目　次

第４部　午前問題　解答・解説編

第５部　午後問題　解答・解説編

第６部　情報セキュリティマネジメント試験

参考資料

2　情報セキュリティマネジメント試験

2-1　情報セキュリティマネジメント試験の特徴

ここからは，情報処理技術者試験に新たに加わった情報セキュリティマネジメント試験の特徴をまとめておきます。

(1)　「共通キャリア・スキルフレームワーク」に準拠した試験

「共通キャリア・スキルフレームワーク」は，IT 関連業務に携わる人の仕事内容，スキルなどを定めた資料で，1〜4 のレベル分けがされています。この中のレベル 1 に対応する試験が「IT パスポート試験」，レベル 2 が「基本情報技術者試験」，「情報セキュリティマネジメント試験」，レベル 3 が「応用情報技術者試験」というように対応しています。レベル 4 は 8 試験区分あり，“高度試験”という総称で扱われます。

なお，上位レベルの試験は，下位レベルの問題を含んで出題されます。

レベル	試験区分	問われる知識や技能のレベル
1	IT パスポート試験	職業人として，IT を利活用するための**共通的基礎知識**が問われる。
2	基本情報技術者試験	高度 IT 人材となるために必要な**基本的知識・技能**が問われる。
	情報セキュリティマネジメント試験	情報セキュリティリーダとして，IT の安全な利活用を推進するための**基本的知識・技能**が問われる。
3	応用情報技術者試験	高度 IT 人材となるために必要な**応用的知識・技能**が問われる。
4	高度試験 (8 試験区分)	高度IT人材に必要な情報技術及び業務に関する**高度かつ専門的な知識・技能**が問われる。

図表 2　各試験区分のレベル

(2)　試験時間，出題形式など

試験時間，出題形式，出題数，解答数は次のとおりです。

試験区分　略号	実施時期	午前 9：30〜11：00（90 分）	午後 12：30〜14：00（90 分）
情報セキュリティマネジメント試験　SG	春秋	多肢選択式 (四肢択一) 50 問出題 50 問解答	多肢選択式 3 問出題 3 問解答

図表 3　試験時間，出題形式，出題数，解答数

4　平成 28 年度春期試験の分析と出題予想

4-1　平成 28 年度春期試験の分析

第 1 回目の実施となった平成 28 年度春期の情報セキュリティマネジメント試験の出題内容を分析しました。

(1)　試験全体について

第 1 回目の情報セキュリティマネジメント試験の応募者数，受験者数，合格者数（合格率）は次のとおりでした。

	平成 28 年度春期
応募者数	21,691 人
受験者数	17,959 人
合格者数	15,800 人
合格率	88.0%

図表 9　情報セキュリティマネジメント試験の応募者数，受験者数，合格者数

出題された問題が基本的な内容で全体に解答しやすかったこと，受験者の半数以上が IT 関連業務に携わる人だったことから，合格率は非常に高い 88.0%という結果になりました。過去の経緯から，新設された試験には， 2 回目以降，難しくなっていくという傾向があります。

(2)　午前試験

午前問題で出題された 50 問の分野別出題数は次の図表 10 のとおりです。初めて実施された試験ですが，過去の情報処理技術者試験で出題された問題も約 4 割ありました。基本情報技術者試験から 10 問，応用情報技術者試験から 8 問ありましたが，情報セキュリティマネジメント試験レベルで解答できる内容でした。

