SG

平成29年度　秋期
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。

秋の情報処理技術者試験は，［ a ］月に実施される。

解答群　ア 8　イ 9　ウ 10　エ 11

適切な字句は“ウ 10”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　情報セキュリティリスクアセスメントに関する次の記述を読んで，設問 1～3 に答えよ。

D 社は，資本金 1 億円，従業員数 1,000 名の中堅機械製造会社であり，精密機械の設計，製造，販売を行っている。経営企画部，人事総務部，情報システム部など管理部門の従業員数は 120 名である。

D 社では，3 年前に最高情報セキュリティ責任者（CISO）を委員長とする情報セキュリティ委員会を設置し，情報セキュリティポリシ及び情報セキュリティ関連規程を整備した。情報セキュリティ委員会の事務局は，経営企画部が担当している。また，各部の部長は，情報セキュリティ委員会の委員，及び自部署における情報セキュリティ責任者を務め，自部署の情報セキュリティを確保し，維持，改善する役割を担っている。各情報セキュリティ責任者は，自部署の情報セキュリティに関わる実務を担当する情報セキュリティリーダを選任している。

D 社では，“情報セキュリティリスクアセスメント手順”を図 1 のとおり定めている。

・情報資産の機密性，完全性，可用性の評価値はそれぞれ 3 段階とし，表 1 のとおりとする。
・情報資産の機密性，完全性，可用性の評価値の最大値を，その情報資産の重要度とする。
・脅威及び脆弱性の評価値は 3 段階とし，表 2 のとおりとする。
・情報資産ごとに，様々な脅威に対するリスク値を算出し，その最大値を当該情報資産のリスク値として情報資産管理台帳に記載する。ここで，情報資産の脅威ごとのリスク値は，次の式によって算出する。
　リスク値＝情報資産の重要度×脅威の評価値×脆弱性の評価値
・情報資産のリスク値のしきい値を 5 とする。
・情報資産ごとのリスク値がしきい値以下であれば受容可能なリスクとする。
・情報資産ごとのリスク値がしきい値を超えた場合は，保有以外のリスク対応を行うことを基本とする。

注記　本評価手順は，JIPDEC“ISMS ユーザーズガイド-JIS Q 27001:2014（ISO/IEC 27001:2013）対応-リスクマネジメント編-”及び IPA“中小企業の情報セキュリティ対策ガイドライン（第 2.1 版）”を基に D 社が作成した。

図 1　情報セキュリティリスクアセスメント手順

表 1　情報資産の機密性，完全性，可用性の評価基準

評価値		評価基準	該当する情報の例
機密性	2	法律で安全管理措置が義務付けられている。	・個人データ ・特定個人情報（マイナンバーを含む個人情報）
	2	守秘義務の対象として指定されている。	・取引先から秘密と指定されて受領した設計図 ・取引先の公開前の新製品情報
	2	自社の営業秘密であり，漏えいすると自社に深刻な影響がある。	・自社の独自技術，ノウハウ ・取引先リスト ・特許出願前の発明情報
	1	関係者外秘情報 社外秘情報	・見積書，仕入価格など取引先や顧客との商取引に関する情報 ・社内規程，事務処理要領
	0	公開情報	・自社製品カタログ ・自社 Web サイト掲載情報
完全性	2	法律で安全管理措置が義務付けられている。	・個人データ ・特定個人情報（マイナンバーを含む個人情報）
	2	改ざんされると自社に深刻な影響，又は取引先や顧客に大きな影響がある。	・取引先の口座情報 ・顧客から製造委託された精密機械の設計図
	1	改ざんされると事業に影響がある。	・受発注情報，決済情報，契約情報
	0	改ざんされても事業に影響はない。	・廃版製品カタログデータ
可用性		a	（省略）

注記　本評価基準は，IPA“中小企業の情報セキュリティ対策ガイドライン（第 2.1 版）”を基に D 社が作成した。

表 2　脅威及び脆弱性の評価基準

評価値		評価基準
脅威	3	脅威となる事象がいつ発生してもおかしくない。
	2	脅威となる事象が年に数回程度発生するおそれがある。
	1	脅威となる事象が発生することはほとんどない。
脆弱性	3	必要な管理策を実施していない（ほぼ無防備）。
	2	必要な管理策のうち，一部の管理策を実施しているが十分でない。
	1	十分な管理策を実施している。

注記　本評価基準は，IPA“中小企業の情報セキュリティ対策ガイドライン（第 2.1 版）”を基に D 社が作成した。

〔在宅勤務の試行導入〕

D社では，従業員のワークライフバランスの実現と業務の生産性向上を目的として，在宅勤務の導入を経営会議で決定した。在宅勤務の最終利用登録者数は，全社で 100 名程度を想定している。この決定を受け，在宅勤務の労務管理上の課題抽出のために，人事総務部内で在宅勤務を 3 か月間試行することになり，人事総務部の F さんが在宅勤務推進担当に任命された。

F さんは，在宅勤務での PC 利用を，リモート接続サービスによって社内ネットワークに接続する形態とし，次の2案について検討することにした。

・案Ⅰ：業務用に会社から貸与されたノート PC（以下，NPC という）を自宅に持ち帰り，社内システムにアクセスして業務を行う。

・案Ⅱ：自宅にある個人所有の PC を使用し，社内システムにアクセスして業務を行う。

なお，NPC の会社からの持出しは NPC 利用規則によって禁止されているので，在宅勤務の開始に当たっては，当該規則の改定が必要になる。

〔在宅勤務の実現案の確認〕

F さんは，検討の進め方について，人事総務部の情報セキュリティリーダである A 主任からアドバイスを受けることにした。F さんからアドバイスを求められた A 主任は，次のとおり回答した。

A主任：在宅勤務形態は表3のとおり三つのパターンが考えられます。当社で採用する場合には，案Ⅰ，案Ⅱのどちらも［ b1 ］型か［ b2 ］型が想定されます。これらのうち，PC の紛失・盗難によるリスクがより小さいパターンは［ b2 ］型であり，［ b2 ］型を採用することが望ましいと考えます。［ b2 ］型が当社で実現可能か，情報システム部の H 課長に確認してみましょう。

表3　在宅勤務形態の三つのパターン

	オフライン持出し型	オンライン持出し型	シンクライアント型（画面転送型）
データの持出し	する	する	しない
リモート接続サービスによる社内システムへのアクセス	しない	する	する
代表的な在宅勤務作業例	・NPC にデータを入れて持ち出す。 ・USB メモリにデータをコピーして持ち出す。	・在宅勤務に使用する PC から社内システムにアクセスして作業（データの作成，ダウンロード，編集，アップロード，電子メールの送受信，グループウェアの利用など）を行う。PC にはアプリケーションソフトウェアやデータが置かれる。	・D 社内に専用サーバを設置し，そのサーバ上の仮想化されたデスクトップ環境を利用して作業（データの作成，編集，電子メールの送受信，グループウェアの利用など）を行う。PC にはアプリケーションソフトウェアやデータは置かれず，サーバ側でアプリケーションソフトウェアが実行されて，画面だけが PC に転送される。

