PECB.ISO-IEC-27002-Foundation.v2026-08-04.q14

試験コード：	ISO-IEC-27002-Foundation
試験名称：	ISO/IEC 27002 Foundation Exam
認証ベンダー：	PECB
無料問題の数：	14
バージョン：	v2026-08-04
ページの閲覧量：	103
問題集の閲覧量：	140

https://www.jpnshiken.com/shiken/PECB.ISO-IEC-27002-Foundation.v2026-08-04.q14.html

質問: **1**
継続的改善とは何ですか？
A. 組織の方針と目標を達成するために、組織の有効性と効率性を向上させるプロセス
B. 何かの性質を調べたり、その本質的な特徴とその関係性を判断したりする方法
C. 検出された不適合を解消するために講じられた措置
正解: **(**正解を表示します**)**
継続的改善とは、組織の有効性と効率性を高め、方針や目標をより良く達成するためのプロセスです。情報セキュリティにおいては、改善は単一の欠陥を修正することだけにとどまりません。それは、管理、プロセス、責任、テクノロジー、意識、監視、および対応能力を継続的に洗練していくことです。オプションBは分析について説明していますが、これは改善をサポートする可能性はあるものの、定義ではありません。オプションCは不適合に対する是正措置または修正措置について説明していますが、これは改善のメカニズムの一つではあるものの、概念全体を網羅しているわけではありません。ISO/IEC 27002は、情報セキュリティインシデントからの学習、独立したレビュー、コンプライアンス監視、脅威インテリジェンス、脆弱性管理、変更管理、文書化された運用手順などの管理を通じて、継続的改善をサポートします。成熟した組織は、インシデント、監査、指標、ユーザー行動、サプライヤーのパフォーマンス、新たな脅威、およびビジネスの変化からの証拠を使用して、管理を調整します。重要な考え方は、適合性、妥当性、および有効性の段階的な向上です。したがって、オプションAは、管理システムおよびISO/IEC 27002の管理ロジックに合致しています。参照/章: ISO/IEC 27002:2022、コントロール 5.27 情報セキュリティインシデントからの学習、コントロール 5.35 情報セキュリティの独立レビュー、コントロール 8.8 技術的脆弱性の管理。

質問: **2**
次のうち、サイバースペースにおける組織資産の例はどれですか？
A. 医療データ
B. デジタル顧客ID
C. 知的財産
正解: **(**正解を表示します**)**

デジタル顧客IDは、サイバースペースにおける組織資産の最良の例です。なぜなら、デジタルシステム、ネットワーク、アプリケーション、およびオンラインサービス内で存在し、機能し、保護されているからです。ISO/IEC 27002では、ID、認証情報、アクセス権、およびデジタルアカウントを重要なセキュリティ対象として扱っています。IDが侵害されると、不正アクセス、詐欺、なりすまし、プライバシー侵害、および説明責任の喪失につながる可能性があるためです。デジタル顧客IDには、ユーザー名、識別子、資格情報、アカウント属性、認証要素、アクセス権限、プロファイルデータ、およびリンクされた個人情報が含まれます。医療データや知的財産も重要な情報資産ですが、 "サイバースペースにおける資産」という表現は、電子的なやり取りに使用されるデジタル表現されたIDを最も直接的に指しています。ISO/IEC 27002には、ID管理、認証情報、アクセス権、セキュア認証、およびアクセス制限など、このタイプの資産を保護するための複数の管理策が含まれています。これらの管理策により、IDが管理された方法で作成、維持、検証、変更、無効化、および削除されることが保証されます。したがって、試験の論理では、サイバースペースがデジタルIDとオンライン表現を重視しているため、オプションBが有利となります。参考文献
/章: ISO/IEC 27002:2022、コントロール 5.16 ID 管理、コントロール 5.17 認証情報、コントロール 5.18 アクセス権限、コントロール 8.5 安全な認証。

