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)