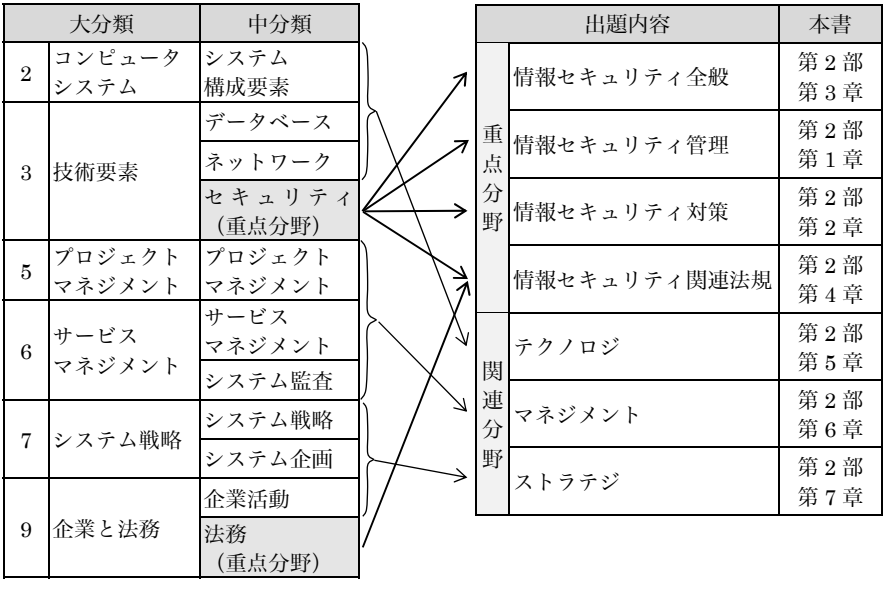
各分野の出題数は，テクノロジ系が 34 問，マネジメント系が 6 問，ストラテジ系が 10 問で，テクノロジを重視した配分だといえます。

テクノロジ系の問題では重点分野である“セキュリティ”が 30 問で全体の 6 割を占め，それ以外の内容からの出題は少なく 4 問でした。セキュリティ関連で出題された問題の特徴としては，セキュリティ管理寄りの内容として，JIS Q 27001 から 2 問，JIS Q 27002 から 1 問，内部不正防止ガイドラインから 2 問の出題がありました。これは試験の位置付けから考えて，予想よりもやや少ないと考えられ，次回以降，もう少し増えると予想されます。また，セキュリティ技術寄り問題が予想より多く，攻撃関連で 6 問出題されました。

6　本書の使い方

6-1　本書の構成

試験センターから発表された「試験区分別出題分野一覧表」（図表 4）と「情報セキュリティマネジメント試験の出題内容」（図表 13）と本書の第 2 部の構成は次のとおりです。



大分類		中分類
2	コンピュータシステム	システム構成要素
3	技術要素	データベース
		ネットワーク
		セキュリティ（重点分野）
5	プロジェクトマネジメント	プロジェクトマネジメント
6	サービスマネジメント	サービスマネジメント
		システム監査
7	システム戦略	システム戦略
		システム企画
9	企業と法務	企業活動
		法務（重点分野）

出題内容		本書
重点分野	情報セキュリティ全般	第 2 部 第 3 章
	情報セキュリティ管理	第 2 部 第 1 章
	情報セキュリティ対策	第 2 部 第 2 章
	情報セキュリティ関連法規	第 2 部 第 4 章
関連分野	テクノロジ	第 2 部 第 5 章
	マネジメント	第 2 部 第 6 章
	ストラテジ	第 2 部 第 7 章

