模擬試験

2024 年 04 月版

目次

はじめに	4
模擬試験	5
解答集	15
評価	34

はじめに

これは EXIN Information Security Foundation based on ISO/IEC 27001 (ISFS.JP) のサンプル試験です。この試験は EXIN 試験の規則および規定を適用します。

本試験は選択式の問題が 40 問で構成されます。各問題には、選択肢が複数ありますが、そのうち正解は 1 つのみです。

この試験で取得できる最大点数は 40 点です。各正解には 1 点の価値があります。試験に合格するには 26 点以上が必要です。

本試験の制限時間は 60 分です。

ご健闘をお祈りいたします。

模擬試験

1 / 40
データベースには、電話会社の数百万件のトランザクションが含まれています。ある顧客への請求書が作成され、送信されました。

この請求書には顧客向けに何が記載されていますか?

A) データ
B) 情報
C) データと情報

2 / 40
データと情報の違いは何ですか？

A) データとは、事実や数値を意味する。情報とは、意味のあるデータの集まりである。
B) データは、構造化されていない数値から構成される。情報は、構造化された数値で構成される。
C) データにはセキュリティは必要ではない。情報にセキュリティは必要である。
D) データには価値がない。データを処理した情報には価値がある。

3 / 40
情報管理の**最も重要**な点は何ですか？

A) 業務活動とプロセスを中断せずに継続できるようにすること
B) 情報の価値を識別し、その価値が活用されるようにすること
C) 認可されていないユーザが自動化されたシステムにアクセスすることを防止すること
D) 組織内の情報の流れを理解すること

4 / 40
組織は、直面しているリスクを理解して、適切な対策を講じなければなりません。

リスクを特定するために把握しなければならないのは何ですか？

A) 何かが起こる発生可能性と、それが組織にもたらす結果
B) ベストプラクティスで定義されている最も一般的な危険とそれらを軽減する方法
C) 組織が直面している脅威と、それに対する組織のぜい弱性の度合い
D) 組織が直面する予期せぬイベント（事象）と、それらのイベントが発生した場合の対処方法

5 / 40
「完全性」と「機密性」以外の情報の信頼性の第3の側面はどれですか？

A) 正確さ
B) 可用性
C) 完全さ
D) 価値

6 / 40
ある組織では、社内の廊下にネットワークプリンタが設置されています。プリントアウトしたものをすぐに取りに行かず、プリンタに放置している社員が多く存在します。

この結果、情報の信頼性にどのような影響を及ぼしますか？

A) 情報の可用性が保証されなくなる。
B) 情報の機密性が保証されなくなる。
C) 情報の完全性が保証されなくなる。

7 / 40
説明責任と可監査性の違いは何ですか？

A) 説明責任とは、組織の財務会計が適切に管理されていることを意味する。
可監査性とは、組織が審査（監査）に合格したことを意味する。
B) 説明責任とは、組織の活動の結果に対して責任を持つことを意味する。
可監査性とは、組織が第三者の審査を受ける準備ができていることを意味する。
C) 説明責任とは、個人の行動に対して責任を持つことを意味する。
可監査性とは、組織の行為に対して責任を持つことを意味する。
D) 説明責任とは、サーベンスオクスリー法（SOX）に準拠した組織を意味する。
可監査性とは、ISO/IEC 27001に準拠した組織を意味する。

8 / 40
情報セキュリティポリシーの目的として**最も適切な説明**はどれですか？

A) 情報セキュリティポリシーは、リスク分析と適切管理策の調査について文書化する。
B) 情報セキュリティポリシーは、情報セキュリティに関する組織の方向性を示して支援する。
C) 情報セキュリティポリシーは、必要な詳細情報を提供して、セキュリティ計画を具体化する。
D) 情報セキュリティポリシーは、脅威と脅威によって起こりうる結果についての知見を提供する。

9 / 40
サラは、組織が個人データの保護規制を確実に遵守するための任務を任されています。

このために彼女が**最初にしなければならないことは**はどれですか？

A) 管理者がポリシーを遵守できるよう支援する責任者を任命する
B) 個人情報の収集と保管の禁止を発令する
C) 個人情報を提出するときに従業員にその責任を負わせる
D) 個人情報保護法の内容をプライバシーポリシーに取り入れる

10 / 40
ある組織が、ITの一部をアウトソーシングすることを決定しました。

サプライヤーと協力する場合、情報セキュリティを**最適に**確保するには何をするべきでしょうか？

A) サプライヤーの組織で、情報セキュリティ責任者（ISO）を新たに任命する
B) サプライヤーに対する情報セキュリティ要件を契約で正式に定める
C) 両組織を完全に分離して、全員がデータに対する説明責任を果たすようにする
D) サプライヤーに顧客組織のプロセスと手順に従うよう要求する

11 / 40
事業戦略および目標を、セキュリティ戦略と目標に変換する責任は誰にありますか？

A) 最高情報セキュリティ責任者（CISO）
B) 一般の管理職
C) 情報セキュリティ責任者（ISO）
D) 情報セキュリティポリシー責任者

12 / 40
人的脅威を**最もよく表している**のはどの説明ですか？

A) 漏電によって電気を供給できなくなる。
B) ウィルスをネットワークに侵入させるUSBメモリ。
C) サーバルームにほこりが多すぎる。

13 / 40
データベースシステムに最新のセキュリティパッチが適用されておらず、ハッキングされてしまいました。ハッカーによって、データにアクセスされ削除されました。

セキュリティパッチ適用の不備を示す情報セキュリティの概念はどれですか？

A) 影響
B) リスク
C) 脅威
D) ぜい弱性

14 / 40
会社で火災が発生しました。消防隊がすぐに現場に到着し、火災が広がって建物全体が焼失する前に鎮火することができました。しかし、サーバは火災により破壊されてしまいました。また、別室に保管されていたバックアップテープも溶けてしまい、多くの他の書類も失われていました。

