った場合にだけ，発生する又は発生するおそれがある項目	b
Ⅱ．支払わなかった場合にだけ，発生する又は発生するおそれがある項目	c
Ⅲ．支払っても支払わなくても発生する又は発生するおそれがある項目	（省略）

注記１　項目には，金額のほか，価値の喪失，損失といったものも含まれるものとする。
注記２　Ⅰ，Ⅱ，Ⅲは互いに排他的である。

折よく，当該マルウェアに関する情報収集を行っていた S 係長から，他社での対応事例の報告があった。これを受け，K 所長と A 課長は，表 1 作成時の前提を置かずに③対応について検討することにし，その結果を情報セキュリティ委員会に報告して CISO の判断を仰ぐことにした。

夕方になって，本社で調査を行っていた S 係長から A 課長に連絡があり，今朝のマルウェア感染以降，Q 営業所のネットワークから本社や外部への不審な通信は行われていないことが分かった。また，業務で利用している本社のサーバにも特に異常は見られなかったという。

これまでの調査から，被害は B-PC 及び B さんの個人フォルダ内のファイルだけであったと A 課長は判断し，B さん用の新たな PC を準備するよう S 係長に依頼した。

翌日の日曜日の朝，ウイルス対策ソフトの開発元から新たな定義ファイルが提供され，B-PC が感染していたマルウェアの検知と駆除が可能になった。そこで，その日の午後に T 社の全ての PC，サーバ及び Q 営業所の NAS に対してマルウェアのスキャンを行ったところ，B-PC 以外にマルウェアに感染していたものはなかった。また，暗号化されていた NAS 上のデータに関しては，NAS のデータのバックアップは実施されていなかったものの，NAS の復元領域から一部を復元できることが判明し，業務への影響はある程度抑えることができた。

〔対策の見直し〕

今回のインシデントを受けて，T 社の情報セキュリティ委員会が開催された。A 課長は，CISO から，今回のインシデントに関する問題点は何かと尋ねられた。A 課長は，④データの取扱い及びバックアップに関するルールの内容が不十分であったこと

が問題点であったと回答し，次のことを提案した。

・データの取扱い及びバックアップに関するルールを全面的に見直し，全社的なルールを定めること

・本社のファイルサーバの容量拡大を早急に実施し，全社共通の利用ルールを定め，それに基づいて各営業所からも利用できるようにすること

・営業所での NAS の利用は半年以内に廃止すること

・NAS の利用を暫定的に継続する間は，営業所では⑤今回の種類のマルウェアに感染することによってファイルが暗号化されてしまうという被害に備えたバックアップを実施し，あわせて⑥バックアップ対象のデータの可用性確保のための対策を検討すること

これらの提案は情報セキュリティ委員会で承認された。T 社はマルウェア感染を契機として情報セキュリティの改善を図ることになった。

設問 1　〔マルウェア感染〕について，(1) ～ (3) に答えよ。

(1)　本文中及び図 2 中の［　a　］に入れる字句はどれか。解答群のうち，最も適切なものを選べ。

a に関する解答群

ア　アドウェア　　イ　キーロガー

ウ　ダウンローダ　　エ　ドロッパ

オ　ランサムウェア　　カ　ルートキット

キ　ワーム

(2) 本文中の下線①について，この種類のマルウェアの特徴を，次の (i) ～ (vii) の中から二つ挙げた組合せはどれか。解答群のうち，最も適切なものを選べ。

(i) OS やアプリケーションソフトウェアの脆弱性が悪用されて感染することが多い点

(ii) Web ページを閲覧するだけで感染することがある点

(iii) 感染経路が暗号化された通信に限定される点

(iv) 感染後，組織内部のデータを収集した上でひそかに外部にデータを送信することが多い点

(v) 端末がロックされたり，ファイルが暗号化されたりすることによって端末やファイルの可用性が失われる点

(vi) マルウェア対策ソフトが導入されていれば感染しない点

(vii) マルウェアに感染した PC の利用者やサーバの管理者に対して脅迫を行う点

解答群

ア (i), (ii)　　イ (i), (iii)

ウ (i), (v)　　エ (ii), (iii)

オ (ii), (iv)　　カ (iii), (v)

キ (iii), (vii)　　ク (iv), (vi)

ケ (v), (vi)　　コ (v), (vii)

(3) 図 2 中の下線 ② について，当てはまる技術だけを挙げた組合せを，解答群の中から選べ。

解答群

ア Bitcoin，SSL-VPN，Tor

イ Bitcoin，Tor

ウ Bitcoin，ゼロデイ攻撃

エ Bitcoin，ポストペイ式電子マネー

オ SSL-VPN，Tor

カ SSL-VPN，ゼロデイ攻撃

キ SSL-VPN，バックドア，ポストペイ式電子マネー

ク Tor，バックドア，ポストペイ式電子マネー

ケ ゼロデイ攻撃，バックドア

コ ゼロデイ攻撃，バックドア，ポストペイ式電子マネー

設問２　〔感染後の対応〕について，(1)，(2)に答えよ。

(1)　表１中の［　b　］，［　c　］に入れる字句を，解答群の中から選べ。ここで，次の[項目 1]～[項目 5]は，解答群の[項目 1]～[項目 5]と対応するものとする。