注記1　本表は総務省“テレワークセキュリティガイドライン（第3版）”を基にA主任が作成した。
注記2　D社ではクラウドサービスの利用を禁止している。

A主任がH課長に［ b2 ］型の実現可能性について確認したところ，H課長から次の3点のコメントがあった。

・当社で［ b2 ］型を実現するためには，専用サーバ，ソフトウェアの費用が発生するので，予算の確保が必要となる。

・専用サーバ，ソフトウェアの製品選定及びシステム構築の時間も掛かることから，情報システム部としてすぐに対応することは困難である。

・在宅勤務の労務管理上の課題抽出が目的であるならば，当初は［ b1 ］型の試行でよいと考える。

〔情報セキュリティリスクの再評価〕

F さんと A 主任は，H 課長のコメントを受け，今回の在宅勤務の試行は［ b1 ］型で検討を行うことにした。

A 主任は，在宅勤務の試行に際し，情報セキュリティリスクの再評価が必要と考え，人事総務部で利用する情報資産について，表 4 に示す情報資産管理台帳を F さんとともに確認することにした。

表 4　情報資産管理台帳（抜粋）

情報資産名称	備考	所管	個人情報などの有無		機密性の評価値	完全性の評価値	可用性の評価値	重要度	脅威の評価値	脆弱性の評価値	リスク値
			個人情報	特定個人情報							
従業員名簿	従業員の基本情報（税務・社会保険用）	人事総務部	有	有	c1	c2	1	c3	2	1	c4
社内規程	行動規範や判断基準を含めた社内ルール	人事総務部	無	無	1	2	1	2	2	1	4
D 社の会社情報	自社 Web サイトに掲載した会社情報	経営企画部	無	無	d1	1	1	d2	2	2	d3

次は，F さんと A 主任の会話である。

F さん：情報資産管理台帳を見る限り，人事総務部で利用する情報資産のリスク値はしきい値以下なので，在宅勤務で利用することが可能ですよね。

A 主任：現状のリスク値がしきい値以下だからといって，必ずしも在宅勤務で利用可能というわけではありません。今回のように利用環境が変わる場合をはじめ，①リスク値が変化する場合もあります。十分な管理策が施された社内での NPC の使用とは異なり，在宅勤務には特有の脅威があります。一般的な在宅勤務における脅威と脆弱性を，表 5 にまとめたので，これを基に案Ⅰと案Ⅱそれぞれの場合についてリスク値を再評価しましょう。

表5　在宅勤務における脅威と脆弱性（抜粋）

脅威		脆弱性
脅威α	情報消失・漏えいにつながるPCの紛失・盗難	・移動時のPCの紛失・盗難によるリスクについての認識不足 ・［ e1 ］の未実施
脅威β	悪意あるソフトウェアによる攻撃	・②利用者による許可されていないソフトウェアのインストールが可能 ・③利用者による不正サイトへのアクセスが可能

注記　本表は，総務省“テレワークセキュリティガイドライン（第3版）”を基にA主任が作成した。

A主任：案Iの場合に，表4中の情報資産“社内規程”について，表5中の脅威αに対するリスク値を算出してみましょう。在宅勤務でNPCを自宅に持ち帰る途中で紛失・盗難に遭うこともあるので，脅威αの評価値は2とします。現状の対策については，当社の本社及び各事業所ではICカードによる入退室管理を行っており，かつNPCはケーブルロックによって固定する［ e2 ］も行っているので，対策は十分と考えて［ e1 ］は実施していません。NPCでは，④脅威αによるリスクに有効な幾つかの技術的対策を行っていますが，紛失・盗難の状況下では第三者によって情報が取り出されるおそれがあります。このため，必要な管理策のうち一部の管理策だけを実施していると判断されますので，脅威αに対する脆弱性の評価値を1から2に見直すとリスク値は8となり，しきい値を超えてしまいます。

Fさん：どのように対応すべきでしょうか。

A主任：この場合は［ f1 ］に当たる［ e1 ］を行うべきです。現在NPCで使用しているOSでは標準機能で［ e1 ］をサポートしているので，新たなソフトウェア・ハードウェアは不要です。［ f2 ］などの人的対策を行った上で，［ e1 ］を行えば，脆弱性の評価値は1と判断してよいでしょう。再度算出するとリスク値は4となり，しきい値内に収まります。

Fさん：脆弱性の評価において，管理策の十分性はどのように判断するのですか。

A主任：管理策の十分性の判断は，評価者によってばらつきが出るおそれがあるので配慮が必要です。

ここで，A主任は，管理策の十分性の判断にばらつきが出ないようにするD社での⑤解決策を説明した。

Fさん：分かりました。ところで，案Ⅰと案Ⅱの間で情報セキュリティ上，考慮すべき点に違いはありますか。

A主任：案Ⅰで使用する NPC は，脅威βに対しても，幾つかの管理策を実施しています。また，ソフトウェア構成やハードウェア構成も統制しています。一方，案Ⅱで使用する自宅にある個人所有の PC の場合は，どのような管理策を実施しているのか，また，OS のバージョンを含めたソフトウェア構成やハードウェア構成がどうなっているのかについて会社が統制することはできないという点を考慮する必要があります。

A 主任の協力によって F さんは無事に情報セキュリティリスクの再評価を終え，しきい値を超えないことが確認できたので今回の在宅勤務の試行は案Ⅰで行うことにした。

情報セキュリティリスクの再評価結果は情報セキュリティ委員会で承認され，在宅勤務の試行が開始された。

設問1　表1中の［　a　］に記載する評価値及び評価基準はどれか。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

評価値	評価基準
2	多くの人に長期間悪いイメージが残り，自社に深刻な影響，又は取引先や顧客に大きな影響がある。
1	限定された人に長期間悪いイメージが残り，事業に影響がある。
0	ほとんど事業に影響がない。

イ

評価値	評価基準
2	人手による代替が可能であり，事業に影響はない。
1	人手による代替が一部可能であるが，事業に影響がある。
0	人手による代替は不可能であり，自社に深刻な影響，又は取引先や顧客に大きな影響がある。

ウ

評価値	評価基準
2	人手による代替は不可能であり，自社に深刻な影響，又は取引先や顧客に大きな影響がある。
1	人手による代替が一部可能であるが，事業に影響がある。
0	人手による代替が可能であり，事業に影響はない。