この火災によって引き起こされる**間接的**な損害はどれですか？

A) コンピュータシステムの燃焼
B) 書類の焼失
C) 溶けたバックアップテープ
D) 水害

15 / 40
企業は自社のビジネスの種類に合わせてさまざまなリスク戦略を展開します。

病院にとって**最適なリスク戦略**はどれですか？

A) リスク受容
B) リスク回避
C) リスク負担
D) リスク中立

16 / 40
リスク分析を適切に行うと、多くの有益な情報がもたらされます。リスク分析には異なる主要な目的があります。

リスク分析の主要な目的では**ないもの**は何ですか？

A) インシデントのコストと管理策のコストのバランスをとる
B) 関連するぜい弱性と脅威を特定する
C) 資産とその価値を特定する
D) 対策と管理策を実施する

17 / 40
火災発生時における制止的管理策はどれですか？

A) 火災を検出した後に、消化活動を行う
B) 火災による損害を修復する
C) 火災保険に加入する

18 / 40
情報を分類する目的は何ですか？

A) ラベルを貼って情報を認識しやすくすること
B) モバイルデバイスの取扱いマニュアルを作成すること
C) 重要度に応じて情報を構造化すること

19 / 40
職務の分離をする**最も重要な理由**は、何ですか？

A) 社員が同じ時間に同じ仕事をすることがなくなる
B) 従業員がミスした場合に、全従業員が連帯責任を負う
C) 誰がどのようなタスクや活動に責任を持つのかを明確にする
D) 不正あるいは意図しない変更の可能性を最小限に抑える

20 / 40
情報へ適切にアクセスできるようにするための**最適な方法**はどれですか？

A) ワークフローを自動化する
B) 作業手順を定義する
C) すべての作業について、作業指示書を作成する
D) トレーニングを提供する

21 / 40
ある組織のオフィスで火災が発生しました。業務を継続するために従業員を近隣のオフィスに移動させることになりました。

非常時におけるスタンド・バイ取極の適用は、インシデントサイクルのどの段階に含まれますか？

A) 損害と復旧の段階の間
B) インシデントと損害の段階の間
C) 復旧と脅威の段階の間
D) 脅威とインシデントの段階の間

22 / 40
従業員が、自分の知らない間に契約の有効期限が変更されていたことを見つけました。有効期限を変更できる権限があるのは彼女だけであり、このセキュリティインシデントをヘルプデスクに報告しました。

ヘルプデスクの担当者は、このインシデントに関する以下の情報を記録しています。
- 日付と時刻
- インシデントの説明
- インシデントによって起こりうる結果

インシデントに関する重要な情報で欠落しているのはどれですか？

A) インシデントを報告した人の名前
B) ソフトウェアパッケージの名前
C) PC番号

23 / 40
組織の情報セキュリティマネジメントシステム（ISMS）を定期的に監査することが重要な理由はどれですか？

A) 監査は、情報セキュリティを確実にするために、顧客との契約において一般的な要件となっている。
B) 監査は、法規制要件を遵守するために必要な要素である。
C) 監査によって、組織の財務目標を達成する能力に関する問題点が特定される。
D) 監査によって、情報セキュリティ管理を実施するときの弱点が見つかる。

24 / 40
会社のメールアドレスを私的な目的で使用することを禁止規則が含まれる文書はどれですか?

A) 犯罪経歴証明書
B) 行動規範
C) 一般データ保護規則（GDPR）
D) 秘密保持契約書（NDA）

25 / 40
従業員がインシデントを発見した場合、通常、**最初に**報告すべきなのは誰ですか？

A) ヘルプデスク
B) 情報セキュリティ管理者
C) 情報セキュリティ責任者（ISO）
D) マネージャー（管理者）

26 / 40
従業員の情報セキュリティに対する意識を向上するために、**最も効果的な方法**は何ですか？

A) 管理層への意識向上トレーニングに注力する
B) 全社員を外部の情報セキュリティトレーニングに参加させる
C) 組織固有の意識向上プログラムを設定する
D) 一般的なオンラインの情報セキュリティトレーニングコースを利用する

27 / 40
組織の情報へのアクセスを管理する物理的な管理策とは何ですか？

A) 空調の設置
B) USBメモリの使用の禁止
C) ユーザ名とパスワードの入力の要求
D) 割れにくいガラスの使用

28 / 40
データセンターでバッテリーパックを使用していますが、発電機はありません。

この設定におけるデータセンターの可用性のリスクを正しく説明しているのはどれですか？

A) 復旧時には発電機が必要となるため、主電源が自動的に復旧しない場合がある。
B) 主電源の停電が数分または数時間以上続く場合、電力が利用できなくなることがある。
C) バッテリーパックの寿命には限りがあるため、2～3日後にディーゼル燃料が切れて機能しなくなる可能性がある。
D) 数時間後には、発電機からバッテリーパックに給電する必要があるため、限られた保護しか提供できない。

29 / 40
サーバ室に空調が設置されているのはなぜですか？

A) バックアップのテープは、薄いプラスチックでできているため、高温環境に耐えることができない。そのため、サーバルームが高温になると、破損する恐れがある。
B) サーバルームで作業する従業員が、室温が高い中で作業しないようにするため。高温の環境では、ミスをする可能性を増加させる。
C) サーバルームを冷却し、機器で発生する熱を取り出す必要がある。また、室内の空気を除湿および清浄するため。
D) オフィスの空気を冷却するための機器を設置するには、サーバルームが最適である。このような大型機器によって、オフィススペースを犠牲にする必要はない。

30 / 40
物理的なセキュリティでは、複数の保護リングを適用して、いくつかの対策を講じることができます。

保護リングでは**ないものは**どれですか？

A) 建物（ビルディング）リング
B) 中間（ミドル）リング
C) 安全な部屋（セキュアルーム）リング
D) 外壁（アウター）リング

31 / 40
資産を保護するための管理策は、その資産によって異なります。

資産とその資産を保護するための**最適な方法の組み合わせ**はどれですか？

A) 用紙への記入と署名によってフォーム（用紙）を保護する
B) 単一のユーザーにラップトップを割り当てることでラップトップを保護します
C) 暗号化を使用してUSBメモリスティックを保護する
D) バックアップを利用して、インターネット接続を保護する

32 / 40
情報セキュリティを考慮したシステム開発に役立つ情報セキュリティ管理策はどれですか？

A) サーバの冗長性を確実にする
B) 物理的な入室管理策を実施する
C) 従業員のバックグラウンドチェック（身元調査）を実施する
D) 情報資産のデータ分類を使用する

