準備ガイド

2024 年 04 月版

目次

1. 概要

EXIN Information Security Foundation based on ISO/IEC 27001 (ISFS.JP)

範囲

EXIN Information Security Foundation based on ISO/IEC 27001 認定は、専門家が自社環境に適用する情報セキュリティの原則と概念を理解し、リスクを軽減する方法を把握していることを確認します。

本認定の対象トピック：
- 情報とセキュリティ
- 脅威とリスク
- セキュリティ管理策
- 法律、規制、規格

要約

経済のグローバル化に伴って、膨大な情報がやり取りされるようになっています。これらの情報は、国境を越えるだけでなく、プライベートな領域とビジネス領域との間の細かい境界線をも超えることがあります。管理される情報が増大するとともに、説明責任の範囲も広がっています。情報セキュリティ管理の国際標準である ISO/IEC 27001 は、広く尊重及び参照されている規格であり、情報セキュリティプログラムの組織と管理のためのフレームワークを提供しています。

EXIN Information Security Management based on ISO/IEC 27001 プログラムでは、情報セキュリティを「情報の機密性、完全性、可用性を維持すること」と定義しています。

EXIN Information Security Foundation based on ISO/IEC 27001 は、情報セキュリティの基本的な概念とそれらの関係についてテストします。このモジュールの目的は、情報は重要であると同時にぜい弱であるという意識を高め、情報を保護するために必要な管理策を習得することです。

背景

EXIN Information Security Foundation based on ISO/IEC 27001 認証は、EXIN Information Security Management based on ISO/IEC 27001 資格プログラムの一部です。

対象グループ

EXIN Information Security Foundation based on ISO/IEC 27001 認定は、情報を処理する組織内のすべての人を対象としています。この認定はまた、情報セキュリティについての基本的な知識が求められる中小企業の経営者にも適しています。この認定は、情報セキュリティプロフェッショナルを新たに目指す方にとって、最適です。

認定のための要件

- EXIN Information Security Foundation based on ISO/IEC 27001 試験の合格。

試験の詳細内容

試験の形式:	多肢選択形式
問題数:	40
合格点:	65%（26/40 問題）
参考書の持ち込み:	不可
ノートをとる:	不可
電子機器の持ち込み:	不可
試験時間:	60 分

EXIN の試験規則はこの試験に適用されます。

ブルームレベル

EXIN Information Security Foundation based on ISO/IEC 27001 認定では、ブルームの改訂版タキソノミーに基づき、ブルームレベル 1 およびレベル 2 で受験者をテストします。

- ブルームレベル１：記憶すること。情報を思い出すことに依存します。受験者は、吸収し、記憶し、認識して思い出すことを必要とします。
- ブルームレベル２：理解すること。記憶よりも上のステップです。理解とは、受験者は提示された内容を把握しており、その学習教材が自分の環境でどのように応用可能かを評価できるということを示します。この種の出題問題は、受験者が事実やアイデアの正しい説明を体系化、比較、解釈及び選択できることを証明することを目的としています。

トレーニング

授業時間

この教育コースの推奨受講時間は 14 時間です。この中にグループ課題、試験準備、休憩なども含まれます。時間の中に含まれないのは、ランチ時間、宿題、試験時間です。

学習時間の目安

56 時間（2 ECTS）、個人が習得している知識によります。

教育事業者

認定教育事業者のリストを www.exin.com で参照できます。

2. 試験要件

試験要件は、試験仕様に明記されています。以下の表にモジュールトピック（試験要件）とサブトピック（試験仕様）の一覧を示します。

試験要件	試験仕様	配分
1. 情報とセキュリティ		**27.5%**
	1.1 情報に関する概念	10%
	1.2 情報の信頼性の側面	7.5%
	1.3 組織における情報の保護	10%
2. 脅威とリスク		**12.5%**
	2.1 脅威とリスク	12.5%
3. セキュリティ管理策		**52.5%**
	3.1 セキュリティ管理策の概要	2.5%
	3.2 組織的管理策	15%
	3.3 人的管理策	7.5%
	3.4 物理的管理策	10%
	3.5 技術的管理策	17.5%
4. 法律、規制、規格		**7.5%**
	4.1 法律と規制	2.5%
	4.2 規格	5%
	合計	**100%**

試験仕様

1　情報とセキュリティ

1.1　情報に関する概念

次のことが行える...