エ

評価値	評価基準
2	ほとんど事業に影響がない。
1	限定された人に長期間悪いイメージが残り，事業に影響がある。
0	多くの人に長期間悪いイメージが残り，自社に深刻な影響，又は取引先や顧客に大きな影響がある。

オ

評価値	評価基準
2	利用できなくなっても事業に影響はない。
1	利用できなくなると事業に影響がある。
0	利用できなくなると自社に深刻な影響，又は取引先や顧客に大きな影響がある。

カ

評価値	評価基準
2	利用できなくなると自社に深刻な影響，又は取引先や顧客に大きな影響がある。
1	利用できなくなると事業に影響がある。
0	利用できなくなっても事業に影響はない。

設問2　本文中の［ b1 ］，［ b2 ］に入れる字句の組合せはどれか。b に関する解答群のうち，適切なものを選べ。

bに関する解答群

	b1	b2
ア	オフライン持出し	オンライン持出し
イ	オフライン持出し	シンクライアント
ウ	オンライン持出し	オフライン持出し
エ	オンライン持出し	シンクライアント
オ	シンクライアント	オフライン持出し
カ	シンクライアント	オンライン持出し

設問3　〔情報セキュリティリスクの再評価〕について，(1) ～ (8) に答えよ。

(1)　表 4 が，図 1 に従って記載されている場合，［ c1 ］～［ c4 ］，［ d1 ］～［ d3 ］に入れる数値の組合せはどれか。c，d に関する解答群のうち，適切なものを選べ。

c に関する解答群

	c1	c2	c3	c4
ア	1	1	1	2
イ	1	1	2	4
ウ	1	2	2	2
エ	1	2	2	4
オ	2	2	2	2
カ	2	2	2	4

d に関する解答群

	d1	d2	d3
ア	0	0	2
イ	0	1	0
ウ	0	1	4
エ	1	1	4
オ	1	2	4
カ	2	2	4

(2) 次の (i) ～ (iii) のうち，図 1 の適用において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) 重要度が 0 の情報資産であっても，部分的な管理策を必ず実施しなければならない。

(ii) 重要度が 1 の情報資産の，評価値が 1 の脅威に対しては，そのリスクを受容できる。

(iii) 重要度が 2 の情報資産の，評価値が 1 の脅威に対しては，必要な管理策のうち，一部の管理策を実施するだけでは不十分なので，必要な管理策を全て実施する必要がある。

解答群

ア (i)　　イ (i), (ii)

ウ (i), (ii), (iii)　　エ (i), (iii)

オ (ii)　　カ (ii), (iii)

キ (iii)　　ク 全て適切ではない

(3) 本文中の下線 ① について，次の (i) ～ (iv) のうち，リスク値が変化する可能性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) OS に深刻な脆弱性が発見され，セキュリティパッチの適用までに時間が掛かる場合

(ii) 使用している暗号アルゴリズムが危たい化した場合

(iii) 取引先から秘密と指定されて受領した情報が，一般に公開され，取引先によって秘密の指定が解除された場合

(iv) 標的型攻撃メールが急増した場合

解答群

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

ウ (i)，(ii)，(iv)　　エ (i)，(iii)，(iv)

オ (i)，(iv)　　カ (ii)，(iv)

キ (iii)，(iv)

(4) 表 5 及び本文中の [e1]，並びに本文中の [e2] に入れる字句の組合せはどれか。e に関する解答群のうち，適切なものを選べ。

e に関する解答群

	e1	e2
ア	OS のアップデート	技術的対策
イ	ウイルス対策ソフトの導入	物理的対策
ウ	セキュリティパッチの適用	技術的対策
エ	ハードディスクドライブ全体の暗号化	技術的対策
オ	ハードディスクドライブ全体の暗号化	物理的対策

(5) 表 5 中の下線②及び下線③について，次の (i) ～ (ix) のうち，脆弱性の低減に有効な管理策だけを全て挙げた組合せを，解答群の中から選べ。

(i) CDN（コンテンツデリバリネットワーク）サービスの導入

(ii) IT 資産管理ソフトウェアによる構成情報の自動収集と管理

(iii) MAC アドレスフィルタリングの実施

(iv) URL フィルタリングの実施

(v) 生体認証の導入

(vi) 特権 ID 管理ツールの導入

(vii) パスワードの定期的な変更

(viii) 利用者アカウントに付与されている管理者権限の剥奪

(ix) リバースプロキシの設置

解答群

ア (i), (ii), (iii), (iv), (ix)

イ (i), (ii), (iv), (vi), (vii)

ウ (ii), (iii), (iv), (v), (ix)

エ (ii), (iii), (iv), (v), (vi)

オ (ii), (iv), (viii)

カ (iii), (vi), (vii), (ix)

キ (iii), (vi), (viii), (ix)

ク (iv), (v), (vii)

ケ (iv), (v), (vii), (ix)

コ (v), (vii), (viii)

(6) 本文中の下線④について，次の(i)～(v)のうち，技術的対策として有効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) NPC利用時の利用者認証

(ii) ウイルス対策ソフトの導入及び最新の定義ファイルの適用

(iii) 在宅勤務利用規則の整備

(iv) 誓約書の提出

(v) データバックアップの実施

解答群

ア (i)

イ (i)，(ii)，(v)

ウ (i)，(iii)，(iv)

エ (i)，(iii)，(iv)，(v)

オ (i)，(v)

カ (iii)，(iv)，(v)

(7) 本文中の［ f1 ］，［ f2 ］に入れる字句の組合せはどれか。f に関する解答群のうち，最も適切なものを選べ。ここで，設問3(4)の［ e1 ］には適切な字句が入っているものとする。

f に関する解答群

	f1	f2
ア	リスクの回避	監査
イ	リスクの回避	パスワード管理
ウ	リスクの共有	入退室管理
エ	リスクの低減	教育
オ	リスクの低減	入退室管理
カ	リスクの保有	アクセス制御

(8) 本文中の下線 ⑤ について，次の (i) ～ (vi) 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) 各脆弱性の評価を複数の評価者が行い，結果を調整している。

(ii) 管理策の数をそろえている。

(iii) しきい値を超えるリスク値が存在する場合，CISO が当該リスクの受容を承認している。

(iv) 情報資産ごとに，しきい値を設けている。

(v) 評価者に対して，評価についての教育，訓練を実施している。

(vi) リスク値を客観的に算定するための基準を設けている。

解答群

ア (i)，(ii)

イ (i)，(ii)，(iii)，(v)

ウ (i)，(iv)，(vi)

エ (i)，(v)，(vi)

オ (i)，(vi)

カ (iii)，(iv)

キ (iii)，(iv)，(v)

ク (iii)，(v)，(vi)