33 / 40
組織がポリシーを変更し、従業員がリモートで働くことが許可されるようになりました。

どのようなセキュリティ管理策を実施する必要がありますか？

A) V-LANを作成して企業ネットワークをセグメント化する
B) 企業ネットワーク上の情報を暗号化する
C) 企業ネットワークにファイアウォールを設置する
D) VPNを利用して企業ネットワークに接続する

34 / 40
ある組織の従業員が、非対称暗号で保護されているノートパソコンで仕事をしています。鍵を安価に管理できるように、すべてのコンサルタントが同じ鍵のペアを使用しています。

情報漏洩が発生した場合は、新しい鍵を提供する必要があります。

どのような場合に新しい鍵を提供する必要がありますか？

A) 秘密鍵が三者に知られた場合
B) 公開鍵が三者に知られた場合
C) 公開鍵基盤（PKI）が第三者に知られた場合

35 / 40
公開鍵基盤（PKI）が提供するセキュリティはどれですか？

A) PKIにより、企業データが定期的にバックアップされる。
B) PKIは、Webベースの取引が安全であることを顧客に示す。
C) PKIは、特定の公開鍵を使用するユーザまたはシステムを検証する。

36 / 40
ある機能を実行するように見せかけて、意図的に二次的な活動を実行するプログラムであるマルウェアのタイプはどれですか？

A) ロジックボム（論理爆弾）
B) スパイウェア
C) トロイの木馬
D) ワーム

37 / 40
自己複製により、複数のコンピュータを感染させネットワークを構築するマルウェアのタイプはどれですか？

A) ロジックボム（論理爆弾）
B) スパイウェア
C) トロイの木馬
D) ワーム

38 / 40
すべての組織に課せられる情報セキュリティに関する法律または規制はどれですか？

A) 一般データ保護規則（GDPR）
B) 知的財産（IP）権
C) ISO/IEC 27001
D) ISO/IEC 27002

39 / 40
情報セキュリティ管理策の実施に焦点を当てたISO規格はどれですか？

A) ISO/IEC 27000
B) ISO/IEC 27001
C) ISO/IEC 27002
D) ISO/IEC 27005

40 / 40
ヨーロッパで**最もよく使われている**のは、どの組織の標準ですか？

A) 米国国家規格協会（ANSI）
B) 国際標準化機構（ISO）
C) アメリカ国立標準技術研究所（NIST）

解答集

1 / 40
データベースには、電話会社の数百万件のトランザクションが含まれています。ある顧客への請求書が作成され、送信されました。

この請求書には顧客向けに何が記載されていますか?

A) データ
B) 情報
C) データと情報

A) 不正解。データベースにはデータが含まれています。ただし、請求書が作成されて受信者に送信される場合、それは受信者向けの情報になります。
B) 正解。情報の価値は受け手によって決まります。請求書には受信者にとって貴重なデータが含まれているため、情報となります。（参考文献：A、4.8.5章）
C) 不正解。請求書には、受信者にとって情報のみが含まれます。

2 / 40
データと情報の違いは何ですか？

A) データとは、事実や数値を意味する。情報とは、意味のあるデータの集まりである。
B) データは、構造化されていない数値から構成される。情報は、構造化された数値で構成される。
C) データにはセキュリティは必要ではない。情報にセキュリティは必要である。
D) データには価値がない。データを処理した情報には価値がある。

A) 正解。情報は、一定の文脈でデータを意味付けすることで得られるものです。（参考文献：A、3.1章）
B) 不正解。データには、構造化データと非構造化データの2つのタイプがあります。情報は通常、構造化されています。
C) 不正解。データも情報も保護しなければなりません。
D) 不正解。データにも情報にも価値があります。

3 / 40
情報管理の**最も重要**な点は何ですか？

A) 業務活動とプロセスを中断せずに継続できるようにすること
B) 情報の価値を識別し、その価値が活用されるようにすること
C) 認可されていないユーザが自動化されたシステムにアクセスすることを防止すること
D) 組織内の情報の流れを理解すること

A) 不正解。これは、事業継続管理（BCM）の重点的な作業です。BCMの目的は、事業活動の中断を防ぎ、情報システムの広範囲にわたる中断の影響から重要なプロセスを保護し、迅速な復旧を可能にすることです。
B) 正解。情報管理とは、組織が情報をどのように効率的に計画、収集、整理、利用、管理、伝達、廃棄するかについての方法を示します。またそれによって情報の価値を識別し、最大限に活用されることを確実にする方法を示すことです。（参考文献：A、4.9章）
C) 不正解。これは、アクセス管理の重点的な作業です。認可されていないユーザやプロセスが自動化されたシステム、データベース、プログラムにアクセスできないようにするものです。
D) 不正解。これは、情報分析の重点的な作業です。情報分析を実施することにより、組織が情報をどのように処理するか、および情報が組織内をどのように流れるかを明確に示すことができます。

4 / 40
組織は、直面しているリスクを理解して、適切な対策を講じなければなりません。

リスクを特定するために把握しなければならないのは何ですか？

A) 何かが起こる発生可能性と、それが組織にもたらす結果
B) ベストプラクティスで定義されている最も一般的な危険とそれらを軽減する方法
C) 組織が直面している脅威と、それに対する組織のぜい弱性の度合い
D) 組織が直面する予期せぬイベント（事象）と、それらのイベントが発生した場合の対処方法

A) 正解。リスクは、「何かが起こる可能性」と「ビジネスへの影響」という2つの重要な要素によって決まります。（参考文献：A、3.1章）
B) 不正解。組織がリスクを定義する際に、一般的な危険性を起点にするのは賢明ではありません。他の組織と同じ対策を実施しても、その組織が安全になるわけではありません。
C) 不正解。これは「発生可能性」の説明です。「発生可能性」を理解することは重要ですが、それがビジネスにどのような影響を与えるかという重要な側面が欠落しています。
D) 不正解。最終的にはリスクと管理策をすり合わせる必要がありますが、これはリスクを理解する方法というよりも、むしろリスクへの対応です。