1.1.1　データと情報の違いを説明する。

1.1.2　情報セキュリティマネジメントの概念を説明する。

1.2　情報の信頼性の側面

次のことが行える...

1.2.1　情報セキュリティの 3 つの要素「CIA」を説明する。

1.2.2　説明責任と監査（適合）性の概念を説明する。

1.3　組織における情報の保護

次のことが行える...

1.3.1　情報セキュリティポリシーの目的と内容を概要する。

1.3.2　サプライヤーと協力する際に、情報セキュリティを確保する方法を説明する。

1.3.3　情報セキュリティに関連する役割と責任を概要する。

2　脅威とリスク

2.1　脅威とリスク

次のことが行える...

2.1.1　脅威、リスク、リスクマネジメントを説明する。

2.1.2　損害のタイプを説明する。

2.1.3　リスク戦略を説明する。

2.1.4　リスク分析を説明する。

3　セキュリティ管理策

3.1　セキュリティ管理策の概要

次のことが行える...

3.1.1　各種のセキュリティ対策の例を示す。

3.2　組織的管理策

次のことが行える...

3.2.1　情報資産の分類方法を説明する。

3.2.2　情報へのアクセス管理をするための管理策を説明する。

3.2.3　情報セキュリティにおける脅威とぜい弱性管理、プロジェクト管理、インシデント管理を説明する。

3.2.4　事業継続の価値を説明する。

3.2.5　監査とレビューの価値を説明する。

3.3　人的管理策

次のことが行える...

3.3.1　契約や合意を通じて情報セキュリティを強化する方法を説明する。

3.3.2　情報セキュリティに関する意識を向上する方法を説明する。

3.4　物理的管理策

次のことが行える...

3.4.1　物理的入退室管理を説明する。

3.4.2　安全なエリアでの情報を保護する方法を説明する。

3.4.3　保護リングの仕組みを説明する。

3.5　技術的管理策

次のことが行える...

3.5.1　情報資産の管理方法を説明する。

3.5.2　情報セキュリティを念頭に置いたシステム開発の方法を説明する。

3.5.3　ネットワークセキュリティ管理策を言及してする。

3.5.4　アクセス管理のための技術的管理策を説明する。

3.5.5　マルウェア、フィッシング、スパムから情報システムを保護する方法を説明する。

3.5.6　情報セキュリティにおける記録と監視の役割を説明する。

4　法律、規制、規格

4.1　法律と規制

次のことが行える...

4.1.1　情報セキュリティに関連する法律と規制の例を示す。

4.2　規格

次のことが行える...

4.2.1　ISO/IEC 27000、ISO/IEC 27001、ISO/IEC 27002 規格を概要する。

4.2.2　情報セキュリティに関連する他の規格を概要する。

3. 基本概念の一覧

この章では、認定候補者が習熟しておく必要がある用語と略語を示します。

これらの用語の知識だけでは試験に十分ではないことに注意してください。受験者は、その概念を理解し、例を提示できる必要があります。

英語	日本語
access control	アクセス制御
accountability	説明責任
responsibility	責任
annualized loss expectancy (ALE)	年間損失見込額 (annualized loss expectancy, ALE)
annualized rate of occurrence (ARO)	年間発生率 (annualized rate of occurrence, ARO)
asset	資産
auditability	可監査性
authentication	認証
authorization	認可
availability	可用性
backup	バックアップ
biometrics	生体認証
business continuity management (BCM)	事業継続管理 (BCM)
certificate	証明書
change management	変更管理
chief information security officer (CISO)	最高情報セキュリティ責任者 (CISO)
classification	分類
code of conduct	行動規範
compliance	コンプライアンス (順守)
confidentiality	機密性
controls	管理策
• corrective	• 是正的
• detective	• 検知的
• insurance	• 保険
• preventive	• 予防的
• reductive	• 軽減的
• repressive (suppressive)	• 制止的 (抑圧的)
cryptography	暗号
cyber crime	サイバー犯罪
damage	損害
• direct damage	• 直接損害
• indirect damage	• 間接損害
data	データ
digital signature	ディジタル署名
due care	デュー・ケア (due care)
due diligence	デューディリジェンス (due diligence)
escalation	エスカレーション
exposure	露出
(business) impact	(ビジネス) 影響
incident cycle	インシデントサイクル
information	情報
information analysis	情報分析