問2　Web サービスでの Web アプリケーションソフトウェア開発委託に関する次の記述を読んで，設問1～4に答えよ。

P 社は，従業員数 1,200 名の大学受験及び高校受験のための大手予備校である。先日開催した経営会議において，次年度から中学受験向けコースの事業部（以下，C 事業部という）を新たに立ち上げることが決まり，現在，開講に向けた準備作業を進めている。C 事業部は，教務部，営業部，総務部，マーケティング部の計 4 部で構成され，マーケティング部は，市場調査，広報活動，外部公開の Web サービスの企画，導入，運用などを担当している。

〔情報セキュリティ管理規程〕

P 社の情報セキュリティ管理規程では，次を規定している。

・情報セキュリティ委員会は，最高情報セキュリティ責任者（CISO）と各事業部の事業部長，各部の部長によって構成される。
・情報セキュリティ委員会は，P 社の情報セキュリティに関する意思決定を行う。
・上記の意思決定には，“暫定策を適用する際のリスク評価結果や残留リスクの承認”，“リスク評価結果などを踏まえた，新規事業又はサービスの開始の可否判断”などを含む。
・各部には，情報セキュリティの推進者として情報セキュリティリーダを配置する。

〔情報セキュリティの重点方針〕

現在，P 社の CISO は，情報セキュリティ活動を推進し情報を守ることと，情報を活用しビジネスを成長させることの両立が必要不可欠であると考えている。そこで，P 社の情報セキュリティの重点方針として，“個人情報の漏えい防止”と“Web サービスの継続性確保”の 2 点を定めて，情報セキュリティ委員会のメンバに通知している。

〔Web サービスの仕様〕

C 事業部のマーケティング部では，模擬試験の結果速報，成績推移などを，P 社の中学受験向けコースに通う児童（以下，児童という），及び児童の保護者（以下，保

護者という）が閲覧できるように，ログイン機能を有した Web サービス（以下，W サービスという）を Web アプリケーションソフトウェア（以下，Web アプリという）として開発し，提供することを検討している。マーケティング部の N さんは，W サービスの企画を担当している。図 1 は，N さんが作成した W サービスの仕様案である。

1. サービスメニューの概要
(1) 模擬試験の結果速報
(2) 成績推移
(3) 料金の自動引落し明細
2. 認証機能
(1) ログイン
　任意に設定できる英数字の利用者 ID と数字 4 桁の児童用パスワードを使用してログインする。
(2) アカウントロック
　5 回連続してログインに失敗すると，1 分間，アカウントをロックする。
(3) 保護者用パスワードによる追加ログイン
　料金の自動引落し明細メニューにアクセスするためには英数記号 8 文字以上の保護者用パスワードによる追加ログインを必要とする。
(4) ログアウト
　“ログアウト”ボタンをクリックするとログアウトする。“ログアウト”ボタンを押さない限り，ログインしたままとする。
(5) パスワードの表示
　児童用パスワードも保護者用パスワードも，パスワード入力内容の表示，非表示を切り替えられるようにする。初期状態は，非表示とする。

図 1　W サービスの仕様案（抜粋）

マーケティング部の情報セキュリティリーダである S 主任は，N さんが作成した W サービスの仕様案を情報セキュリティの観点からレビューした。

次は，S 主任と N さんとの会話である。

S 主任 ：模擬試験の結果などが児童本人及びその保護者以外に閲覧されるリスク（以下，閲覧リスクという）を減らすために，W サービスはログイン機能を実装することになっていたね。

N さん：はい。児童でも覚えやすい数字 4 桁のパスワードを用いる仕様です。

S 主任 ：料金の自動引落し明細メニューのログインについても教えてくれないか。

Nさん：こちらは，保護者がアクセスします。児童が閲覧する必要はないことから，英数記号 8 文字以上の保護者用パスワードで追加ログインする仕様です。また，パスワードの入力間違いを減らすために，保護者がパスワード入力内容を表示に切り替えて，入力内容を確認することができます。

S主任：よく分かった。この仕様案では，ブルートフォース攻撃のリスクが大きいね。また，児童の場合，自分専用の PC をもっているケースは少ないと思うよ。図書館，学校などの共用 PC を利用することが多く，そこでログアウトを忘れることもあるので，閲覧リスクが大きいね。

S主任は，レビュー後に，次の2点の変更，追加をNさんに指示した。

・① ブルートフォース攻撃のリスクを低減するために認証機能の仕様を変更する。

・② 共用 PC における閲覧リスクを低減するために機能を追加する。

〔委託仕様書の検討〕

近年，Web アプリの脆弱(ぜい)性を悪用した攻撃が増えている。脆弱性の代表的な例としては，SQL インジェクションやクロスサイトスクリプティングが知られている。

S 主任は，Web アプリの開発を外部に委託するに当たり，情報システム部の U 課長に相談し，委託仕様書は IPA が公開している“ウェブ健康診断仕様”を参考にすることにした。また，検収の際はセキュリティ専門会社の Y 社に脆弱性診断を依頼することにした。“ウェブ健康診断仕様”とは，元々は地方公共団体が運営する Web サイトの基本的な対策状況を診断するための仕様であり，低コストで診断できるように，必要かつ最小限の診断項目，検査パターンを採用している。したがって，Web アプリの一般的な脆弱性診断サービスと比較すると簡素な診断項目となっている。

“ウェブ健康診断仕様”の診断項目を表1に示す。

表1　“ウェブ健康診断仕様”の診断項目（抜粋）

項番	診断項目（脆弱性名など）	危険度	受動的攻撃[1]／能動的攻撃[2]	攻撃によって影響を受ける特性[3]		
				機密性	完全性	可用性
1	SQL インジェクション	高	a1	○	○	○
2	クロスサイトスクリプティング	中	a2	○	○	
3	クロスサイトリクエストフォージェリ	中	受動的	○	○	○
4	OS コマンドインジェクション	高	能動的	○	○	○
5	意図しないリダイレクト	中	受動的	○		
6	HTTP ヘッダインジェクション	中	受動的	○	○	
7	b	低～中	能動的			○

注記　本表は，P 社の情報セキュリティ委員会が“ウェブ健康診断仕様”の内容，表現を自社向けに一部変更したものである。

注[1]　脆弱性を悪用する攻撃の成功には，攻撃者の用意した不正なリンクをクリックするなどの被害者の操作が必要である。

注[2]　脆弱性を悪用する攻撃の成功には，被害者の操作なしに，攻撃者が Web アプリに対して攻撃するだけでよい。

注[3]　○は影響を受けることを示す。

S 主任は，表 1 を基に対処の必要な脆弱性を委託仕様書に列挙した。また，③情報セキュリティを向上させる上で有効かつ適切な他の事項についても，委託仕様書に盛り込み，情報システム部のレビューを受けてから，開発会社の Z 社に Web アプリの開発を委託した。