質問**: 3**
組織が情報セキュリティをプロジェクト管理に組み込むべき理由は？
A. プロジェクトおよび成果物に関連するISO/IEC 27001の原則の効果的な適用を確保する
B. プロジェクトおよび成果物に関する情報セキュリティ監査が定期的に実施されることを保証する。
C. プロジェクトおよび成果物に関連する情報セキュリティリスクが効果的に対処されるようにする
正解**: C (**コメントを発表する**)**
情報セキュリティはプロジェクト管理に統合されるべきであり、そうすることでプロジェクトおよび成果物に関連するセキュリティリスクに効果的に対処できます。プロジェクトでは、新しいシステム、プロセス、サプライヤー、データフロー、テクノロジー、アプリケーション、設備、またはビジネス変更が導入されることがよくあります。セキュリティが実装後にのみ検討される場合、設計、アーキテクチャ、契約、コード、構成、または運用手順に既に脆弱性が組み込まれている可能性があります。ISO/IEC 27002 コントロール 5.8 では、情報セキュリティをプロジェクト管理活動に統合し、プロジェクトライフサイクル全体を通してリスクを特定して対処することが求められています。これには、セキュリティ要件、リスク評価、役割と責任、受け入れ基準、テスト、サプライヤー要件、プライバシーに関する考慮事項、変更管理、および安全な運用への移行が含まれます。
オプションAは一般的すぎ、管理の具体的な目的ではなくISO/IEC 27001の原則の適用に焦点を当てています。オプションBは狭すぎます。監査は保証をサポートすることはできますが、統合の主な理由ではありません。主な目的は、プロジェクトおよび成果物内のリスク管理です。したがって、オプションCが検証されました。参照/章: ISO/IEC 27002:2022、管理

5.8 プロジェクト管理における情報セキュリティ、管理8.26 アプリケーションセキュリティ要件、管理8.29 開発および受入におけるセキュリティテスト。

質問: **4**
ある組織が、許可された従業員のみが機密ファイルにアクセスできるようにするアクセス制御ソフトウェアを使用しています。これはどのような種類の制御でしょうか？
A. 探偵
B. 矯正
C. 予防
正解: **(**正解を表示します**)**
機密ファイルへのアクセスを許可された従業員のみに許可するアクセス制御ソフトウェアは、予防的制御策である。
その目的は、承認されたアクセス規則を適用することにより、不正アクセスが発生する前に阻止することです。ISO/IECでは
27002、アクセス制御は、ポリシー、ID管理、認証、認可、アクセス権限レビュー、特権アクセス制御、および情報アクセス制限を通じて実装されます。この種のソフトウェアは、機密データの不正開示、不正改ざん、悪用、プライバシーまたは契約上の義務違反を防止できます。これは、単に発生した事象を発見するだけでなく、主に検出機能を持つソフトウェアではありません。また、破損した情報を復元したり、インシデントの影響を元に戻したりするものではないため、是正機能を持つソフトウェアでもありません。そのセキュリティ上の価値は、認可基準を満たさないアクセス試行をブロックすることにあります。
制御の背後にある原則は最小権限です。つまり、ユーザーは自分の役割と責任に必要なアクセス権のみを与えられるべきです。機密性の高いファイルの場合、機密性、完全性、説明責任は適切な認証に依存するため、これは特に重要です。参照/章: ISO/IEC 27002:2022、制御5.15 アクセス制御、制御5.16 ID管理、制御5.18 アクセス権、制御8.3 情報アクセス制限。

質問: **5**
時計の同期が難しくなるのはどのような場合ですか？
A. オンプレミスサービスのみを使用する場合
B. 複数のクラウドサービスを使用する場合
C. AとBの両方
正解: **B (**コメントを発表する**)**
複数のクラウドサービスを使用する場合、クロックの同期は困難になることがあります。ISO/IEC 27002 管理基準8.17では、情報処理システムのクロックは承認された時刻ソースに同期させるべきであると強調しています。
正確な時刻は、ログ記録、監視、インシデント調査、トランザクションの整合性、フォレンジック分析、認証、証明書の検証、およびイベント相関に不可欠です。シンプルなオンプレミス環境では、組織は内部NTPサーバーまたはドメインサービスを使用してタイムソースを一元管理できます。マルチクラウド環境では、システムは異なるプロバイダー、リージョン、プラットフォーム、マネージドサービス、コンテナ、サーバーレス関数、およびサード