[項目 1] 攻撃者から要求されている金額

[項目 2] 再発防止に要する金額

[項目 3] 自力でのデータ復元の試みに要する金額

[項目 4] 犯罪を助長したという事実に起因する企業価値の損失

[項目 5] マルウェアに感染したという事実に起因する企業価値の損失

b，cに関する解答群

ア　[項目 1]，[項目 2]

イ　[項目 1]，[項目 2]，[項目 3]

ウ　[項目 1]，[項目 2]，[項目 4]

エ　[項目 1]，[項目 3]

オ　[項目 1]，[項目 4]

カ　[項目 2]，[項目 4]

キ　[項目 2]，[項目 5]

ク　[項目 3]

ケ　[項目 4]

コ　[項目 5]

(2) 本文中の下線③について，支払に応じるべきではないと情報セキュリティ委員会で報告するとしたら，その理由は何か。次の(i)～(iv)のうち，適切なものだけを全て挙げた組合せを，解答群の中から選べ。

(i) 金銭を支払うことによって，自社への更なる攻撃につながり得るから

(ii) 金銭を支払っても，ファイルを復号できる保証がないから

(iii) 外部業者にディジタルフォレンジックスを依頼すれば，暗号化されたデータを確実に復号できるから

(iv) 表1において，ⅠとⅡを比較した結果，Ⅰの方が，被害及び費用が小さいから

解答群

ア (i)，(ii)　　イ (i)，(ii)，(iii)

ウ (i)，(ii)，(iv)　　エ (i)，(iii)

オ (i)，(iii)，(iv)　　カ (i)，(iv)

キ (ii)，(iii)　　ク (ii)，(iii)，(iv)

ケ (ii)，(iv)　　コ (iii)，(iv)

設問3 〔対策の見直し〕について，(1)～(3)に答えよ。

(1) 本文中の下線④の直接的な結果として，何が起きたか。解答群の中から二つ選べ。

解答群

ア B-PCのOSの復元領域が削除されたこと

イ T社の業務サーバ及びメールサーバがVPNで営業所と接続され，受発注や出荷などのデータが送受信されたこと

ウ Q営業所でNASのデータのバックアップが実施されなかったこと

エ 業務で利用するデータについて，何をNASに保存するか，PCに保存するかが人によってまちまちだったこと

(2) 本文中の下線 ⑤ について，次の (i) ～ (iv) のうち，効果があるものだけを全て挙げた組合せを，解答群の中から選べ。

(i) NAS 上の特に重要なフォルダについては，定期的に BD-R にデータを複製し，BD-R は鍵が掛かるキャビネットに保管する。

(ii) NAS に定期的に別途ハードディスクドライブを追加接続してデータをアーカイブし，終了後にハードディスクドライブを取り外して保管する。

(iii) NAS にハードディスクドライブを増設し，RAID5 構成にすることによってデータ自体の冗長性を向上させる。

(iv) NAS にハードディスクドライブを増設して，増設したハードディスクドライブにデータを常時レプリケーションするようにする。

解答群

ア (i)　　イ (i), (ii)

ウ (i), (ii), (iv)　　エ (i), (iii)

オ (i), (iii), (iv)　　カ (ii)

キ (ii), (iv)　　ク (iii)

ケ (iii), (iv)　　コ (iv)

(3) 本文中の下線 ⑥ について，次の (i) ～ (iv) のうち，効果があるものだけを全て挙げた組合せを，解答群の中から選べ。

(i) バックアップした媒体からデータが正しく復元できるかテストする。

(ii) バックアップした媒体を二つ作成し，一つは営業所に，もう一つは別の安全な場所に保管する。

(iii) バックアップした媒体を再び読み出せないようにしてから廃棄する。

(iv) バックアップする際にデータに暗号化を施す。

解答群

ア (i)　　イ (i), (ii)

ウ (i), (ii), (iii)　　エ (i), (iv)

オ (ii)　　カ (ii), (iii)

キ (ii), (iii), (iv)　　ク (ii), (iv)

ケ (iii)　　コ (iii), (iv)

問2　クラウドサービスを利用した情報システムの導入と運用に関する次の記述を読んで，設問1，2に答えよ。

X社は，従業員数8,000名の生命保険会社である。本社には，営業本部販売企画課，情報システム部などがあり，また，全国に営業所が設置されている。各営業所には，所長，主任，社内事務を担当する従業員（以下，スタッフという）及び営業を担当する従業員（以下，販売員という）がいる。X社の組織の主な担当業務及び体制を表1に示す。

表1　X社の組織の主な担当業務及び体制（抜粋）

組織	主な担当業務	体制
営業所	各地域での保険販売，販売員の管理など	所長：1名 主任：1名（情報セキュリティリーダ兼務） スタッフ：1～2名 販売員：30～50名
販売企画課	販売方法の企画立案など	課長：1名 主任：4名（うち1名は情報セキュリティリーダ兼務） その他の従業員：15名
情報システム部	X社の情報システムに係る企画，開発，運用管理など	（省略）