5 / 40
「完全性」と「機密性」以外の情報の信頼性の第3の側面はどれですか？

A) 正確さ
B) 可用性
C) 完全さ
D) 価値

A) 不正解。情報の信頼性の3つの側面には、可用性、完全性、機密性があります。正確さは、完全性の一部です。
B) 正解。情報の信頼性の3つの側面には、可用性、完全性、機密性があります。（参考文献：A、3.4.3章）
C) 不正解。情報の信頼性の3つの側面には、可用性、完全性、機密性があります。完全さは、完全性の一部です。
D) 不正解。情報の信頼性の3つの側面には、可用性、完全性、機密性があります。

6 / 40
ある組織では、社内の廊下にネットワークプリンタが設置されています。プリントアウトしたものをすぐに取りに行かず、プリンタに放置している社員が多く存在します。

この結果、情報の信頼性にどのような影響を及ぼしますか？

A) 情報の可用性が保証されなくなる。
B) 情報の機密性が保証されなくなる。
C) 情報の完全性が保証されなくなる。

A) 不正解。情報を作成および印刷するために使用していたシステムにこの情報は残っています。
B) 正解。この情報にアクセスすべきではない人が情報を入手したり、その情報を読み取ったりする可能性があります。（参考文献：A、3.4.1章）
C) 不正解。この情報は紙に印刷されるため、その完全性は保証されます。

7 / 40
説明責任と可監査性の違いは何ですか？

A) 説明責任とは、組織の財務会計が適切に管理されていることを意味する。
可監査性とは、組織が審査（監査）に合格したことを意味する。
B) 説明責任とは、組織の活動の結果に対して責任を持つことを意味する。
可監査性とは、組織が第三者の審査を受ける準備ができていることを意味する。
C) 説明責任とは、個人の行動に対して責任を持つことを意味する。
可監査性とは、組織の行為に対して責任を持つことを意味する。
D) 説明責任とは、サーベンスオクスリー法（SOX）に準拠した組織を意味する。
可監査性とは、ISO/IEC 27001に準拠した組織を意味する。

A) 不正解。説明責任は財務会計と直接関係しません。可監査性は、監査に合格したこととは関係ありません。
B) 正解。これが、説明責任と可監査性の正しい定義です。（参考文献：A、3.4.4章）
C) 不正解。説明責任の定義は正しいのですが、可監査性の定義が正しくありません。可監査性は、組織の行為に対する責任とは関係がありません。
D) 不正解。説明責任も可監査性も、SOXやISO/IEC規格への準拠について言及していません。

8 / 40
情報セキュリティポリシーの目的として**最も適切な説明**はどれですか？

A) 情報セキュリティポリシーは、リスク分析と適切管理策の調査について文書化する。
B) 情報セキュリティポリシーは、情報セキュリティに関する組織の方向性を示して支援する。
C) 情報セキュリティポリシーは、必要な詳細情報を提供して、セキュリティ計画を具体化する。
D) 情報セキュリティポリシーは、脅威と脅威によって起こりうる結果についての知見を提供する。

A) 不正解。リスクの分析及び管理策を探求することが、リスク分析及びリスクマネジメントの目的です。
B) 正解。経営陣は、セキュリティポリシーを提供し、情報セキュリティについて指示し支援します。（参考文献：A、4.2.1章）
C) 不正解。セキュリティ計画により、情報セキュリティポリシーを具体化します。この計画には、どのような管理策が選択されたか、誰が何に責任を持つか、管理策を実施するためのガイドラインなどが含まれます。
D) 不正解。脅威分析の目的は、脅威と脅威によってもたらされるよって起こりうる結果について、知見を提供することです。

9 / 40
サラは、組織が個人データの保護規制を確実に遵守するための任務を任されています。

このために彼女が**最初にしなければならないことは**はどれですか？

A) 管理者がポリシーを遵守できるよう支援する責任者を任命する
B) 個人情報の収集と保管の禁止を発令する
C) 個人情報を提出するときに従業員にその責任を負わせる
D) 個人情報保護法の内容をプライバシーポリシーに取り入れる

A) 不正解。管理者を支援する人物の任命は、個人情報保護法を準拠するための要件ではありません。最初に、社内のプライバシーポリシーを、個人情報保護法に合わせる必要があります。
B) 不正解。これは、個人情報保護法を遵守するための最良の方法ではありません。
C) 不正解。これは、個人情報保護法を準拠するための方法ではありません。
D) 正解。遵守に向けた第一歩は、組織で使用する社内ポリシーを作成することです。（参考文献：A、5.1章）

10 / 40
ある組織が、ITの一部をアウトソーシングすることを決定しました。

サプライヤーと協力する場合、情報セキュリティを**最適に**確保するには何をするべきでしょうか？

A) サプライヤーの組織で、情報セキュリティ責任者（ISO）を新たに任命する
B) サプライヤーに対する情報セキュリティ要件を契約で正式に定める
C) 両組織を完全に分離して、全員がデータに対する説明責任を果たすようにする
D) サプライヤーに顧客組織のプロセスと手順に従うよう要求する

A) 不正解。サプライヤーの組織で既にISOが任命されている場合は、新たにISOを任命する必要はありません。
B) 正解。契約の締結は、サプライヤーのリスクを管理するための確実な仕組み（フェイルセーフな仕組み）ではありませんが、最も効果的な方法です。（参考文献：A、5.20章）
C) 不正解。分離しても、顧客組織は引き続きすべての情報に対して責任を負います。組織を完全に分離したままにすると、顧客組織は、サプライヤーの組織で情報セキュリティを確保したり、影響を与えたりする方法を把握できないことを意味します。
D) 不正解。サプライヤーは自社独自の情報セキュリティプロセスを確立することが許可されるべきであり、これは最良の方法ではありません。

11 / 40
事業戦略および目標を、セキュリティ戦略と目標に変換する責任は誰にありますか？

A) 最高情報セキュリティ責任者（CISO）
B) 一般の管理職
C) 情報セキュリティ責任者（ISO）
D) 情報セキュリティポリシー責任者

A) 正解。CISOは組織の最高レベルの管理者であり、事業全体のセキュリティ戦略全般を策定します。（参考文献：A、5.2章）
B) 不正解。一般の管理職は、CISOがセキュリティ戦略全般を立案するためのインプットとなる戦略を定義します。
C) 不正解。ISOは、会社のポリシーに基づいて事業部門の情報セキュリティポリシーを策定し、それが遵守されることを確実なものにします。
D) 不正解。情報セキュリティポリシー責任者は、セキュリティ戦略から派生したポリシーを維持する責任があります。