〔脆弱性診断結果〕

3 か月後，S 主任は，Z 社が開発した Web アプリの検収に当たって，Y 社に脆弱性診断を依頼した。Y 社の脆弱性診断では，情報処理安全確保支援士が，“ウェブ健康診断仕様”に比べて診断項目が多い詳細な診断を実施する。

Y 社の診断での“危険度基準”を表 2 に，“総合判定基準”を表 3 に示す。

表2　危険度基準

危険度	内容
高	能動的攻撃が成功する可能性が高く，機密性や完全性の被害につながりやすい脆弱性がある。
中	受動的攻撃が成功する可能性が高い脆弱性がある。 又は，機密性や完全性の被害にはつながりにくいものの，能動的攻撃が成功する可能性が高い脆弱性がある。
低	攻撃成功の可能性が低い脆弱性がある。 又は，攻撃が成功しても被害が軽微であると考えられる脆弱性がある。

注記　本表は，“ウェブ健康診断仕様”を基に，Y社が脆弱性診断の評価基準として作成した。

表3　総合判定基準

総合判定所見	説明
要治療・精密検査（優先度：高）	危険度が“高”の脆弱性が検出された。直ちに Web アプリの改修などの措置を講じる必要がある。
要治療・精密検査（優先度：通常）	危険度が“中”の脆弱性が検出された。Web アプリの改修などの措置を講じる必要がある。
差し支えない	危険度が“低”の脆弱性が検出された。Web アプリの改修などの措置を講じることが望ましい。
異常検出なし	脆弱性は検出されなかった。

注記　本表は，“ウェブ健康診断仕様”を基に，Y社が脆弱性診断の評価基準として作成した。

Y社が Web アプリの脆弱性診断を行ったところ，［　c　］検出されたので，総合判定所見は，“要治療・精密検査（優先度：高）”であった。

次は，診断報告会でのS主任とY社の診断担当T氏との会話である。

S主任：脆弱性診断で脆弱性が検出された場合，Web アプリを改修する以外の代替手段はあるのですか。

T氏　：WAF を導入することによって，パラメタ操作による攻撃などを防御することができます。ただし，認証やセッション管理の不備を悪用する攻撃の中には，防御できない攻撃もあるので，WAF は，Web アプリに対する攻撃によるリスクを低減するための対策と考えてください。

S主任：なるほど，対策として不十分なので，Web アプリを改修するよりも残留リスクが大きくなるのですね。それでは，Web アプリを改修する場合であれば，WAF の導入は不要ですか。

T氏　：いいえ，そうとも限りません。Web アプリの改修が完了するまでの間，Web サービスを停止する代わりに，④ WAF を暫定策として活用することも可能です。

S主任：分かりました。Web アプリの情報セキュリティ対策では他にも注意すべきことはありますか。

T氏　：Web アプリの脆弱性を突く攻撃とは別に，パスワードリスト攻撃のような利用者側の管理面の脆弱性を突く攻撃が，最近，増えています。

S主任は，今回の脆弱性診断で検出された脆弱性については，Z社に対して Web アプリの改修を求めることにした。また，パスワードリスト攻撃については，⑤児童や保護者に対する注意喚起を行うために，児童にも分かりやすい情報セキュリティのしおりを作成し，配布することにした。

Z社は，Web アプリを改修した上でP社に納品した。数日後，S主任は，W サービス開始に向けて情報セキュリティ委員会に報告した。

〔W サービス開始とその後〕

情報セキュリティ委員会には，脆弱性診断結果と，その後の Web アプリの改修対応が報告され，W サービス開始に向けて問題ないと判断された。情報セキュリティ委員会の終了後，S主任は，情報システム部に対して，W サービス提供開始後に新たな脆弱性が発見される可能性，及び，⑥P 社の情報セキュリティの重点方針を実現する上で WAF 導入によって期待できるメリットを説明した。情報システム部は，WAF を導入することを決定し，その後，C事業部の W サービスは，予定どおりサービス提供を開始した。

W サービスの提供開始から数か月後，S主任は，Z社に対して，⑦パスワードリスト攻撃などによる不正ログインの発生状況に利用者側でも気付くための機能などの追加を依頼した。

その結果，P社は W サービスをより安全に提供することができるようになった。

設問1　〔Webサービスの仕様〕について，(1)，(2)に答えよ。

(1)　本文中の下線①の仕様変更について，Wサービスの仕様案よりもリスクを低減できる変更内容を，解答群の中から二つ選べ。

解答群

ア　児童用パスワード及び保護者用パスワードの入力内容を，常に非表示にするように変更する。

イ　児童用パスワードを，数字4桁から英数記号8文字以上に変更する。

ウ　保護者用パスワードを，英数記号8文字以上から数字9桁に変更する。

エ　ログイン失敗回数によるアカウントロックのしきい値を，5回から8回に変更する。

オ　ログイン失敗時のアカウントロック時間を，1分間から60分間に変更する。

(2)　本文中の下線②について，追加すべき機能はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　アカウントロックを利用者が自ら解除できる機能の追加

イ　定期的なパスワード変更を利用者に促すメッセージ機能の追加

ウ　パスワード強度をチェックする機能の追加

エ　パスワードを忘れた際に使う利用者への“秘密の質問”機能の追加

オ　マルウェア検知機能の追加

カ　ログイン状態をタイムアウトさせる機能の追加

設問2　〔委託仕様書の検討〕について，(1) ～ (3) に答えよ。

(1)　表 1 中の［ a1 ］，［ a2 ］に入れる字句はどれか。a に関する解答群のうち，最も適切なものを選べ。

a に関する解答群

	a1	a2
ア	受動的	受動的
イ	受動的	能動的
ウ	能動的	受動的
エ	能動的	能動的

(2)　表 1 中の［ b ］に入れる字句を，解答群の中から選べ。

b に関する解答群

ア　クローラへの耐性

イ　セッション管理の不備

ウ　ディレクトリトラバーサル

エ　ディレクトリリスティング

オ　認可制御の不備，欠落

(3) 本文中の下線③について，次の(i)～(v)のうち，有効かつ適切な事項だけを全て挙げた組合せを，解答群の中から選べ。

(i) 開発を進めていくうちに，追加のセキュリティ対策が必要なものが発生した場合，委託元に提案すること

(ii) 再委託先も含めたセキュアな開発体制を，委託元に説明すること

(iii) 脆弱性観点からのセキュリティ試験結果を，委託元に成果物として納品すること

(iv) 他社のセキュリティ開発案件で顧客から受領した委託仕様書を，委託元に開示すること

(v) 納品後のセキュリティに関するサポート方法と費用負担を，委託元に説明すること

解答群

ア (i), (ii), (iii), (iv)

イ (i), (ii), (iii), (iv), (v)