パーティのログシステムにまたがる可能性があります。各環境には、異なる時刻設定、タイムソース制御、管理アクセス制限、タイムゾーン処理、タイムスタンプ形式、およびログの精度がある場合があります。これにより、一貫した同期と相関がより困難になります。オプションAは、「オンプレミスサービスのみ」の場合、通常は単一の管理モデルの下で同期が容易になるため、最適な回答ではありません。オプションCは、同期が困難になる場合を尋ねているため、広すぎる回答です。
ISO/IEC 27002試験のロジックは、複数のクラウドサービスを指し示しています。参照/章: ISO/IEC 27002:2022、管理
8.17 クロック同期; 制御 8.15 ロギング; 制御 5.23 クラウドサービス利用時の情報セキュリティ。

質問: **6**
以下の状況のうち、情報の機密性が侵害されたことを示しているのはどれですか？
A. 組織の全部門の従業員は、同僚の個人データにアクセスできます。
B. 機器の故障により、カスタマーサービス部門はお客様の電話番号にアクセスできません。
C. ある組織の財務部の従業員の一人が、誤って他の従業員の銀行口座情報を変更してしまった。
正解: **(**正解を表示します**)**
機密保持は、情報が権限のない個人、組織、またはプロセスに提供または開示された場合に侵害されます。オプションAが正解です。なぜなら、人事、給与、コンプライアンス、または指定された管理職など、通常は権限のある役割に限定されるべきアクセスであっても、すべての部門の従業員が同僚の個人データにアクセスできるからです。役割がアクセスを正当化しない場合、内部ユーザーは権限のないユーザーになる可能性があります。ISO/IEC 27002は、アクセス制御、アクセス権限管理、分類、プライバシー保護、および情報アクセス制限によってこの問題に対処しています。オプションBは、機器の故障により部門が必要な顧客の電話番号にアクセスできないため、可用性の問題です。オプションCは、銀行情報が誤って変更されたため、完全性の問題です。機密保持の原則は、情報の開示と利用可能性を権限のある当事者のみに制限することに特化しています。個人データは、プライバシー義務が適用される可能性があり、過剰な内部アクセスが法的、倫理的、および評判上の損害を引き起こす可能性があるため、特別な注意が必要です。したがって、検証済みの回答はオプションAです。参照/章: ISO/IEC 27002:2022、コントロール5.15 アクセス制御、コントロール5.18 アクセス権限、コントロール5.34 プライバシーと個人情報の保護、コントロール8.3 情報アクセス制限。

質問: **7**
ある組織の一部の従業員は、データ処理手順が複雑だと感じており、効果的に手順に従うのに苦労しています。この場合、組織は次のうちどの脅威に直面しているでしょうか？
A. 従業員によるデータ入力エラー

B. ハッキング
C. 情報窃盗
正解: **(**正解を表示します**)**
この状況は、従業員によるデータ入力エラーという、人的要因に起因する運用上の脅威を示しています。根本原因は、悪意のある外部からの攻撃や盗難ではなく、従業員が複雑な処理手順を確実に実行できないことにあります。ISO/IEC 27002では、情報セキュリティには、人材、能力、意識、および文書化された手順が不可欠であると認識されています。手順が不明確、過剰、または実行が困難な場合、従業員は誤ったデータを入力したり、フィールドを省略したり、間違ったカテゴリを選択したり、分類を誤って処理したり、情報を誤って転送したり、意図せず記録を破損したりする可能性があります。これは主に、情報がもはや正確または完全ではなくなる可能性があるため、データの完全性を脅かします。ハッキングは、不正な技術的侵入を伴い、情報盗難は、意図的な不正な情報取得または開示を伴います。どちらもこのシナリオには記載されていません。
ISO/IEC 27002 は、情報セキュリティ意識、教育および訓練、文書化された運用手順、明確な責任、および適切な職務分掌を通じて、この種のリスクに対処します。効果的な管理策は、正しい行動を単に文書化するだけでなく、実践的かつ再現可能なものにする必要があります。したがって、検証済みの回答はオプション A です。参照/章: ISO/IEC 27002:2022、管理策 6.3 情報セキュリティ意識、教育および訓練、管理策 5.37 文書化された運用手順、管理策 5.3 職務分掌。