X社は，従来，各営業所の担当地域にある企業（以下，訪問先という）から許可を得て，訪問先の昼休みや就業時間後に，販売員が職場を訪問して，保険の募集活動を行っていた。しかし，近年は，訪問先の情報セキュリティ対策が強化され，許可がなかなか得られず，得られても昼休みに商品案内資料を配布するなど限定的な活動しかできない状況であった。そのため，訪問先の従業員とどのようにコンタクトして保険販売につなげていくのかがX社にとって課題であった。

この状況を打開するために，販売企画課に4月に着任したU課長が，E主任をリーダとしてその配下の従業員をメンバとするプロジェクト（以下，Hプロジェクトという）を立ち上げた。Hプロジェクトの目標は，打開策を検討して実施の上，来年3月までに今後の対応案を確定させることである。そこで，まず打開策の集中検討を行った。その結果，訪問先の従業員のうち，販売員が，保険商品の情報提供，広

告宣伝などのために，氏名及びメールアドレスを取得できた見込客に対して，事前に同意を得た上で，電子メール（以下，メールという）を使ってコンタクトすることが提案され，販売企画課で承認された。メールは一斉配信ではなく，見込客の家族構成などに応じた保険情報などを付けて個別に送信する。

H プロジェクトでは，今年の 9 月末までに準備を終えて，10 月から来年 3 月まで，3 営業所でメールを使ったコンタクトを試行する計画である。準備や教育は，原則，販売企画課で行うという条件で 3 営業所に試行の協力を依頼することにした。来年 4 月以降は，試行の結果を評価した上で，対象の営業所を順次拡大していく計画である。

U 課長は，見込客データの管理などを効率的に行うには情報システムの活用が必要であると考え，情報システム部と相談して，早急に準備を進めるように E 主任に指示した。また，見込客データを取り扱うので，情報セキュリティについて万全を期すために，販売企画課の情報セキュリティリーダである C 主任にも H プロジェクトに参画するように指示した。

E 主任が C 主任と一緒に情報システム部に相談したところ，H プロジェクト用に社内の顧客管理システムや人事情報システムなどの情報システムを 9 月末までに改修するのは難しいので，代わりに，クラウドサービスを利用することを提案された。X 社では，クラウドサービスを利用する場合の情報システム部と利用部門の役割分担を表 2 のとおり定めている。

表 2　X 社におけるクラウドサービス利用に関する役割分担（抜粋）

情報システム部の役割	利用部門の役割
・クラウドサービスプロバイダの事業者評価 ・クラウドサービスの情報セキュリティ対策の確認（利用部門の情報セキュリティリーダとともに行う） ・サービス利用契約の締結 ・障害時のシステム対応（利用部門と協議）	・サービスの利用可否及び利用継続要否の判断 ・利用上の各種設定，管理（カスタマイズ機能の選択，アカウント管理など） ・障害時の連絡，対応体制の整備（情報システム部と協議）

情報システム部は，クラウドサービスプロバイダ Y 社が提供する SaaS（以下，Y 社 SaaS という）の顧客管理サービスを販売企画課に推薦した。このサービスは，顧客管理のための標準機能が追加開発なしに利用可能であり，さらに，カスタマイズ機能として，画面表示項目や情報セキュリティ機能などを利用側で設定可能である。ま

た，Y 社 SaaS が別途提供しているメールサービスと連携させて利用できるなど，利用側での柔軟なカスタマイズが可能である。

H プロジェクトでは，Y 社 SaaS の顧客管理サービスについて，X 社の情報セキュリティ対策基準に沿って情報セキュリティ機能を設定し，Y 社 SaaS のメールサービスと連携させて利用することにした。これを X 社内では販売支援システム（以下，P システムという）と名付けて，9 月末までに準備する案とした。P システムの概要を図 1 に示す。

Ⅰ. P システムの利用形態

利用場所	利用 PC [1]	P システムへのアクセス手順
X 社の本社及び営業所のオフィス内	デスクトップ PC 及びモバイル PC	1. Web ブラウザを用いて，社内ポータルにログイン 2. 社内ポータルにあるリンクから，インターネット経由で P システムにログイン [2]
社外	モバイル PC	1. VPN によって社内 LAN [3] に接続 2. Web ブラウザを用いて，社内ポータルにログイン 3. 社内ポータルにあるリンクから，インターネット経由で P システムにログイン [2]

Ⅱ. P システムの主な機能

機能	説明
見込客データ管理	見込客データの追加，参照，更新，削除 データ項目：氏名，性別，生年月日，電話番号，メールアドレス，勤務先企業名，部署名，役職名，家族構成など
メール送受信	メール送信指示，送信停止・停止解除，メール受信，送受信履歴の参照
データ分析	見込客データやメール送受信履歴を基にしたデータ分析
アカウント管理	利用者及び管理者のアカウント登録，無効化，権限変更
カスタマイズ	画面表示項目，情報セキュリティ機能など

Ⅲ. Y 社 SaaS に関し，X 社が Y 社に確認した主な項目

(i) 計画停止が行われる際の予告方法及びリードタイム
(ii) X 社によるサービス利用終了時の，Y 社 SaaS で管理されていたデータの取扱い
(iii) Y 社 SaaS におけるデータ暗号化機能の有無
(iv) Y 社 SaaS のダッシュボードで表示される，サービスのリソース使用状況
(v) Y 社のデータセンタにおける入退室管理，管理者特権の管理の状況