12 / 40
人的脅威を**最もよく表している**のはどの説明ですか？

A) 漏電によって電気を供給できなくなる。
B) ウィルスをネットワークに侵入させるUSBメモリ。
C) サーバルームにほこりが多すぎる。

A) 不正解。漏電は人による脅威ではなく、非人的脅威です。
B) 正解。USBメモリは必ず人によって挿入されます。USBメモリによってウイルスがネットワークに侵入した場合、それは人的脅威となります。（参考文献：A、3.9.1章）
C) 不正解。ホコリは人による脅威ではなく、非人的脅威です。

13 / 40
データベースシステムに最新のセキュリティパッチが適用されておらず、ハッキングされてしまいました。ハッカーによって、データにアクセスされ削除されました。

セキュリティパッチ適用の不備を示す情報セキュリティの概念はどれですか？

A) 影響
B) リスク
C) 脅威
D) ぜい弱性

A) 不正解。影響は、イベント（事象）が組織や組織の情報に与える影響を意味します。
B) 不正解。リスクとは、あるイベント（事象）が発生する可能性と影響の組み合わせです。
C) 不正解。脅威の例としては、ぜい弱性を悪用しようとする外部エンティティが挙げられます。この場合においては、ハッカーが脅威となります。
D) 正解。ぜい弱性の例として、保護の欠如が挙げられます。（参考文献：A、3.5.3章）

14 / 40
会社で火災が発生しました。消防隊がすぐに現場に到着し、火災が広がって建物全体が焼失する前に鎮火することができました。しかし、サーバは火災により破壊されてしまいました。また、別室に保管されていたバックアップテープも溶けてしまい、多くの他の書類も失われていました。

この火災によって引き起こされる**間接的**な損害はどれですか？

A) コンピュータシステムの燃焼
B) 書類の焼失
C) 溶けたバックアップテープ
D) 水害

A) 不正解。コンピュータシステムの燃焼は、火災による直接損害です。
B) 不正解。書類の焼失は、火災による直接損害です。
C) 不正解。バックアップテープの溶解は、火災による直接の被害です。
D) 正解。消火設備による水害は、火災によって引き起こされる間接的な損害です。これは、火災による損害を最小限に抑えることを目的とした消火活動の副作用です。 （参考文献：A、3.10章）

15 / 40
企業は自社のビジネスの種類に合わせてさまざまなリスク戦略を展開します。

病院にとって**最適なリスク戦略**はどれですか？

A) リスク受容
B) リスク回避
C) リスク負担
D) リスク中立

A) 不正解。経済的な損失や患者の死亡などの影響があるため、病院は、簡単にリスクを受容することはできません。
B) 正解。病院はリスクを回避するように努めなければなりません。（参考文献：A、3.11章）
C) 不正解。リスク負担とは、一定のリスクを受容することを意味します。リスク負担は、管理策のためのコストが、起こりうる損害を上回る場合に取り入れられる場合があります。病院においては、これはリスクに対応する最良の方法ではありません。
D) 不正解。リスク中立とは、脅威が発生しないか、発生しても被害が最小になるようにセキュリティ対策を講じることを意味します。患者に損害を与えることは決して許容される考えではないため、病院はリスクを回避する必要があります。

16 / 40
リスク分析を適切に行うと、多くの有益な情報がもたらされます。リスク分析には異なる主要な目的があります。

リスク分析の主要な目的では**ないもの**は何ですか？

A) インシデントのコストと管理策のコストのバランスをとる
B) 関連するぜい弱性と脅威を特定する
C) 資産とその価値を特定する
D) 対策と管理策を実施する

A) 不正解。これはリスク分析の主目的の1つです。
B) 不正解。これはリスク分析の主目的の1つです。
C) 不正解。これはリスク分析の主目的の1つです。
D) 正解。これはリスク分析の目的ではありません。（参考文献：A、3.7章）

17 / 40
火災発生時における制止的管理策はどれですか？

A) 火災を検出した後に、消化活動を行う
B) 火災による損害を修復する
C) 火災保険に加入する

A) 正解。この制止的管理策により、火災による損害を最小限に抑えることができます。（参考文献：A、3.8章）
B) 不正解。これは制止的管理策ではなく、火災による被害を最小限に抑えるものではありません。
C) 不正解。保険への加入は、火災による経済的な影響を防ぐものであり、リスクに対する保険です。

18 / 40
情報を分類する目的は何ですか？

A) ラベルを貼って情報を認識しやすくすること
B) モバイルデバイスの取扱いマニュアルを作成すること
C) 重要度に応じて情報を構造化すること

A) 不正解。情報にラベルを付けることは、「指定」であり、情報の分類後に行われる情報分類の特殊な形式です。
B) 不正解。マニュアルの作成は、ユーザ向けのガイドラインを作成することに関連しており、情報の分類ではありません。
C) 正解。情報の分類は、情報を構造化するためのさまざまな機密レベルを定義するために使用されます。（参考文献：A、5.12章）

19 / 40
職務の分離をする**最も重要な理由**は、何ですか？

A) 社員が同じ時間に同じ仕事をすることがなくなる
B) 従業員がミスした場合に、全従業員が連帯責任を負う
C) 誰がどのようなタスクや活動に責任を持つのかを明確にする
D) 不正あるいは意図しない変更の可能性を最小限に抑える

A) 不正解。職務の分離は、承認されていないあるいは意図しない変更や企業資産の不正使用を防止するために使用されます。活動を実施するべき時期を定義するものではありません。
B) 不正解。職務の分離は、タスクと責任を分離するために行われ、連帯責任を負わせることではありません。
C) 不正解。職務の分離は、承認されていないあるいは意図しない変更や企業資産の不正使用を防止するために使用されます。その目的は、誰が何に対して責任を負うのかを明確にすることではありません。
D) 正解。職務の分離は、許可されていないあるいは意図しない変更、または組織の資産の悪用の可能性を防止するために、職務を分離する必要があります。（参考文献：A、5.3章）