質問: **8**
ISO/IEC 27002によると、次の記述のうち正しいものはどれですか？
A. 機器は、環境的および物理的な脅威によるリスクを軽減するために、安全な場所に設置し、保護する必要があります。
B. 本機器は停電やその他の障害の影響を受けません
C. サポートユーティリティは、プロセスの開始時にのみテストする必要があります。
正解: **(**正解を表示します**)**
ISO/IEC 27002 では、物理的および環境的脅威によるリスクを軽減する方法で機器を配置および保護することを要求しています。これらの脅威には、火災、洪水、粉塵、振動、電気的干渉、不正アクセス、電力の不安定性、極端な温度、およびその他の環境上の危険が含まれます。オプション A は、機器の安全な配置と保護が情報処理施設の機密性、完全性、および可用性を維持するために不可欠であるため、正しいです。オプション B は、機器が停電、ユーティリティの中断、電圧変動、過熱、および関連する事象によって確実に影響を受ける可能性があるため、誤りです。オプション C は、サポートユーティリティは、開始時だけでなく、時間の経過とともに適切に維持、監視、およびテストする必要があるため、誤りです。ISO/IEC 27002 の物理的管理では、技術システムが物理的環境に依存することを強調しています。サーバー、ネットワーク デバイス、ストレージ、およびエンドポイント システムには、適切な場所、電力、冷却、ケーブル保護、および回復力対策が必要です。機器の配置は、不正な閲覧、改ざん、盗難、および環境への暴露も軽減する必要があります。検証済みの

回答はオプションAです。これはISO/IEC 27002の物理的保護の目的を反映しているためです。参照/章: ISO/IEC 27002:2022、管理7.8 機器の配置と保護、管理7.5 物理的および環境的脅威からの保護、管理
7.11 サポートユーティリティ。

質問: **9**
コントロール5.7 脅威インテリジェンス」は、どのコントロールグループに属しますか？
A. 技術的
B. 人々
C. 組織
正解: **C** (コメントを発表する)
コントロール5.7 脅威インテリジェンス」は、組織コントロールグループに属します。ISO/IEC 27002:2022では、コントロールは条項ごとに整理されています。条項5には組織コントロール、条項6には人的コントロール、条項7には物理的コントロール、条項8には技術的コントロールが含まれています。脅威インテリジェンスは、組織全体のガバナンス、意思決定、リスク認識、計画、優先順位付け、およびセキュリティ戦略をサポートするため、組織コントロールに分類されます。脅威インテリジェンスは、既存または新たな脅威に関する情報を収集、分析、使用することで、組織がリスクを軽減し、コントロールを改善できるようにします。脅威インテリジェンスは、脆弱性管理、インシデント対応、監視、サプライヤーリスク管理、意識向上トレーニング、セキュリティアーキテクチャ、およびリスク対策計画に影響を与える可能性があります。脅威インテリジェンスは技術ツールを使用する場合があります。しかし、その主な目的はセキュリティに関する意思決定と準備を支援することであるため、ISO/IEC 27002では組織コントロールに分類されます。オプションAは、技術的コントロールが条項8であるため誤りです。オプションBは、人的コントロールが条項6であるため誤りです。正解はオプションCです。参照/章 :ISO
/IEC 27002:2022、第5項 組織的統制、統制5.7 脅威インテリジェンス、第4項 規格の構成。

質問: **10**
組織は、対応する脅威が存在しない脆弱性を検出した場合、どうすべきでしょうか？
A. 脆弱性を認識する
B. AとCの両方
C. 脆弱性の変化を監視する
正解: (正解を表示します)
現在、対応する脅威が特定されていない脆弱性であっても、認識し監視する必要があります。脆弱性とは悪用される可能性のある弱点ですが、リスクは通常、資産、脅威、脆弱性、発生可能性、および結果の関係によって決まります。現在活動中の脅威や関連する脅威が特定されていない場合、即時の対応は適切ではない可能性があります。しかし、脆弱性を無視することは、ISO/IEC 27002のリスク認識型アプローチと矛盾します。脅威の状況は変化します。今日優先度が低いと思われる弱点も、新たな攻撃手法、システムへの露出、ビジネス