図表 15　情報セキュリティマネジメント試験の出題内容と本書の第 2 部

なお，章の順序は，第 1 回目の情報セキュリティマネジメント試験の出題順に合わせています。

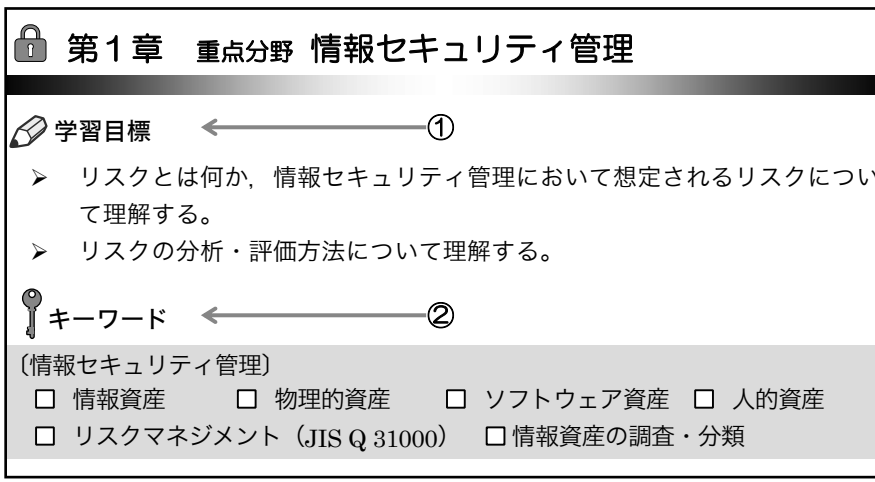
午後の出題範囲（図表 7）と本書の第 3 部の構成も次に示します。

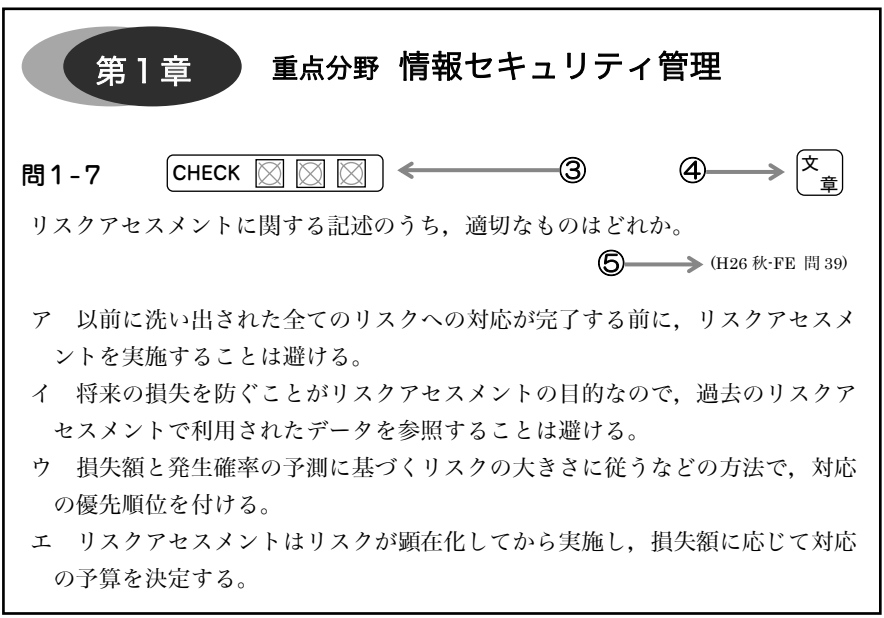
午後の出題範囲	本書
1　情報セキュリティマネジメントの計画，情報セキュリティ要求事項に関すること	第 3 部 第 1 章
2　情報セキュリティマネジメントの運用・継続的改善に関すること	第 3 部 第 2 章

図表 16　情報セキュリティマネジメント試験の出題範囲と本書の第 3 部

6-2　本書を使った学習の進め方

本書では，午前問題の出題内容に基づいて，章ごとに学習目標，キーワードを設定しています。学習の際には，まず，この部分を読み，どのような内容が含まれているかを頭に入れましょう。





第１章　重点分野 情報セキュリティ管理

学習目標

- リスクとは何か，情報セキュリティ管理において想定されるリスクについて理解する。
- リスクの分析・評価方法について理解する。
- 情報セキュリティマネジメントシステム（ISMS）について理解する。
- JIS Q 27001，JIS Q 27002 を中心とした情報セキュリティ規格について理解する。

キーワード

〔情報セキュリティ管理〕
☐ 情報資産　☐ 物理的資産　☐ ソフトウェア資産　☐ 人的資産
☐ リスクマネジメント（JIS Q 31000）　☐ 情報資産の調査・分類

〔リスクの種類〕
☐ 財産損失　☐ 責任損失　☐ 人的損失
☐ SNS による情報発信のリスク　☐ モラルハザード

〔情報セキュリティリスクアセスメント〕
☐ リスク基準　☐ リスクレベル　☐ リスク特定　☐ リスク分析
☐ リスク評価　☐ 定量的リスク分析手法

〔リスク対応〕
☐ リスクコントロール　☐ リスク移転　☐ リスク保有

〔情報セキュリティ継続〕
☐ 緊急時対応計画（☐ コンティンジェンシープラン）　☐ バックアップ対策

〔情報セキュリティ諸規程〕
☐ 情報セキュリティポリシ　☐ 情報管理規程　☐ 機密管理規程
☐ 文書管理規程　☐ コンピュータウイルス感染時の対応規程
☐ プライバシポリシ（☐ 個人情報保護方針）

第1章 重点分野 情報セキュリティ管理

問1-1 CHECK ☒ ☒ ☒

文章

情報セキュリティは情報資産の機密性，完全性，可用性を維持することを目指している。次の記述の中で完全性に関するものはどれか。

(713902)