20 / 40
情報へ適切にアクセスできるようにするための**最適な方法**はどれですか？

A) ワークフローを自動化する
B) 作業手順を定義する
C) すべての作業について、作業指示書を作成する
D) トレーニングを提供する

A) 不正解。ワークフローの自動化は、確かに情報セキュリティに貢献しますが、情報へ適切にアクセスさせるためには役立ちません。
B) 正解。適切かつ安全に、責任ある方法で作業する方法を定めた手順を使用することは、効果的な情報セキュリティを達成するための有効な方法です。（参考文献：A、5.36.1章）
C) 不正解。これは詳細すぎて規範的であるため、最良の方法ではありません。
D) 不正解。トレーニングは重要ですが、それによって情報への適切なアクセスが保証されるわけではありません。

21 / 40
ある組織のオフィスで火災が発生しました。業務を継続するために従業員を近隣のオフィスに移動させることになりました。

非常時におけるスタンド・バイ取極の適用は、インシデントサイクルのどの段階に含まれますか？

A) 損害と復旧の段階の間
B) インシデントと損害の段階の間
C) 復旧と脅威の段階の間
D) 脅威とインシデントの段階の間

A) 不正解。損害と復旧はスタンド・バイ取極めによって制限されます。
B) 正解。スタンド・バイ取極とは、損害を制限するために開始される制止的な対策です。（参考文献：A、3.8.4章）
C) 不正解。復旧の段階は、スタンド・バイ取極めを実施した後に行われます。
D) 不正解。インシデントのないスタンド・バイ取極めの実施は、極めて高額になります。

22 / 40
従業員が、自分の知らない間に契約の有効期限が変更されていたことを見つけました。有効期限を変更できる権限があるのは彼女だけであり、このセキュリティインシデントをヘルプデスクに報告しました。

ヘルプデスクの担当者は、このインシデントに関する以下の情報を記録しています。
- 日付と時刻
- インシデントの説明
- インシデントによって起こりうる結果

インシデントに関する重要な情報で欠落しているのはどれですか？

A) インシデントを報告した人の名前
B) ソフトウェアパッケージの名前
C) PC番号

A) 正解。インシデントを報告する際には、少なくとも報告者の名前を記録する必要があります。（参考文献：A、5.25章）
B) 不正解。これは後でも追加できる情報です。
C) 不正解。これは後でも追加できる情報です。

23 / 40
組織の情報セキュリティマネジメントシステム（ISMS）を定期的に監査することが重要な理由はどれですか？

A) 監査は、情報セキュリティを確実にするために、顧客との契約において一般的な要件となっている。
B) 監査は、法規制要件を遵守するために必要な要素である。
C) 監査によって、組織の財務目標を達成する能力に関する問題点が特定される。
D) 監査によって、情報セキュリティ管理を実施するときの弱点が見つかる。

A) 不正解。顧客との契約に、監査要件が含まれていることはほとんどありません。
B) 不正解。法規制要件では、通常、監査の実施は要求されません。
C) 不正解。監査は、財務業績の検証には使用されることは通常はありません。
D) 正解。監査の目的は、導入されている管理策の弱点を見つけることです。（参考文献：A、5.35章）

24 / 40
会社のメールアドレスを私的な目的で使用することを禁止規則が含まれる文書はどれですか?

A) 犯罪経歴証明書
B) 行動規範
C) 一般データ保護規則（GDPR）
D) 秘密保持契約書（NDA）

A) 不正解。犯罪経歴証明書は、司法省→警視庁などの機関が発行するもので、個人が犯罪を犯していないことを示すものです。
B) 正解。行動規範とは、従業員に適用される会社のポリシーを記した文書であり、従業員向けマニュアルの一部として含まれることが多くあります。（参考文献：A、6.2章）
C) 不正解。GDPRは、個人情報の保護を目的としています。
D) 不正解。NDAは、特定の情報の開示を禁止する契約であり、会社のメールアドレスを私的な目的で使用することは、このような文書では管理されません。

25 / 40
従業員がインシデントを発見した場合、通常、**最初に**報告すべきなのは誰ですか？

A) ヘルプデスク
B) 情報セキュリティ管理者
C) 情報セキュリティ責任者（ISO）
D) マネージャー（管理者）

A) 正解。通常、インシデントはヘルプデスクに報告します。ここで評価と初期対応が適用され、必要に応じてエスカレーションされます。すぐに垂直的エスカレートすべきではありません。（参考文献：A、6.8章）
B) 不正解。インシデントはすぐに垂直的エスカレートすべきではありません。また、すべてのインシデントがセキュリティインシデントになるわけではありません。最初にヘルプデスクでインシデントを評価し、セキュリティインシデントであるかどうかを判断する必要があります。
C) 不正解。インシデントはすぐに垂直的エスカレートすべきではありません。また、すべてのインシデントがセキュリティインシデントになるわけではありません。最初にヘルプデスクでインシデントを評価し、セキュリティインシデントであるかどうかを判断する必要があります。
D) 不正解。インシデントはすぐに垂直的エスカレートすべきではありません。

26 / 40
従業員の情報セキュリティに対する意識を向上するために、**最も効果的な方法**は何ですか？

A) 管理層への意識向上トレーニングに注力する
B) 全社員を外部の情報セキュリティトレーニングに参加させる
C) 組織固有の意識向上プログラムを設定する
D) 一般的なオンラインの情報セキュリティトレーニングコースを利用する

A) 不正解。管理層だけでなく、すべての従業員が情報セキュリティに対する意識を向上する必要があります。
B) 不正解。外部のトレーニングは、特定の組織のニーズに完全に一致していない場合があります。
C) 正解。組織の特定のニーズに合わせたセキュリティ意識向上プログラムを実行することが最も効果的です。（参考文献：A、6.3章）
D) 不正解。一般的な情報セキュリティトレーニングは、特定の組織のニーズに完全に一致していない場合があります。