注 [1] 販売員を除く X 社の全従業員はデスクトップ PC を，販売員はモバイル PC を貸与され利用している。会社貸与の PC は，外部記憶媒体の接続を技術的な方法によって禁止している。

[2] P システムのログインは，社内ポータルのログインとは別に行う。

[3] X 社の社内 LAN は，会社貸与の PC 以外の機器（私物の PC，スマートフォンなど）の接続を技術的な方法によって禁止している。

図 1　P システムの概要（抜粋）

Y 社 SaaS は，ファイアウォールの設置をはじめ，通信ログの監視など，サイバー攻撃対策にも万全を期している。

なお，P システムのサーバは全て日本国内にある。また，Y 社 SaaS の利用規約には Y 社の守秘義務も規定されている。

〔P システムの利用に関する検討〕

次は，P システムの利用に関して検討した際の，E 主任と C 主任の会話である。

E 主任：P システムをオンプレミスで準備する場合と比べてみましょう。クラウドサービスを利用するメリットには，［ a ］こと，及び導入期間が短いことがあります。前者のメリットは，来年 4 月以降の計画にも適しています。ただ，見込客データを外部に預けることに，機密性の点で不安があります。

C 主任：機密性の点は，①情報システム部と一緒に Y 社 SaaS における情報セキュリティ対策を確認し，問題ないと判断しました。

E 主任：クラウドサービスを用いると，販売員が自宅の PC などから直接アクセスするといったことも起きかねません。そのようなアクセスを禁止できるとよいのですが，できますか。

C 主任：はい。P システムの情報セキュリティ機能において，［ b ］からのアクセスだけを受け付ける設定にすることによって，禁止できます。

E 主任：なるほど。ところで，Y 社 SaaS で障害が発生した場合でも，P システムは利用できますか。

C 主任：Y 社 SaaS は，例えば，一部のサーバが故障しても，サービスは継続されます。しかし，障害の内容によってはサービスの利用に影響が生じるので，障害時の連絡，対応体制は当社でも整備しておく必要があります。また，Y 社の倒産など，突然サービスが終了するといった事態を想定し，さらにコストパフォーマンスも考慮すると，最低限，当社側での［ c ］について検討が必要です。それについて，情報システム部と一緒に Y 社に相談することにしています。

その後，E 主任と C 主任は，P システムの利用に関する案を作成し，U 課長に報告して承認を得た。

〔アカウント及び操作権限の管理〕

E主任は，図2に示すX社の情報セキュリティ対策基準などを参照しながら，Pシステムのアカウントの種類と各機能の操作権限の案を表3にまとめた。権限設定に当たって，試行なので営業所の負担が軽くなるようにするとともに，見込客データを参照しながら，メールの送受信履歴の分析ができるように考慮した。

アカウントの設定と付与
1. アカウントは，業務上，必要最小限の従業員に限定して付与し，従業員の役職，職務などに応じて，アクセス可能なデータの範囲及び機能の操作権限を適切に設定すること
2. アカウントの登録，無効化，権限変更などを行う管理者を定めること
3. 従業員の異動などが生じた際には，当該従業員のアカウントに速やかに反映すること
4. アカウント管理においては，相互牽制が働く手順を定めること

図2　X社の情報セキュリティ対策基準（抜粋）

表3　Pシステムのアカウントの種類と各機能の操作権限の案（抜粋）

Hプロジェクトに参加する者に付与するアカウントの種類	アクセス可能な見込客データの範囲	見込客データ管理機能の操作権限				メール送受信機能の操作権限			アカウント管理機能の操作権限	
		データの追加	データの参照	データの更新	データの削除	メール送受信	送信停止・停止解除	送受信履歴の参照	登録・無効化・権限変更の申請	登録・無効化・権限変更の承認
販売員用アカウント（販売員に付与する）	当該販売員の担当分	○	○	○	×	○	○	○	×	×
営業所管理者用アカウント（営業所の所長及び主任に付与する）	当該営業所の販売員の担当分	×	○	×	×	×	×	○	×	×
販売企画課担当者用アカウント（Hプロジェクトの従業員に付与するが，E主任とC主任は除く）	全て	×	○	×	×	×	×	○	×	×
販売企画課管理者用アカウント（E主任に付与する）	全て	×	○	×	○	×	×	○	○	○

注記　○は操作権限が設定されることを，×は操作権限が設定されないことを示す。

次は，E主任が作成した表3について，C主任に意見を求めた際の会話である。

C主任：気になることが3点あります。

1点目は，営業所管理者用アカウントに，アカウント管理機能の操作権限が設定されないことです。

E主任：Hプロジェクトでは，事務手続に関する作業は主に販売企画課で担当することにしたので，販売企画課管理者用アカウントに権限を設定する案にしました。

C主任：販売企画課がアカウント管理を行う場合でも，入退社が不定期な販売員に付与するアカウントを，速やかに登録，無効化，権限変更する必要があります。

E主任：その点については，10月1日から実施でき，かつ，X社の情報セキュリティ対策基準を満たす方法として，［ d ］という対応を行います。

C主任：分かりました。2点目は，販売企画課管理者用アカウントに，アカウント管理機能の操作権限が全て設定されていることです。この点については，［ e ］のがよいと思います。