ア　顧客情報が外部に漏えいしないように運用ルールを規定して厳重に管理する。

イ　サーバのアクセスログが改ざんされないようにログへのアクセスコントロールを行う。

ウ　電子メールがネットワーク上で盗聴されないように暗号化プロトコルを採用する。

エ　ハードウェアに障害が発生してもシステムダウンにならないように二重化する。

問1-2 CHECK ☒ ☒ ☒

文章

リスク分析に関する記述のうち，適切なものはどれか。

(H20 春-AD 問 54)

ア　考えられるすべてのリスクに対処することは時間と費用がかかりすぎるので，損失額と発生確率を予測し，リスクの大きさに従って優先順位を付けるべきである。

イ　リスク分析によって評価されたリスクに対し，すべての対策が完了しないうちに，繰り返しリスク分析を実施することは避けるべきである。

ウ　リスク分析は，将来の損失を防ぐことが目的であるから，過去の類似プロジェクトで蓄積されたデータを参照することは避けるべきである。

エ　リスク分析は，リスクの発生によって被る実損失額を知ることが目的であり，その損失額に応じて対策の費用を決定すべきである。

解答一覧

問1-1	イ
問1-2	ア
問1-3	イ
問1-4	ア
問1-5	イ
問1-6	エ
問1-7	ウ
問1-8	イ
問1-9	ウ
問1-10	ウ
問1-11	エ
問1-12	エ
問1-13	イ
問1-14	イ
問1-15	ウ
問1-16	ア
問1-17	エ
問1-18	エ
問1-19	ウ
問1-20	ア
問1-21	イ
問1-22	ア
問1-23	イ
問1-24	ア
問1-25	エ
問1-26	イ
問1-27	エ

第1章 情報セキュリティマネジメントの計画，情報セキュリティ要求事項に関すること

問1-1 CHECK ☒☒☒

企業情報ネットワークの構築におけるセキュリティ対策に関する次の記述を読んで，設問1〜6に答えよ。

(H15秋-SS午後Ⅱ問2改)

N社は，従業員400名，年商100億円の中規模なコンピュータ周辺機器のメーカである。都心にある本社と郊外にある組立工場及び部品製造工場では，それぞれLANに接続されたサーバとパソコン（以下，PCという）を利用して，生産計画，生産管理及び在庫管理（以下，業務APという）を行っていた。N社では，本社と各工場間を専用線で接続して，各サーバを参照していた。また，インターネットには，本社の限られたPCだけでしかアクセスできず，他社情報の収集に支障を来していた。そのため，本社と各工場間を通信事業者のIP-VPNで接続して，業務APを利用するN社企業情報ネットワークシステム（以下，Nネットという）を導入することにした。さらに，インターネットを利用して，取引先などとの電子メールの交換，Webでの他社情報の収集，N社の企業情報や新製品情報の発信及び部品材料の購入手配（以下，新規APという）を行うことにした。

〔Nネットの基本検討〕

N社では，本社情報システム部のW部長をリーダとしたNネットの構築を行うプロジェクトチーム（以下，チームという）が，情報システム技術者，情報ネットワーク技術者のU君，情報ネットワーク管理者のX君及び情報セキュリティ管理者のY君で編成された。チームは，図1に示すNネットの技術要件をまとめた。

(1) インターネットの利用には，インターネットサービスプロバイダの光回線を利用する。
(2) 外部のWebには，Webプロキシサーバを介してアクセスする。
(3) N社のPCから本社や各工場のサーバにアクセスして，業務APを実行する。業務APは，既存のものを移植して使用する。
(4) 資産管理には，資産管理サーバを設置する。
（以下，省略）

図1 Nネットの技術要件

第1章 重点分野 情報セキュリティ管理

問1-1 イ

情報資産の機密性，完全性，可用性（713902）

ISO 規格などでは，情報セキュリティについて，情報資産の機密性（Confidentiality；コンフィデンシャリティ），完全性（Integrity；インテグリティ），可用性（Availability；アベイラビリティ）の三つの観点が述べられている。これら三つの観点の頭文字をとって CIA などとも呼ばれる。機密性は「アクセスを認可された者だけが情報にアクセスできることを確実にすること」，完全性は「情報及び処理方法が正確であること及び完全であることを保護すること」，可用性は「認可された利用者が必要なときに情報及び関連する資産にアクセスできることを確実にすること」と定義されている。完全性に対する脅威としては，データの改ざんや破壊，消去などがあるので，（イ）が適切である。