information management	情報管理
information security management system (ISMS)	情報セキュリティマネジメントシステム（ISMS）
information security manager (ISM)	情報セキュリティ管理者
information security officer (ISO)	情報セキュリティ責任者（ISO）
information security policy	情報セキュリティポリシー
information security strategy	情報セキュリティ戦略
information system	情報システム
integrity	完全性
likelihood	可能性
non-disclosure agreement (NDA)	秘密保持契約書（NDA）
Plan, Do, Check, Act (PDCA)	計画、実行、評価、改善（PDCA）
personally identifiable information (PII)	個人識別情報（PII）
phishing	フィッシング
privacy	プライバシー
protection ring	保護リング
public key infrastructure (PKI)	公開鍵基盤（PKI）
reliability	信頼性
risk	リスク
risk analysis	リスク分析
• qualitative risk analysis	• 定性的リスク分析
• quantitative risk analysis	• 定量的リスク分析
risk assessment	リスクアセスメント
risk management	リスクマネジメント
risk strategy	リスク戦略
• risk avoiding	• リスク回避
• risk bearing (risk acceptance)	• リスク負担（リスク受容）
• risk neutral	• リスク中立
risk treatment	リスク対応
security incident	セキュリティインシデント
segregation of duties	職務の分離
single loss expectancy (SLE)	単一損失予想（SLE）
stand-by arrangement	スタンド・バイ取極
threat	脅威
• human threat	• 人的脅威
• non-human threat	• 非人的脅威
threat agent	脅威エージェント
validation	妥当性検証
verification	検証
virtual private network (VPN)	仮想プライベートネットワーク（VPN）
vulnerability	ぜい弱性

4. 文献

試験の参考文献

試験に必要な知識は、次の文献に記載されています。

A. Baars, H., Hintzbergen, J., and Hintzbergen, K.
Foundations of Information Security - Based on ISO 27001 and ISO 27002
Van Haren Publishing: 第 4 版、完全改訂版, 2023
ISBN: 978 94 018 0958 0（ハードコピー）
ISBN: 978 94 018 0959 7（電子ブック）
ISBN: 978 94 018 0960 3（電子的に公開）

参考文献の表

試験要件	試験仕様	参考文献
1. 情報とセキュリティ		
	1.1 情報に関する概念	章 3.1 – 3.3, 4.7 – 4.9
	1.2 情報の信頼性の側面	章 3.4, 4.4 – 4.6
	1.3 組織における情報の保護	章 4.2, 4.3, 4.11 – 4.14, 5.1 – 5.6, 5.14, 5.19 – 5.23, 5.35, 7.7, 7.9, 7.10, 8.30
2. 脅威とリスク		
	2.1 脅威とリスク	章 3.5, 3.7, 3.9 - 3.11
3. セキュリティ管理策		
	3.1 セキュリティ管理策の概要	章 3.8
	3.2 組織的管理策	章 3.6.2, 5.3, 5.7 - 5.18, 5.24 - 5.30, 5.35, 5.36, 6.8
	3.3 人的管理策	章 6
	3.4 物理的管理策	章 7
	3.5 技術的管理策	章 4.10, 8
4. 法律、規制、規格		
	4.1 法律と規制	章 5.31 - 5.34
	4.2 規格	章 1, 3.6, 3.12, 4.1, 4.12, 5.36

EXIN の連絡先

www.exin.com