E主任：分かりました。

C主任：3点目は，メール送信を開始した後で，見込客がメールの送信を停止してほしいと考えたときの手続です。見込客はどうすればよいですか。

E主任：見込客が，担当の販売員に申し出れば，販売員が停止操作を行います。

C主任：それだけでは不十分だと思います。まずは，②販売員用アカウント以外のアカウントにも送信停止の権限を設定する必要があると思います。それに加えて，停止処理用URLをメールに付して，見込客が自ら停止できるように，［ f ］が容易に行える仕組みを提供すべきです。

E主任：分かりました。

C主任とE主任は，検討の結果をU課長に説明し了解を得た。

その後，C主任が指摘した事項も実施され，U課長に完了報告をして，準備が全て整った。そして，社内の手続に従った本番移行判定も問題なく終了し，予定どおり，10月から，Pシステムの利用が開始された。

設問1　〔Pシステムの利用に関する検討〕について，(1)～(4)に答えよ。

(1)　本文中の［　a　］に入れる字句はどれか。解答群のうち，最も適切なものを選べ。

aに関する解答群

ア　IT資源を迅速かつ柔軟に利用できる

イ　サービス利用契約及び情報システム導入の際の事務負担が軽減できる

ウ　見込客に送信するメールの内容や頻度が自由に変更できる

エ　見込客へのコンタクトがメールを使って，いつでもどこからでも制約なくできる

(2)　図1中のⅢにおける項目(i)～(v)の中から，本文中の下線①で確認した情報セキュリティ対策を三つ挙げた組合せはどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　(i)，(ii)，(iii)　　イ　(i)，(ii)，(iv)　　ウ　(i)，(ii)，(v)

エ　(i)，(iii)，(iv)　　オ　(i)，(iii)，(v)　　カ　(i)，(iv)，(v)

キ　(ii)，(iii)，(iv)　　ク　(ii)，(iii)，(v)　　ケ　(ii)，(iv)，(v)

コ　(iii)，(iv)，(v)

(3) 本文中の［ b ］に入れる字句はどれか。解答群のうち，最も適切なものを選べ。

b に関する解答群

ア　P システムの URL

イ　X 社のグローバル IP アドレス

ウ　会社貸与の PC の MAC アドレス

エ　会社貸与の PC のシリアルナンバ

(4) 本文中の［ c ］に入れる字句はどれか。解答群のうち，最も適切なものを選べ。

c に関する解答群

ア　P システムの RPO，RTO の確認

イ　P システムのコールドスタンバイ

ウ　P システムの操作履歴の確認

エ　見込客データの暗号化

オ　見込客データの匿名化

カ　見込客データのバックアップ

設問2　〔アカウント及び操作権限の管理〕について，(1)，(2)に答えよ。

(1)　本文中の［ d ］～［ f ］に入れる字句はどれか。解答群のうち，最も適切なものを選べ。

dに関する解答群

ア　営業所の所長又は主任が，都度，販売企画課にメールで連絡する

イ　人事情報システムを改修して，データ連携を自動化する

ウ　販売員自らが，都度，販売企画課にメールで連絡する

エ　毎年度末に，販売企画課が営業所に確認し，登録や無効化を行う

eに関する解答群

ア　販売企画課管理者用アカウントの付与はE主任のままとして，E主任の操作に私（C主任）が立会い，目視確認する

イ　販売企画課管理者用アカウントを私（C主任）にも付与して，申請・承認した結果をE主任と私（C主任）で相互チェックする

ウ　販売企画課担当者用アカウントにも申請権限及び承認権限を設定して，申請・承認した結果をE主任が確認する

エ　販売企画課担当者用アカウントには申請権限だけを設定し，販売企画課管理者用アカウントには承認権限だけを設定して，後者の付与はE主任のままとする

fに関する解答群

ア　アカウントロック　　イ　オプトアウト

ウ　オプトイン　　エ　チェックアウト

オ　チェックイン　　カ　リモートワイプ

(2) 次の (i) ～ (v) の中から，本文中の下線 ② の対応が必要である理由を三つ挙げた組合せはどれか。解答群のうち，最も適切なものを選べ。

(i) 全ての事務手続に関する作業を，販売企画課だけが処理できるように操作権限を設定する必要があるから

(ii) 販売員が，送信停止処理よりも販売活動を優先するおそれがあるから

(iii) 見込客が本社宛てに電話などで申し出た場合でも，停止処理ができるようにする必要があるから

(iv) 見込客を担当する販売員が不在の場合でも，電話を受けた営業所で停止処理ができるようにする必要があるから

(v) メールの“送受信履歴の参照”の権限を全てのアカウントに設定しているから

解答群

ア (i), (ii), (iii)	イ (i), (ii), (iv)	ウ (i), (ii), (v)
エ (i), (iii), (iv)	オ (i), (iii), (v)	カ (i), (iv), (v)
キ (ii), (iii), (iv)	ク (ii), (iii), (v)	ケ (ii), (iv), (v)
コ (iii), (iv), (v)		