ア：情報の漏えいは機密性に関する脅威である。

ウ：盗聴も機密性に関する脅威である。

エ：システムがダウンすることは可用性が損なわれることである。

問1-2 ア

リスク分析（H20 春-AD 問 54）

正確には，リスクとは予想結果と実際の結果の相違のことであり，必ずしも組織が損害を被るものだけとは限らない。しかし，一般にリスク分析というと，組織が損害を被るような原因を洗い出すことを指す。リスク分析を行う目的は，組織に対する損害をなるべく少なく抑えることであるので，すべてのリスクに対して対策を実施することが適切とは限らない。例えば，その対策に損害額以上の費用がかかるような場合には，対策をせずにその損害を被ったほうが，組織としては損害額が少ない。このため，リスク分析では，リスクの種類だけでなく，その発生確率や損失額などを合わせて分析し，その対策の費用対効果を考慮して実施の優先順位付けを行う。したがって，（ア）が適切である。

イ：リスク分析は，対策の実施が目的ではなく，リスクの発生を防ぐことが目的である。環境などの変化によって対策を見直し，柔軟に実施する。

ウ：同じような状況では同じようなリスクが付き物なので，過去の経験は大いに参考にすべきである。

エ：前述のように，リスク分析の目的は，そのリスクの発生確率や損失額を知り，リスク回避やリスク移転（保険を掛けるなど）を行うことで，損害をなるべく少なく抑えることである。

［設問６］

外部の派遣社員を活用して業務を遂行するときに，運用管理の観点から実施するセキュリティ対策が問われている。派遣社員を活用することになった背景は，ネットワーク管理課のメンバだけではネットワークの管理や PC ユーザへの対応が十分行えなかったので，運用管理体制を強化する一環としての施策である。問題文の最後には，「異動させた情報システム運用担当者を各工場に戻し，本社に経験のある派遣社員 1 名を配置することにした」とある。〔N ネットの情報セキュリティ対策の検討〕の冒頭に記述されているように，N ネットについては「監視と運用管理は，本社に業務を集中させて効率的に行うことにした」経緯があったが，各工場での対応負荷が大きいことから，一部分散管理へ戻したということである。派遣社員の活用に関するセキュリティ管理策としては，図 3 の外部委託の項目が参考になる。また，同様に罰則の規定も参考になる。N 社の社員であれば，就業規則の適用対象であるが，派遣社員は対象外になるので留意する必要がある。このため，具体的には派遣社員に N 社内でのシステム運用作業を依頼する際には，アクセスログの監視や重要作業の立会いなどの管理が必要になる。したがって，（ア）が正解である。

問１－２　購買管理システムの刷新と社内システムの情報セキュリティ　（H20 秋-SU 午後Ⅱ問 1 改）

【解答例】

［設問１］　(1)　a－オ，b－イ，c－ウ，d－カ
［設問２］　(1)　ア，オ　　(2)　イ
［設問３］　ウ
［設問４］　(1)　エ　　(2)　ア　　(3)　エ
［設問５］　(1)　ア　　(2)　エ

【解説】

設問 2(2)や設問 4(1)は情報セキュリティの範囲を超えて内部統制の視点にかかわる出題になっている。その他はウイルス対策，アカウント管理やログ管理などのオーソドックスなセキュリティ管理策をテーマにしており，得点しやすい。内部統制を題材にしたものにも慣れておきたい。

［設問１］

・空欄 a，b：解答群の用語を確認して，セキュリティ対策に関する用語の予防，検知があった場合，優先的に検討するとよい。利用者認証は不正なログインを未然に防止するセキュリティ対策であり，空欄 a には（オ）の「予防」が入る。ログ取得は，不正なログインやその前兆を検知するための対策になるので，空欄 b には（イ）の「検知」が入る。
・空欄 c：PC にアンチウイルスソフトを導入しない場合のリスクが問われている。

平成28年度　春期
情報セキュリティマネジメント試験
午前　問題

試験時間	9:30 ～ 11:00（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50
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ご注意ください。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**に一つだけ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〕　春の情報処理技術者試験が実施される月はどれか。