ウ (i), (ii), (iii), (v)

エ (i), (ii), (iv), (v)

オ (i), (ii), (v)

カ (i), (iii), (iv), (v)

キ (i), (iv), (v)

ク (ii), (iii), (iv)

ケ (ii), (iii), (iv), (v)

コ (iii), (iv), (v)

設問３　〔脆弱性診断結果〕について，(1) ～ (3) に答えよ。

(1) 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　“HTTP ヘッダインジェクション”の脆弱性が，１件

イ　“OS コマンドインジェクション”の脆弱性が，１件

ウ　“クロスサイトリクエストフォージェリ”の脆弱性が，１件

エ　“クロスサイトリクエストフォージェリ”の脆弱性と“意図しないリダイレクト”の脆弱性が，それぞれ１件

オ　攻撃が成功しても被害が軽微であると考えられる脆弱性が，３件

カ　攻撃成功の可能性が低い脆弱性が，１件

(2) 本文中の下線④について，P 社の情報セキュリティ管理規程と照らし合わせると，どのような対応が必要になるか。解答群のうち，最も適切なものを選べ。

解答群

ア　C 事業部の営業部による，W サービスを停止させるかどうかという業務観点からの判断

イ　WAF 提供元による，リスク回避の観点からの WAF 設定などの技術的なアドバイス

ウ　情報セキュリティ委員会による，リスク対応の観点からの承認

エ　使いやすさや画面の見やすさの観点からの児童の意見の聴取

オ　保護者による，個人の権利利益保護の観点からの同意

(3) 本文中の下線⑤について，注意喚起すべき内容はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　他のWebサイトと同じ利用者IDとパスワードを使わないこと

イ　パスワードを定期的に変更すること

ウ　パスワードを変更した直後に再変更はしないこと

エ　パスワードを忘れた場合に備えて，周りの友達とパスワードを共用すること

オ　パスワードを忘れないように，パスワードをメモして安全な場所に保管すること

カ　利用できる全ての文字種を組み合わせ，可能な限り複雑なパスワードを設定すること

設問4　〔Wサービス開始とその後〕について，(1)，(2)に答えよ。

(1) 本文中の下線⑥のメリットはどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　Webアプリ改修期間中のサービス中断を回避することができる。

イ　Webアプリの改修を一切不要にすることができる。

ウ　保護者などに対外的なアピールをすることができる。

エ　マルウェアによる個人情報の漏えいを防止することができる。

オ　レスポンスを向上させることができる。

(2) 本文中の下線⑦について，追加すべき機能はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　2要素認証

イ　休眠アカウントの無効化

ウ　推測可能なパスワードの設定禁止

エ　特定のIPアドレスからの通信遮断

オ　認証エラーに対するアカウントロック

カ　パスワードの有効期間設定

キ　パスワード履歴保存と現在と同じパスワードの再設定禁止

ク　普段と異なるIPアドレスからの通信遮断

ケ　ログイン履歴の表示

問3　スマートデバイスの業務利用における情報セキュリティ対策に関する次の記述を読んで，設問1，2に答えよ。

J社は，従業員数150名の消費者向け化粧品販売会社である。J社は，自社で構築したECサイトを通して商品を販売している。J社には営業企画部，情報システム部，人事総務部，ロジスティック部などがある。

J社では，情報セキュリティ委員会（以下，委員会という）を毎月末に開催しており，最高情報セキュリティ責任者（CISO）が委員長を，各部の部長が委員を務めている。各部の部長は，自部署の情報セキュリティ責任者を兼ねている。また各部には，情報セキュリティの推進者として，情報セキュリティリーダを配置している。委員会では，情報セキュリティ関連規程の整備，情報セキュリティ対策の強化などが検討される。CISOは，委員会に提案する規程，マニュアル，対策などは提案前に十分に検証するように提案者に指示している。

J社は，取引先訪問中など，いつでも，どこでも仕事ができる制度（以下，モバイルワークという）を，主に営業企画部の従業員を対象に，1年前から導入している。営業企画部のモバイルワークは，営業企画部の情報セキュリティリーダであるR課長が中心となって管理することになっており，情報システム部のG主任がモバイルワークのシステム運用担当者（以下，運用担当者という）として支援している。

現在，モバイルワークを利用する従業員（以下，モバイルワーカという）は20名おり，モバイルワークについて改善点や問題点などを発見した場合は，R課長に連絡することになっている。J社はモバイルワーク用に許可した機器（以下，モバイル端末という）としてノートPCを一人1台貸与している。

モバイルワーク利用規程を図1に，モバイルワークで使用が認められているソフトウェア及びその用途を表1に示す。

・モバイルワークの利用を希望する従業員は，モバイル端末利用申請書に必要事項（所属部門，従業員 ID，従業員氏名，申請理由，モバイルワーク利用期間）を記入し，所属部門長の承認を得た後，情報システム部に提出すること
・モバイルワーカは，モバイル端末のセキュリティ設定のうち，情報システム部が指定したものを変更しないこと
・モバイルワーカは，モバイル端末で社外から内部ネットワーク及びインターネットにアクセスする場合，会社が用意した VPN 経由で VPN サーバに接続し，自らの利用者アカウントを用いてログインすること
・モバイルワーカは，業務データをモバイル端末に保存したままにせずに，内部ネットワークのファイルサーバに保存すること
・モバイルワーカは，取引先とのファイル共有に会社が用意したファイル共有サービスだけを使用すること
・モバイルワーカは，モバイル端末を紛失した場合，速やかに運用担当者に連絡すること
・運用担当者は，モバイルワーク利用期間が終了したモバイル端末を速やかに初期化すること

図 1　モバイルワーク利用規程（抜粋）

表 1　モバイルワークで使用が認められているソフトウェア及びその用途

ソフトウェア	提供元	用途
電子メールソフト	B 社	・社内及び社外の関係者との業務連絡
オフィスソフト	B 社	・データの集計や分析，報告書などの資料作成
Web ブラウザ	B 社	・業務での Web サイトへのアクセス及び会社が用意したファイル共有サービスの利用

J 社では，取引先や社外の関係者とのファイル共有のために B 社のファイル共有サービスを用意している。B 社のファイル共有サービスは法人向けのクラウドサービスである。モバイルワーカが社外からインターネットにアクセスする場合は，必ず J 社の DMZ 上の VPN サーバからプロキシサーバを経由してアクセスする。プロキシサーバには利用者認証機能はあるが，その機能は現在使用していない。一方，J 社からインターネット上の Web サイト及びファイル共有サービスへのアクセスは，ホワイトリスト方式によって制御している。B 社のファイル共有サービスには，アクセス元に対する IP アドレス制限機能が実装されているが，その機能は現在使用していない。