問３　オフィスの物理的セキュリティに関する次の記述を読んで，設問 1～3 に答えよ。

F 社は従業員数 300 名の高級家具卸販売会社である。

〔D 事業所のレイアウト変更〕

F 社は，今年，通販事業部を新設し，消費者に直接通信販売する新規事業を開始した。通販事業部は，本社から離れた所にある平屋建ての D 事業所を卸事業部とともに使用している。D 事業所では，卸事業部の人数と通販事業部の人数を合計して 40 名の従業員が働いている。これまで F 社は，個人情報はほとんど取り扱っていなかったが，通信販売事業が順調に拡大し，複合機で印刷した送り状など，顧客の個人情報を大量に取り扱うようになってきた。そこで，通販事業部の N 部長は，情報セキュリティを強化するために，オフィスレイアウトの変更を本社の総務部に依頼することにした。

これまで F 社では，D 事業所の事業部エリアへの入退室時に何のチェックもしていなかった。そこで，D 事業所で働く全ての従業員に IC カード機能を備えた従業員証を新たに配布した上で，通販事業部の従業員だけが通販事業部エリアに入退室できるようにした。具体的には，オフィスレイアウトを変更し，通販事業部エリアの出入口に，IC カード認証でドアを解錠するシステム（以下，IC カードドアという）を設置することにした。D 事業所の新たなオフィスレイアウトを図 1 に示す。

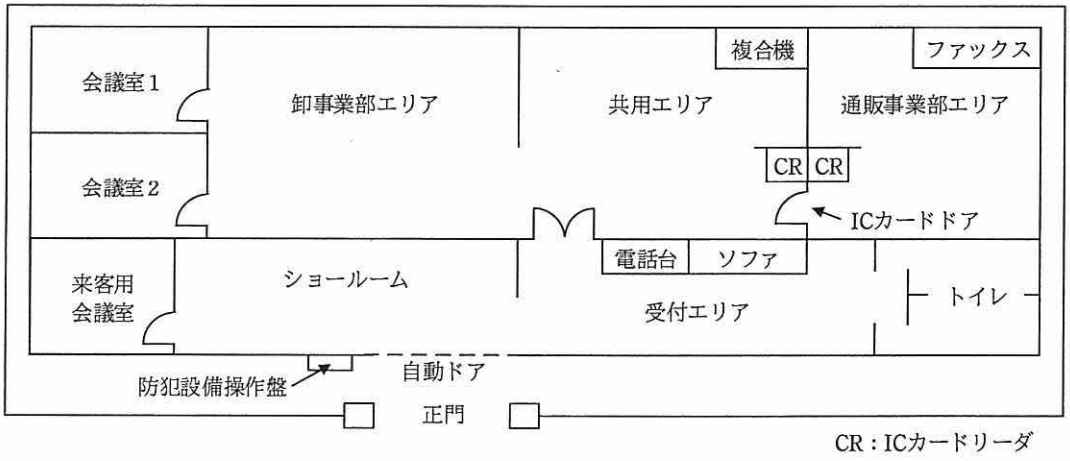

図 1　D 事業所の新たなオフィスレイアウト

D 事業所には防犯設備が設置されており，防犯設備操作盤で D 事業所の自動ドアの施錠と解錠，及び防犯状態の設定と解除を行うことができる。防犯状態では D 事業所内の侵入検知センサが有効になり，侵入者を検知すると警備会社へ自動通報するように設定されている。防犯設備操作盤は普段は施錠されており，管理職全員に貸与されている鍵で解錠して操作し，操作後は施錠することになっている。D 事業所の就業時間は午前 9 時から午後 6 時までであり，朝早く出勤する従業員も，残業をする従業員もいるが，残業が午後 10 時を超えることはない。

〔新たなオフィスレイアウトでの業務観察〕

レイアウト変更の工事が終了し，新たなオフィスレイアウトでの業務が開始された。N 部長は，D 事業所の情報セキュリティリーダである通販事業部の W 氏に，新たなオフィスレイアウトにおける業務運用に情報セキュリティ上の問題がないかどうかを改めて確認し，問題がある場合は改善の提案をするように指示した。W 氏が新たなレイアウトでの業務を観察したところ，表 1 に示す三つの問題点が発見された。

表 1　W 氏が発見した問題点

問題点番号	問題点
問題点 1	共用エリアの複合機で，個人情報を含む文書を印刷した後，その印刷物をそのまま放置している。
問題点 2	通販事業部が，ファックスで受信した注文書，商品発送時の送り状の控えなど，個人情報が記録された紙媒体を大量に保有しているが，十分な管理がされていない。
問題点 3	通販事業部エリアへの入室時に，通販事業部の従業員同士による共連れが行われている。

そこで W 氏は，各問題点に対する改善案を自ら検討し，あわせて，業務に日々従事している D 事業所の従業員からも意見を広く募り，それらを取りまとめることにした。表 2 に，各問題点に対する改善案及び W 氏の判断を示す。