ア　2　　イ　3　　ウ　4　　エ　5

正しい答えは“ウ　4”ですから，次のようにマークしてください。

例題	ア　イ　●　エ

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。

平成 28 年度春期 情報セキュリティマネジメント試験
午前問題　解答・解説

問1　ウ
CSIRT の説明（H28 春-SG 問 1）

CSIRT（Computer Security Incident Response Team；シーサート）は，コンピュータネットワーク上のセキュリティインシデントを監視し，問題発生時には解決策や影響調査を行う組織を指す一般名称である。つまり企業や政府などの組織がセキュリティインシデントの監視・調査を行うための部署として設ける組織を指す。したがって，（ウ）が正解である。

ア：IANA（Internet Assigned Numbers Authority）の説明である。

イ：IETF（Internet Engineering Task Force）の説明である。

エ：ハクティビストなどと呼ばれる宗教的，政治的な主張を目的とした共通思想集団の説明である。Anonymous や Wikileaks が有名である。

問2　ウ
クリアデスクに該当するもの（H28 春-SG 問 2）

クリアデスクとは，職場の机の上に情報を記録したものを放置したまま離席しないことを意味する。機密情報や個人情報を記録した書類を机の上に出したままにしたり，ノート PC をログインしたままにしたりすることは情報漏えいにつながるため，これを防止するための措置である。したがって，（ウ）が正解である。

ア：情報をスクリーンに残したままにしないことを意味するクリアスクリーンに該当する。デスクトップは PC にログインしたとき，最初に目にする画面なので，たとえ閉じてあったとしてもここに置いたフォルダやファイルは人目に付きやすく，アクセスされやすい。デスクトップ上は必要最低限のアイコンだけにすることが望ましい。

イ：スクリーンに残した情報を盗み見から保護するスクリーンセーバロックに該当する。

エ：情報の盗難を防止する物理的セキュリティ対策に該当する。

問3　イ
実施者に独立かつ専門的な立場が求められるもの（H28 春-SG 問 3）

問題文は，情報セキュリティ監査基準の中の「情報セキュリティ監査の目的」からの抜粋である。情報セキュリティ監査基準では，情報セキュリティ監査の目的を「情報セキュリティに係るリスクマネジメントが効果的に実施されるように，リスクアセスメントに基づく適切なコントロールの整備，運用状況を，情報セキ

平成 28 年度春期 情報セキュリティマネジメント試験
午後問題　解答・解説

問１　標的型攻撃メールの脅威と対策　(H28 春-SG 午後問 1)

【解答】

［設問１］(1) a－キ，b－ク
(2) c－ウ
(3) ア，エ
(4) カ

［設問２］(1) カ
(2) d－エ
(3) e－イ
(4) f－ア
(5) エ

【解説】

標的型攻撃メールによるマルウェア感染とその対応を題材として，情報セキュリティマネジメントの運用における，情報セキュリティインシデント対応をテーマとした問題である。標的型攻撃メールの特徴や関連用語，初動対応の考察，規程順守や意識向上のための改善策の考察などが出題されている。IPA が公開している“対策のしおりシリーズ”の“標的型攻撃メール＜危険回避＞対策のしおり”に記載されている内容のうち，基本的な知識を整理できていれば高得点できたと思われる。

［設問１］

(1) 空欄 a，b は，S 主任の最初の発言である「標的型攻撃メールとは，［ a ］の組織や個人を対象として，受信者の PC にマルウェアを送りつけ，情報を窃取することなどを目的とするメールであり，［ b ］の組織や個人を対象として送られるウイルスメールとは異なるものです」という部分にある。そして，標的型攻撃メールとは，標的型攻撃において，攻撃者が標的（攻撃の対象）へ送りつけるメールのことである。また，標的型攻撃とは，文字どおり，標的を特定して行われる攻撃を意味している。したがって，空欄 a には，“特定”が入るので（キ）が正しい。また，空欄 b には，空欄 a の“特定”の対語である“不特定多数”が入るので（ク）が正しい。標的型攻撃における実際の標的は，「大手企業や官公庁以外もターゲットになり得る」という E 課長の発言からも分かるように，攻撃者の目的によって異なる。その他の解答群にあるように，国内あるいは海外，大企業あるいは中小企業，