27 / 40
組織の情報へのアクセスを管理する物理的な管理策とは何ですか？

A) 空調の設置
B) USBメモリの使用の禁止
C) ユーザ名とパスワードの入力の要求
D) 割れにくいガラスの使用

A) 不正解。空調は組織の情報へのアクセスを管理するものではありません。
B) 不正解。これは組織的な管理策です。
C) 不正解。これは技術的な管理策です。
D) 正解。割れにくいガラスの使用は、許可のない人物が不正に侵入することを防ぐ物理的な管理策の一例です。（参考文献：A、7.4章）

28 / 40
データセンターでバッテリーパックを使用していますが、発電機はありません。

この設定におけるデータセンターの可用性のリスクを正しく説明しているのはどれですか？

A) 復旧時には発電機が必要となるため、主電源が自動的に復旧しない場合がある。
B) 主電源の停電が数分または数時間以上続く場合、電力が利用できなくなることがある。
C) バッテリーパックの寿命には限りがあるため、2～3日後にディーゼル燃料が切れて機能しなくなる可能性がある。
D) 数時間後には、発電機からバッテリーパックに給電する必要があるため、限られた保護しか提供できない。

A) 不正解。発電機は主電源を回復するために使用されません。
B) 正解。バッテリーパックは、停電や電力サージに対する一時的な保護を提供するのに対し、発電機は長時間の停電に対する保護を可能にします。（参考文献：A、7.11.1章）
C) 不正解。発電機の動力にはディーゼルが使用され、バッテリーパックはバッテリーによって電力が供給されます。
D) 不正解。バッテリーパックは短時間しか使用できませんが、発電機から給電されるわけではありません。発電機はバッテリーパックを引き継ぐだけです。

29 / 40
サーバ室に空調が設置されているのはなぜですか？

A) バックアップのテープは、薄いプラスチックでできているため、高温環境に耐えることができない。そのため、サーバルームが高温になると、破損する恐れがある。
B) サーバルームで作業する従業員が、室温が高い中で作業しないようにするため。高温の環境では、ミスをする可能性を増加させる。
C) サーバルームを冷却し、機器で発生する熱を取り出す必要がある。また、室内の空気を除湿および清浄するため。
D) オフィスの空気を冷却するための機器を設置するには、サーバルームが最適である。このような大型機器によって、オフィススペースを犠牲にする必要はない。

A) 不正解。バックアップ用のテープは、サーバルームに保管すべきではありません。火災が発生すると、使用している情報もバックアップも消失します。
B) 不正解。これは、サーバルームに空調を設置する理由にはなりません。
C) 正解。物理的なセキュリティを検討する際、サーバルームは個別に対策を講ずる必要があります。サーバルームには、湿気や熱に弱く、自らも熱を発生する精密な機器が置かれています。（参考文献：A、7.11.2章）
D) 不正解。サーバルームは、オフィス全体の空調を管理する機器を設置する場所ではありません。

30 / 40
物理的なセキュリティでは、複数の保護リングを適用して、いくつかの対策を講じることができます。

保護リングでは**ないものは**どれですか？

A) 建物（ビルディング）リング
B) 中間（ミドル）リング
C) 安全な部屋（セキュアルーム）リング
D) 外壁（アウター）リング

A) 不正解。建物は敷地内へのアクセスに関連するリングです。
B) 正解。保護リングには、外壁リング、建物リング、作業室（ワークスペース）リング、安全な部屋リングの4つがあります。（参考文献：A、7.0.1章）
C) 不正解。安全な部屋リングは有効なゾーンであり、保護する必要がある資産を扱います。
D) 不正解。外壁リングは有効なゾーンであり、企業の構内周辺の領域を扱います。

31 / 40
資産を保護するための管理策は、その資産によって異なります。

資産とその資産を保護するための**最適な方法の組み合わせ**はどれですか？

A) 用紙への記入と署名によってフォーム（用紙）を保護する
B) 単一のユーザーにラップトップを割り当てることでラップトップを保護します
C) 暗号化を使用してUSBメモリスティックを保護する
D) バックアップを利用して、インターネット接続を保護する

A) 不正解。情報が記録された紙をファイリングすることは、適切な管理策ではありません。
B) 不正解。1人が1台のラップトップを使用することは良い対策ですが、これは最も適切な選択肢ではありません。ユーザーアカウント管理とパスワード管理策の方が優れた管理策です。
C) 正解。暗号化は、USBメモリスティックの安全性を確保するための有効な管理策です。多くの組織が、USBメモリに保存される情報の分類に関わらず、この管理策を利用しています。（参考文献：A、8.12章）
D) 不正解。バックアップの使用は、インターネット接続を保護する最善の直接的な方法ではありません。

32 / 40
情報セキュリティを考慮したシステム開発に役立つ情報セキュリティ管理策はどれですか？

A) サーバの冗長性を確実にする
B) 物理的な入室管理策を実施する
C) 従業員のバックグラウンドチェック（身元調査）を実施する
D) 情報資産のデータ分類を使用する

A) 正解。サーバの冗長化は、システム開発時に考慮する必要がある管理策です。（参考文献：A、8.14章）
B) 不正解。これは、情報セキュリティを強化するための有効な管理策ですが、システム開発とは関係がありません。
C) 不正解。これは、情報セキュリティを強化するための有効な管理策ですが、システム開発とは関係がありません。
D) 不正解。これは、情報セキュリティを強化するための有効な管理策ですが、システム開発とは関係がありません。

33 / 40
組織がポリシーを変更し、従業員がリモートで働くことが許可されるようになりました。

どのようなセキュリティ管理策を実施する必要がありますか？

A) V-LANを作成して企業ネットワークをセグメント化する
B) 企業ネットワーク上の情報を暗号化する
C) 企業ネットワークにファイアウォールを設置する
D) VPNを利用して企業ネットワークに接続する

A) 不正解。機密性と職務の分離を確保するためのネットワークのセグメント化は、すでに導入されていなければなりません。これらは、リモートワークポリシーの変更には特に関係はありません。
B) 不正解。暗号化は情報を保護するために必要なツールですが、従業員のリモートワークを許可するときに必ず適用されるわけではありません。
C) 不正解。企業ネットワークを保護するためのファイアウォールは重要ですが、すでに設置されている必要があります。また、ファイアウォールは、リモート接続を直接保護するものではありません。
D) 正解。VPNの利用は、従業員にリモートワークを許可するときに、導入するべき管理策です。（参考文献：A、8.2章）