表2　表1の問題点に対する改善案及びW氏の判断

問題点番号	問題点に対する改善案	W氏の判断
問題点1	(案1) 現在の複合機に備わっている，“文書の印刷指示をした従業員が複合機のところに行って従業員証を使って認証されると印刷が開始される”という機能を有効にする。 (案2) 情報セキュリティを高めるために，個人情報を含む文書の印刷を禁止する。 (案3) 複合機を，印刷後に複合機内の印刷データが完全に消去される，ISO/IEC 15408 認証を取得した安全性が高い複合機に交換する。 (案4) 複合機を通販事業部エリア内にも設置し，通販事業部の従業員は当該複合機でしか印刷できないようにする。	(案1)～(案4)のうち，［ a ］が改善策として有効である。
問題点2	(案5) 個人情報が記録された紙媒体は，業務上の必要の有無にかかわらず，1週間以内に細断し，廃棄する。細断するまでは，キャビネットに施錠保管する。 (案6) 新たに文書管理システムを導入し，個人情報が記録された紙媒体は，スキャナで電子化して適切に管理する。不要となった紙媒体は細断し，廃棄する。 (案7) 個人情報が記録された紙媒体は，バインダにとじた上で，機密情報であることが分かるように機密区分を明示し，キャビネットに施錠保管する。 (案8) 個人情報が記録された紙媒体は，どこにあるか分からないように，他の文書と混ぜて机の上に並べる。	(案5)～(案8)のうち，［ b ］が改善策として有効である。
問題点3	(案9) ICカードドアを，AESの暗号方式を用いたものに変更する。 (案10) 共連れがもたらすリスクを知らせる標語を作成して，ICカードドアの脇に掲示する。 (案11) ICカードの認証に加えて指静脈認証も行うようにする。 (案12) 情報セキュリティリーダが共連れを発見した場合は個別に注意する。	(案9)～(案12)のうち，［ c ］が改善策として有効である。

W氏が，取りまとめた改善案及び判断をN部長及び関係部署に提示して議論した結果，幾つかの改善策が実施されることになった。

共連れの改善策を実施してから 2 週間後，W 氏は，効果を検証したいと考え，総務部から 1 か月間の入退室ログを取り寄せ，①共連れだと思われるログを抽出し，抽出されたログを基に，該当する従業員に共連れをしていないかどうかを確認した。その結果，改善策実施前と比べると件数は減少していたものの，まだ時々共連れが行われていることが分かった。次はN部長とW氏の会話である。

N部長 ：まだ共連れが行われているな。②現状のままにするという対応もあるが，他に方法はないだろうか。

W氏 ：③アンチパスバックを有効にするように総務部から勧められています。

N部長 ：それはいいな。早速総務部に依頼して有効にしておいてくれ。

W氏 ：分かりました。加えて，共連れ防止ゲートを導入すれば，更に効果があると思います。

N部長 ：でもそれは費用がとても掛かるらしい。共連れによるリスクを考慮すると，そこまではしなくてよい。

W氏 ：万が一，個人情報が漏えいした場合に備えて，④個人情報漏えい保険に加入するというのはどうでしょうか。

N部長 ：そのような保険があるとは知らなかったよ。保険の件は，アンチパスバックの設定の効果を検証した後に，やはり必要であれば検討することにしよう。

W氏 ：分かりました。

N部長 ：リスクをゼロにしようとしたら，⑤事業をやめるしかない。事業を行っている限りリスクは付き物だ。

〔防犯設備操作盤の施錠方式の検討〕

ある日，通販事業部の管理職である課長が退職することになった。次は N 部長とW氏の会話である。

N部長 ：退職する課長から防犯設備操作盤の鍵を忘れずに返してもらってくれ。

W氏 ：分かりました。でも，［ d1 ］の鍵ですから，鍵店に行けば簡単に合い鍵が作れます。その課長に，合い鍵を作っていないことを確認しますが，

[d1] はセキュリティ強度が高いとはいえないですね。

N部長 ：確かにそれはそうだな。そういえば，前に私がいた事業所では [d2] を使っていたよ。

W氏 ：[d2] なら，管理職が退職したときには，設定を変えるだけで，その退職者は利用できないようになります。ただ，[d2] は，情報が他人に漏れたら解錠されてしまいますね。

N部長 ：しっかりしていない管理職もいるから採用できないな。知り合いの会社では，[d3] を使っているという話を聞いたことがある。

W氏 ：[d1] の鍵と違って複製が困難ですね。他にも，[d4] を使うのはどうでしょう。

N部長 ：管理職が必ずしも朝一番で出勤できるとは限らないから，解錠に必要なものを貸与可能な [d3] の方が都合がいいだろう。

W氏は，N部長の指示を受け，防犯設備操作盤の錠の変更について総務部と相談することにした。

〔コールセンタの情報セキュリティ対策の検討〕

通信販売事業における消費者からの問合せ増加に伴い，別の事業所で通販事業部専用のコールセンタを立ち上げることになった。F社従業員の一部を配置転換するとともに，新たに20人のパート又はアルバイトを雇用してコールセンタ要員とする。さらに，新製品の発売などで問合せが増加した際には，臨時で短期間のアルバイトを雇用する。W氏は，N部長に依頼され，コールセンタでの情報セキュリティ対策案（表3）を作成した。

表3　コールセンタでの情報セキュリティ対策案

No	脅威	対策
1	コールセンタ要員以外の者が侵入する。	・ e ・ f
2	コールセンタ要員が記憶媒体を持ち込み，情報を窃取する。	・ f ・ g
3	コールセンタ要員がノートPCを盗み出す。	・ f ・ g ・ h