営業企画部は，モバイルワーカを対象にモバイルワークに関する満足度調査を実施した。調査では，ノート PC は大きく重いのでスマートフォンやタブレット（以下，スマートデバイスという）に替えてほしいという要望が多かった。また，他社では個人所有のスマートデバイスを業務で活用することによって業務の生産性が向上したという事例があるので，併せて検討してほしいという要望もあった。

〔情報セキュリティ上のリスクと対策〕

営業企画部の情報セキュリティ責任者である K 部長は，スマートデバイスを人数を限定して試験的に利用させることにし，スマートデバイスの利用案を G 主任と検討して，報告するよう R 課長に指示した。

利用案の検討に当たり，G 主任は，スマートデバイスの一般的な機能を図 2 のとおりまとめた。G 主任は R 課長に，モバイルワークで使用する表 1 のソフトウェアはスマートデバイス用のアプリケーションソフトウェア（以下，アプリという）としても B 社から提供されている（以下，B 社から提供されているアプリを B 社アプリという）と伝えた。

a) ネットワーク接続
・無線 LAN 又は携帯電話網を利用できる。
b) アプリの利用
・アプリを配布するマーケット [1]（以下，アプリストアという）からアプリを選んでスマートデバイスに導入できる。
c) 記憶媒体へのデータ保存
・内蔵されている記憶媒体（以下，内部記憶媒体という）にアプリや写真などのデータを保存できる。
・機種によっては，データをマイクロ SD カードなどの外部記憶媒体にも保存できる。
d) SIM カードの使い分け
・機種によっては，携帯電話事業者の SIM カードを使い分けることができる。

注 [1] マーケットは，スマートデバイスの OS ベンダなどが運用している。それらの中には，アプリの安全性審査を行っていないところがある。

図 2　スマートデバイスの一般的な機能（抜粋）

R 課長がスマートデバイスの利用案をまとめ，K 部長に報告したところ，モバイルワークにスマートデバイスを利用した場合の情報セキュリティ上のリスクと対策についても検討し，報告するよう指示を受けた。

早速，R 課長と G 主任は，リスクと対策案を表 2 のとおりまとめ，さらに R 課長は G 主任に，表 2 の対策を実現する方法を調査するよう依頼した。

表2　モバイルワークにスマートデバイスを利用した場合のリスクと対策案（抜粋）

リスク	対策案（J社で実施中の対策を含む）
モバイルワーカ以外によるスマートデバイスの不正利用及び内部ネットワークへの侵入	・スマートデバイスのロック[1)]を解除するためのパスワードを設定・変更 ・［　a　］
スマートデバイスの紛失・盗難による情報漏えい及び消失	・紛失・盗難時に，スマートデバイスを遠隔操作で運用担当者がロック ・紛失・盗難時に，スマートデバイスの内部記憶媒体及びスマートデバイスに装着している外部記憶媒体の全領域を遠隔操作で運用担当者が初期化 ・［　b　］
通信内容の盗聴及び改ざん	（省略）
スマートデバイスのマルウェア感染	・OS及びアプリの最新版を利用 ・マルウェア対策用のアプリを導入 ・J社が指定したWebサイトにだけアクセス ・J社が指定したアプリだけを使用 ・［　c　］
知識不足による誤操作	・［　d1　］ ・［　d2　］
①利用者による OS の改造（Jailbreak，root 化など）	・OSの改造の禁止をモバイルワーク利用規程に追加

注記　リスクに対して複数の対策案が示されている場合は，全て行うことを意味する。

注[1)]　スマートデバイスのロックとは，パスワードなどによって認証されないとスマートデバイスの操作ができないようにする機能のことである。

〔対策の実現に向けた調査〕

G主任が調査したところ，表2の対策を実現する上で利用可能な機能をもつクラウドサービスが複数のベンダから提供されていた。G主任はその中でも，市場シェアが高いE社のクラウドサービスMM1及びMM2を対策の候補とし，それぞれが提供している機能を図3のとおりまとめ，R課長に報告した。

1. MM1 の機能
 1-1 自動で実行される機能
  ・端末データ（電話番号，国際移動体装置識別番号 [1]，機種名，位置情報，OS 名及びバージョン，並びに導入済みの全てのアプリの名称及びバージョン）の収集
  ・スマートデバイスの内部記憶媒体及びスマートデバイスに装着されている外部記憶媒体の全領域の暗号化
  ・OS 改造の検知
 1-2 管理画面 [2] 上で手動で実行できる機能
  ・スマートデバイスのロック
  ・スマートデバイスのロックを解除するためのパスワード設定・変更
  ・アクセスできる Web サイト及び導入できるアプリの制限
  ・スマートデバイスの内部記憶媒体及びスマートデバイスに装着されている外部記憶媒体の全領域の初期化
  ・スマートデバイスへのアプリの配布
  ・端末データの閲覧
2. MM2 の機能
 2-1 自動で実行される機能
  ・アプリによって生成される業務データを保存するフォルダ（以下，業務フォルダという）の作成
  ・内部記憶媒体のうち，業務フォルダが使用する領域の暗号化
  ・業務フォルダ内のデータの，スマートデバイス内の業務フォルダ以外の領域への移動禁止，複製禁止
  ・端末データ（電話番号，国際移動体装置識別番号，機種名，OS 名及びバージョン，並びに業務フォルダ内のアプリの名称及びバージョン）の収集
  ・OS 改造の検知
 2-2 管理画面上で手動で実行できる機能
  ・業務フォルダにアクセスするためのパスワード設定の強制
  ・業務フォルダへのアプリの配布
  ・業務フォルダ内の初期化
  ・端末データの閲覧

注記　図中の機能は，アプリストアで提供されている E 社のエージェントアプリをスマートデバイスに導入している場合にだけ有効である。

注 [1]　国際移動体装置識別番号とは，スマートデバイスなどの情報端末ごとに割り当てられた固有の識別番号のことである。

注 [2]　管理画面とは，運用担当者がアクセスできるクラウドサービス上の Web 画面のことである。MM2 も同様である。

図 3　MM1 及び MM2 の機能（抜粋）

MM1 と MM2 の機能を比較すると，MM1 は［ e1 ］を保護対象にすることによって情報漏えいを防ぐ。MM2 は［ e2 ］を保護対象にすることによって情報漏えいを防ぐ。

R 課長は，MM1 又は MM2 を個人所有のスマートデバイスで使用する場合，幾つかの課題があることに気付いた。そこで，R 課長は G 主任の協力を得て，課題とその解決案を表 3 のとおりまとめた。