34 / 40
ある組織の従業員が、非対称暗号で保護されているノートパソコンで仕事をしています。鍵を安価に管理できるように、すべてのコンサルタントが同じ鍵のペアを使用しています。

情報漏洩が発生した場合は、新しい鍵を提供する必要があります。

どのような場合に新しい鍵を提供する必要がありますか？

A) 秘密鍵が三者に知られた場合
B) 公開鍵が三者に知られた場合
C) 公開鍵基盤（PKI）が第三者に知られた場合

A) 正解。非対称暗号化では、秘密鍵を秘密のまま維持することが重要です。公開鍵は知られても構いません。（参考文献：A、8.24.5章）
B) 不正解。公開鍵は全世界に公開されている場合があります。秘密鍵は、完全性と可用性を確保するために秘密にしておく必要があります。
C) 不正解。PKIは非対称暗号システムの鍵を交換するために使用されます。

35 / 40
公開鍵基盤（PKI）が提供するセキュリティはどれですか？

A) PKIにより、企業データが定期的にバックアップされる。
B) PKIは、Webベースの取引が安全であることを顧客に示す。
C) PKIは、特定の公開鍵を使用するユーザまたはシステムを検証する。

A) 不正解。PKIは、バックアップの作成を保証するものではありません。
B) 不正解。PKIは、特定の公開鍵を使用するユーザまたはシステムを検証して保証します。
C) 正解。PKIの特徴は、契約、手続き、組織構造を通じて、特定の公開鍵を使用するユーザやシステムを検証して保証することです。（参考文献：A、8.24.6章）

36 / 40
ある機能を実行するように見せかけて、意図的に二次的な活動を実行するプログラムであるマルウェアのタイプはどれですか？

A) ロジックボム（論理爆弾）
B) スパイウェア
C) トロイの木馬
D) ワーム

A) 不正解。ロジックボムは、ソフトウェアシステムに組み込まれるたコードの一部です。このコードは、特定の条件が満たされたときに機能を実行します。必ずしも悪意のある目的で使用されるわけではなく、常に二次的な活動を行うわけでもありません。
B) 不正解。スパイウェアは、ユーザのコンピュータの情報を収集し、その情報を第三者に送信するコンピュータプログラムです。
C) 正解。トロイの木馬は、実行しているように見える機能に加えて、コンピュータユーザが気づかないうちに、感染したシステムの完全性を損なう可能性のある二次的な活動を意図的に実行するプログラムです。（参考文献：A、8.7.2章）
D) 不正解。ワームは自身を複製することで感染したコンピュータのネットワークを構築します。

37 / 40
自己複製により、複数のコンピュータを感染させネットワークを構築するマルウェアのタイプはどれですか？

A) ロジックボム（論理爆弾）
B) スパイウェア
C) トロイの木馬
D) ワーム

A) 不正解。ロジックボムは、ソフトウェアシステムに組み込まれるたコードの一部です。このコードは、特定の条件が満たされたときに機能を実行します。必ずしも悪意のある目的で使用されるわけではありません。
B) 不正解。スパイウェアは、コンピュータユーザの情報を収集し、その情報を第三者に送信するコンピュータプログラムです。
C) 不正解。トロイの木馬は、実行しているように見える機能に加えて、コンピュータユーザが気づかないうちに、感染したシステムの完全性を損なう可能性のある二次的な活動を意図的に実行するプログラムです。
D) 正解。これがワームの活動です。（参考文献：A、8.7章）

38 / 40
すべての組織に課せられる情報セキュリティに関する法律または規制はどれですか？

A) 一般データ保護規則（GDPR）
B) 知的財産（IP）権
C) ISO/IEC 27001
D) ISO/IEC 27002

A) 正解。すべての組織は、個人データ保護のためのポリシーと保護のための手順を確立すべきであり、これらのポリシーと手順は個人データを処理するすべての担当者が把握していなければなりません。（参考文献：A、5.33章）
B) 不正解。この規制は、組織の情報セキュリティとは関係ありません。
C) 不正解。これは、情報セキュリティに関するプロセスを設定する方法に関する組織向けのガイドラインを記載した規格です。
D) 不正解。この規格は、「情報セキュリティ、サイバーセキュリティおよびプライバシー保護 - 情報セキュリティ管理策」とも呼ばれ、情報セキュリティポリシーおよび管理策に関するガイドラインが記載されています。

39 / 40
情報セキュリティ管理策の実施に焦点を当てたISO規格はどれですか？

A) ISO/IEC 27000
B) ISO/IEC 27001
C) ISO/IEC 27002
D) ISO/IEC 27005

A) 不正解。これは、ISO/IEC 27000シリーズ規格の概略です。
B) 不正解。これは、情報セキュリティマネジメントシステム（ISMS）の要件が記載された規格です。
C) 正解。これは、情報セキュリティ管理策を規定し、実施するためのガイダンスを示した規格です。（参考文献：A、4.12章）
D) 不正解。ISO/IEC27005は、情報セキュリティのリスクマネジメントを中心とした規格です。

40 / 40
ヨーロッパで**最もよく使われている**のは、どの組織の標準ですか？

A) 米国国家規格協会（ANSI）
B) 国際標準化機構（ISO）
C) アメリカ国立標準技術研究所（NIST）

A) 不正解。ANSI規格は、米国においてより一般的です。
B) 正解。ヨーロッパでは、ISO規格が一般的です。（参考文献：A、5.36章）
C) 不正解。NIST規格は、米国においてより一般的です。

評価

次の表に、本模擬試験問題の正解を示します。

番号	正解	番号	正解
1	B	21	B
2	A	22	A
3	B	23	D
4	A	24	B
5	B	25	A
6	B	26	C
7	B	27	D
8	B	28	B
9	D	29	C
10	B	30	B
11	A	31	C
12	B	32	A
13	D	33	D
14	D	34	A
15	B	35	C
16	D	36	C
17	A	37	D
18	C	38	A
19	D	39	C
20	B	40	B

EXIN の連絡先

www.exin.com