次はN部長とW氏の会話である。

N部長　：脅威は私の想定どおりだ。監視カメラは設置しないのかね。

W氏　　：忘れていました。出入口に設置しようと思います。執務室内にも設置しましょうか。

N部長　：働く人が嫌がるかもしれないな。総務部と相談して決めてくれ。コールセンタ要員以外の者が侵入する脅威への対策として，共連れ防止ゲートを設置したらどうだろう。

W氏　　：それも検討したのですが，コールセンタの事業所のビルの所有者から設置を断られてしまいました。

N部長　：そうか，それは仕方がないな。これ以外の細かいところは総務部と相談して進めてほしい。また，コールセンタの運用が始まってからも，対策の費用対効果を定期的に確認して改善していってほしい。

W氏　　：分かりました。

その後，W氏と総務部の協力によってコールセンタの情報セキュリティ対策が導入され，無事にコールセンタでの業務が開始された。

設問1　〔新たなオフィスレイアウトでの業務観察〕について，(1) ～ (3) に答えよ。

(1) 表 2 中の［ a ］～［ c ］に入れる適切な字句を，解答群の中から選べ。

a に関する解答群

ア (案 1)，(案 2)
イ (案 1)，(案 2)，(案 3)
ウ (案 1)，(案 2)，(案 4)
エ (案 1)，(案 3)
オ (案 1)，(案 3)，(案 4)
カ (案 1)，(案 4)
キ (案 2)，(案 3)
ク (案 2)，(案 3)，(案 4)
ケ (案 2)，(案 4)
コ (案 3)，(案 4)

b に関する解答群

ア (案 5)
イ (案 5)，(案 7)
ウ (案 5)，(案 8)
エ (案 6)
オ (案 6)，(案 7)
カ (案 6)，(案 8)
キ (案 7)
ク (案 8)

c に関する解答群

ア (案 9)，(案 10)
イ (案 9)，(案 10)，(案 11)
ウ (案 9)，(案 10)，(案 12)
エ (案 9)，(案 11)
オ (案 9)，(案 11)，(案 12)
カ (案 9)，(案 12)
キ (案 10)，(案 11)
ク (案 10)，(案 11)，(案 12)
ケ (案 10)，(案 12)
コ (案 11)，(案 12)

(2) 本文中の下線①について，W 氏がログを抽出した条件はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　1日の入室ログ件数と退室ログ件数が異なる従業員のログ

イ　従業員の入室権限がなく，入れなかったことを示すログ

ウ　入室ログの後，1時間以上退室ログがない従業員のログ

エ　別の従業員の入室ログから1秒以内に入室している従業員のログ

(3) 本文中の下線②～⑤は，それぞれ，リスク対応のどれに相当するか。解答群のうち，最も適切なものを選べ。

②～⑤に関する解答群

ア　リスク回避　　イ　リスク共有

ウ　リスク集約　　エ　リスク認知

オ　リスク発生可能性の低減　　カ　リスク保有

設問2　本文中の［ d1 ］～［ d4 ］に入れる，次の (i) ～ (iv) の組合せはどれか。d に関する解答群のうち，適切なものを選べ。

(i)　RFID 認証式の錠

(ii)　シリンダ錠

(iii)　プッシュボタン式の暗証番号錠

(iv)　指静脈認証錠

d に関する解答群

	d1	d2	d3	d4
ア	(i)	(ii)	(iii)	(iv)
イ	(i)	(ii)	(iv)	(iii)
ウ	(i)	(iii)	(iv)	(ii)
エ	(i)	(iv)	(iii)	(ii)
オ	(ii)	(i)	(iii)	(iv)
カ	(ii)	(i)	(iv)	(iii)
キ	(ii)	(iii)	(i)	(iv)
ク	(ii)	(iii)	(iv)	(i)
ケ	(ii)	(iv)	(i)	(iii)
コ	(ii)	(iv)	(iii)	(i)

設問3　表 3 中の［　e　］～［　h　］に入れる字句はどれか。解答群のうち，最も適切なものを選べ。

e～h に関する解答群

ア　入り口の外にロッカーを設置し，私物をそこに預け，業務上必要な物だけを透明なバッグに入れて執務室に出入りするようにする。

イ　コールセンタ内での記憶媒体の使用を禁止する。

ウ　出入口に警備員を配置し，入館証チェックや持ち物チェックを行う。

エ　ネックストラップ式の入館証をコールセンタ要員に貸与し，着用させる。

オ　ノート PC の画面にプライバシフィルタを装着する。

カ　ノート PC をセキュリティケーブルで机に固定する。

キ　ホスト型侵入検知装置（HIDS）を設置する。

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

6. 退室可能時間に途中で退室する場合には，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	13:10 ～ 13:50

7. **問題に関する質問にはお答えできません。**文意どおり解釈してください。
8. 問題冊子の余白などは，適宜利用して構いません。ただし，問題冊子を切り離して利用することはできません。
9. 試験時間中，机上に置けるものは，次のものに限ります。

   なお，会場での貸出しは行っていません。

   受験票，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（時計型ウェアラブル端末は除く。アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬

   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
12. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。