表 3　課題とその解決案

項番	課題	解決案
1	MM1 が収集した端末データを運用担当者が閲覧した場合，モバイルワーカから J 社にプライバシ侵害のクレームがある。	・委員会がモバイルワークの利用を希望する従業員に対して，運用担当者による端末データの閲覧範囲について，［ f ］。 （省略）
2	スマートデバイスの紛失・盗難時に，運用担当者が MM1 の機能を実行すると機能によっては次のいずれかが起きる。 ・［ g ］。 ・［ h ］。	（省略）
3	許可されていない個人所有のスマートデバイスが使用される。	・②モバイル端末利用申請書の一部を修正する。
4	J 社が購入した B 社アプリのライセンスが，許可されていない個人所有のスマートデバイスで使用される。	・③B 社アプリを J 社が許可した個人所有のスマートデバイスにだけ配布するという運用手順を定める。

R 課長は，G 主任と一緒に検討した案をまとめ，K 部長に報告した。

後日，検討した案は委員会で説明され，モバイルワークでのスマートデバイスの人数を限定した試験的な利用が承認された。試験的な利用はモバイルワーカに好評であり，情報セキュリティインシデントも起きていないことから，モバイルワークでのスマートデバイスの全社利用へと発展した。

設問1　〔情報セキュリティ上のリスクと対策〕について，(1)～(3)に答えよ。

(1)　表2中の［　a　］～［　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。

aに関する解答群

ア　B社のファイル共有サービスのIPアドレス制限機能を有効化

イ　VPNサーバへの接続時に利用者を認証

ウ　プロキシサーバでの利用者認証を有効化

エ　プロキシサーバのアクセス管理をブラックリスト方式に変更

bに関する解答群

ア　J社の内部ネットワークのファイルサーバに業務データを保存

イ　スマートデバイス内にフォルダを作成し，そこに業務データをバックアップ

ウ　スマートデバイスに常に装着されている外部記憶媒体に業務データをバックアップ

エ　モバイルワーカが個人で契約しているファイル共有サービスに業務データをバックアップ

cに関する解答群

ア　J社が指定したアプリストアだけを利用

イ　J社が指定した携帯電話事業者の無線LANサービスだけを利用

ウ　J社が指定した時間帯だけにアプリストアを利用

エ　J社が指定したプログラム言語だけでアプリを開発

(2) 表 2 中の［ d1 ］，［ d2 ］に入れる，次の (i) ～ (v) の組合せはどれか。d に関する解答群のうち，最も適切なものを選べ。

(i) 営業企画部は，参照先としてスマートデバイス及び B 社アプリの設定方法が掲載されているインターネット上の SNS やブログなどの URL を利用マニュアルに記載

(ii) 営業企画部は，実際に手順の検証を行い，スマートデバイス及び B 社アプリの利用マニュアルを作成

(iii) 営業企画部は，モバイルワーカが自分専用の利用マニュアルを独自に作成できるようにインターネット上の SNS やブログへのアクセスを許可

(iv) 営業企画部は，モバイルワーカがスマートデバイス及び B 社アプリの利用マニュアルに不備を発見した場合，直ちにモバイルワーカが修正することを推奨

(v) 営業企画部は，モバイルワーカにスマートデバイス及び B 社アプリの正しい設定，利用手順，注意事項などについて定期的に教育を実施

d に関する解答群

	d1	d2
ア	(i)	(iii)
イ	(i)	(iv)
ウ	(ii)	(iv)
エ	(ii)	(v)
オ	(iii)	(iv)
カ	(iv)	(v)

(3) 表 2 中の下線 ① が原因で起こり得る事象はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア OS の脆弱性を悪用されて，バックドアを仕掛けられる。

イ 公衆無線 LAN の電波と携帯電話回線の電波が干渉したときに，通話とインターネット通信ができなくなる。

ウ スマートデバイスの利用者が出荷時のセキュリティ設定を解除できるようになる。

エ 不正なショートメッセージサービスがスマートデバイスに送られたとき，架空の未払料金を請求されて支払うことになる。

オ 不正な電子メールがスマートデバイスに送られたときに，フィッシングサイトに誘導されて，個人情報が漏えいする。

設問2　〔対策の実現に向けた調査〕について，(1) ～ (4) に答えよ。

(1)　本文中の［ e1 ］，［ e2 ］に入れる，次の (i) ～ (v) の組合せはどれか。e に関する解答群のうち，最も適切なものを選べ。

(i)　エージェントアプリ

(ii)　公衆無線 LAN 及び携帯電話回線

(iii)　スマートデバイスに保存されている全てのデータ

(iv)　スマートデバイスの業務フォルダ内に保存されているデータ

(v)　スマートデバイスの操作ログ

e に関する解答群

	e1	e2
ア	(i)	(ii)
イ	(iii)	(iv)
ウ	(iii)	(v)
エ	(iv)	(iii)
オ	(iv)	(v)
カ	(v)	(iii)
キ	(v)	(iv)

(2) 表 3 項番 1 に示したクレームを避けるために，端末データの閲覧に先立ち実施しておくべき措置として，表 3 中の［ 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。

f に関する解答群

ア　モバイルワーク利用前に口頭で説明する

イ　モバイルワーク利用前に書面で同意を得る

ウ　モバイルワーク利用前に説明し，その日時を記録する

エ　モバイルワーク利用前に電子メールで通知し，開封通知を保存する

(3) 表 3 中の［ g ］，［ h ］に入れる適切な字句を，解答群の中から選べ。

g，h に関する解答群

ア　業務データと私的データの両方のデータが消える

イ　業務データと私的データは残り，B 社アプリは消える

ウ　スマートデバイスがロックされるので，自動で初期化される

エ　スマートデバイスのロックを解除するためのパスワードが変更されるので，スマートデバイスを発見した場合，モバイルワーカ本人はロックを解除できず，利用することができない

(4) 表 3 中の下線 ② 及び下線 ③ について，修正内容と運用手順を，次の (i) ～ (v) の中から一つず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。

［モバイル端末利用申請書の修正内容］

(i) モバイルワークで使用する可能性がある全ての個人所有のスマートデバイスの機種名及び OS 名を記入できるように修正する。

(ii) モバイルワークで使用する個人所有のスマートデバイスの電話番号及び機種名を記入できるように修正する。

(iii) モバイルワークで使用する個人所有のスマートデバイスの電話番号及び国際移動体装置識別番号を記入できるように修正する。

［運用手順］

(iv) MM1 又は MM2 の管理画面上で，端末データが全項目とも収集されていることを複数の運用担当者が一緒に目視で確認した後，B 社アプリを MM1 又は MM2 を利用して配布する。

(v) MM1 又は MM2 の管理画面上の端末データと，モバイル端末利用申請書を運用担当者が目視で突合し，一致した場合にだけ B 社アプリを MM1 又は MM2 を利用して配布する。

解答群

ア (i), (iv)　　イ (i), (v)　　ウ (ii), (iv)

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

〔 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。