の変化、サプライヤーの変更、または脅威アクターの能力の出現後に悪用可能になる可能性があります。脆弱性を認識することで、記録され、将来の評価に利用できるようになります。脆弱性を監視することで、組織は悪用可能性、露出、または脅威の関連性の変化を検出できます。ISO/IEC 27002は、脅威インテリジェンスと技術的脆弱性の管理を通じてこれをサポートしており、どちらも組織が脅威と脆弱性の状況の変化に常に注意を払うことを要求します。したがって、正しい答えは、脆弱性を認識し監視することです。参考文献/章: ISO/IEC 27002:2022、管理策 5.7 脅威インテリジェンス、管理策 8.8 技術的脆弱性の管理、管理策 5.36 情報セキュリティに関する方針、規則、および標準の遵守。

質問: **11**
組織が情報セキュリティ管理へのアプローチが適切かつ十分で効果的であり続けることを保証するために、以下のどの管理策を実施すべきでしょうか？
A. 管理5.4 管理責任
B. 管理5.35 情報セキュリティの独立レビュー
C. コントロール5.24 情報セキュリティインシデント管理の計画と準備
正解: **B** (コメントを発表する)
管理策5.35 「情報セキュリティの独立レビュー」は、組織の情報セキュリティ管理手法が適切かつ十分で効果的であり続けることを保証するための管理策です。
独立レビューは、方針、プロセス、統制、責任、および実施が、事業ニーズ、リスク、法的要件、および組織のセキュリティ目標と整合しているかどうかを客観的に評価します。レビューでは、ガバナンス、統制設計、統制運用、リスク処理、コンプライアンス、インシデント傾向、技術変化、サプライヤー依存、および監査結果が検討される場合があります。統制5.4 「管理者の責任」は、管理者が従業員が方針と手順に従ってセキュリティを適用することを保証する必要があるため重要ですが、独立レビューに特化して焦点を当てた統制ではありません。
コントロール 5.24 は、インシデント管理の計画と準備に関するもので、対応能力をサポートするものですが、セキュリティ アプローチ全体の継続的な適合性を広く評価するものではありません。 「適切、十分かつ効果的」という表現は、レビューと保証の強力な指標です。ISO/IEC 27002 では、独立したレビューを使用して、前提を検証し、弱点を検出し、継続的な改善をサポートします。したがって、オプション B が検証済みの回答です。参照/章: ISO/IEC 27002:2022、コントロール 5.35 情報セキュリティの独立したレビュー、コントロール 5.36 情報セキュリティに関するポリシー、ルール、および標準の遵守、コントロール 5.4 管理者の責任。

質問: **12**
ISO/IEC 27002のコントロール8.20 「ネットワークセキュリティ」の目的は何ですか？
A. ネットワークおよびそのサポート情報処理設備内の情報を、ネットワークを介した侵害から保護する
B. ネットワークサービスの利用におけるセキュリティを確保するため

C. セキュリティ境界でネットワークを分割する
正解: **(**正解を表示します**)**
コントロール 8.20 「ネットワーク セキュリティ」の目的は、ネットワークおよびそれをサポートする情報処理設備内の情報を、ネットワークを介した侵害から保護することです。これには、転送中のデータ、ネットワーク デバイス、ネットワーク サービス、通信パス、ルーティング、管理インターフェイス、および接続されたシステムの保護が含まれます。ネットワークの侵害は、不正アクセス、傍受、マルウェアの拡散、サービス拒否、横方向の移動、データの漏洩、またはトラフィックの操作につながる可能性があります。オプション B は、ネットワーク サービスのセキュリティ メカニズム、サービス レベル、および管理要件を扱うコントロール 8.21 「ネットワーク サービスのセキュリティ」により密接に関連しています。オプション C は、ネットワークをセキュリティ境界またはドメインに分割することに特に関係するコントロール 8.22 「ネットワークの分離」に関連しています。コントロール 8.20 はより広範で、ネットワークを侵害から保護するという一般的な目的を確立しています。ISO/IEC 27002 では、組織がアーキテクチャ、監視、認証、必要に応じた暗号化、デバイスの強化、およびネットワーク管理機能の保護など、リスクに応じてネットワークを管理および制御することを期待しています。
したがって、正解はオプションAです。参照/章: ISO/IEC 27002:2022、コントロール8.20 ネットワークセキュリティ、コントロール8.21 ネットワークサービスのセキュリティ、コントロール8.22 ネットワークの分離。

質問: **13**
組織は大規模ネットワークのセキュリティをどのように管理できるのか？
A. ネットワークを個別のネットワークドメインに分割し、パブリックネットワークから分離することによって
B. ネットワークを個別のネットワークドメインに分割し、それらをパブリックネットワークに含めることによって
C. 情報サービス、ユーザー、情報システムを大規模ネットワークに統合することを避けることで
正解: **(**正解を表示します**)**
組織は、大規模ネットワークを複数のネットワークドメインに分割し、必要に応じてパブリックネットワークから分離することで、ネットワークのセキュリティを管理できます。これは、攻撃者、マルウェア、または不正ユーザーがネットワーク環境内を自由に移動する能力を低減するネットワーク分離の原則に基づいています。ドメインは、信頼レベル、業務機能、システムの重要度、データの機密性、ユーザーグループ、サプライヤーのアクセス権限、開発環境、または規制要件に基づいて分割できます。ISO/IEC 27002は、ネットワークセキュリティ、ネットワーク分離、アクセス制御、およびセキュアアーキテクチャの実践を通じて、この原則をサポートしています。
選択肢Bは、内部ドメインをパブリックネットワークに含めると、露出が増加し、境界が弱まるため誤りです。選択肢Cは現実的ではなく、現代のエンタープライズアーキテクチャに

も合致していません。組織は統合されたサービス、ユーザー、システムを必要とすることが多いですが、それらを安全に統合する必要があります。セグメンテーションは、ファイアウォール、ゲートウェイ、ルーティングルール、アクセス制御、監視、フィルタリングを通じて、制御された通信を可能にします。目的は、分離そのものにあるのではなく、リスクに基づいた分離と制御された接続です。
したがって、オプションAが検証されました。参照/章 :ISO/IEC 27002:2022、コントロール8.20 ネットワークセキュリティ、コントロール8.22 ネットワークの分離、コントロール5.15 アクセス制御。

質問: **14**
PIIコントローラーとは何ですか？
A. 個人情報が関係する自然人
B. 個人がデータを個人的な目的で使用する場合に加え、個人情報の処理目的と手段を決定するプライバシー関係者
C. 個人情報管理者の指示に従い、その代理として個人情報を取り扱うプライバシー関係者
正解: **(**正解を表示します**)**
PII コントローラーは、個人識別情報の処理目的と手段を決定するプライバシーの利害関係者です。つまり、コントローラーは、PII が処理される理由、必要な PII の種類、処理方法、保持期間、受領者、および必要な制御を決定します。オプション A は、PII の対象となる自然人である PII プリンシパルについて説明します。オプション C は、コントローラーの指示に従って PII を処理する PII プロセッサーについて説明します。ISO/IEC 27002 は、プライバシー義務が適用される場合の情報セキュリティ管理ガイダンスの一部として、プライバシーと PII の保護を含めています。コントローラーは、合法で安全かつ適切な処理について意思決定責任と説明責任を負っているため、この区別は重要です。プロセッサーは情報を保護する必要がありますが、処理目的を独自に決定することはできません。関連する制御には、プライバシーと PII の保護、アクセス制御、サプライヤーとの関係、情報の削除、データのマスキング、データ漏洩の防止、およびクラウド サービス制御が含まれます。したがって、検証済みの回答はオプションBです。参照/章: ISO/IEC 27002:2022、コントロール5.34 プライバシーと個人情報の保護、コントロール5.19 サプライヤー関係における情報セキュリティ、コントロール8.11 データマスキング。

ス、https://www.jpntest.com/shiken/ISO-IEC-27002-Foundation-mondaishu　**42**問、３０％ディスカウント、特別な割引コード: **JPNshiken**」