準備ガイド

2018 年 04 月版

目次

1. 概要

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

範囲

EXIN ISO/IEC 27001 準拠 情報セキュリティファンデーションは、専門家の知識を証明する証明書です。

- 情報とセキュリティ：概念、情報の価値、および信頼性の重要性
- 脅威とリスク：脅威と信頼性の関係
- アプローチと組織：セキュリティ基本方針と、情報セキュリティの整備
- 対策：物理的、技術的、組織的
- 法律と規制：重要性と運用

試験サマリー

情報セキュリティとは、事業継続性を確実にし、事業リスクを最小にし、事業投資の回収と機会を最大にするために、幅広い脅威から情報を保護することです。

情報セキュリティマネジメント規格である ISO/IEC27001 は、国際規格として、広く認知され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に関する組織と管理の枠組みを提供します。この標準にもとづいてプログラムを実施することは、組織が今日の複雑な運営環境で直面する多くの要求事項を満たすというゴールを達成するために有効です。この標準について深く理解することは、あらゆる情報セキュリティのプロフェッショナルの自己啓発にとって重要です。

情報セキュリティモジュールでは次の定義が使用されています。情報セキュリティは、
定義、実施、保守、遵守および手動・自動による情報提供の可用性、完全性、機密性を保護する一連の管理(対策)を論じます。

情報セキュリティの重要性は増しています。経済のグローバル化により、組織（その従業員、顧客、およびサプライヤ）の間での情報交換や、社内ネットワーク、他社のネットワークやインターネットとの接続などのネットワークの利用が増加しています。
ほかにも、関連するトレンドとして、次のものがあります。

- 情報セキュリティ分野の（国際）規格および認証
- （IT）マネジメントのコンピュータ化の傾向
- 自動化されたセキュリティ・ツールの開発
- リモート制御
- 管理業務のアウトソーシング
- 法令遵守

ISO/IEC 27001 準拠 情報セキュリティ ファンデーション（ISFS）モジュールでは、情報セキュリティの基本概念とその一貫性について確認します。ISFS の対象者は、組織のすべての人です。本モジュールで確認する基礎知識は、情報のぜい弱性と、その情報を保護するために必要な対策を理解するために役立ちます。

背景

EXIN ISO/IEC 27001 準拠 情報セキュリティファンデーションの証明書は、情報セキュリティに関する資格プログラムの一部です。モジュールには、EXIN ISO/IEC 27001 準拠 情報セキュリティマネジメント　プロフェッショナル及び　EXIN ISO/IEC 27001 準拠　情報セキュリティマネジメント　エキスパート　の証明書が続きます。

対象者

組織で情報を取り扱うすべての人。本モジュールは、情報セキュリティの基礎知識を必要とする小規模な独立系企業にも適しています。
本モジュールは、経験の浅い情報セキュリティ専門家にとっても有効な開始点となります。

必須条件

- EXIN ISO/IEC 27001 準拠 情報セキュリティファンデーション 試験の合格。

試験の詳細内容

試験の形式:	コンピュータベースまたは紙ベースの多肢選択形式
問題数:	40
合格点:	65%
参考書やノートの持ち込み:	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 試験では、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。受験者がさらに高いレベルに進む前の学習の基礎要素となります。
- 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。理解することにより、受験者は提示されているものを把握しており、その学習教材が受験者の環境にどのように応用できるかを評価できることがわかります。

教育・訓練

授業時間

この教育コースの推奨受講時間は 14 時間です。 グループ課題、試験準備、休憩が含まれます。宿題、試験準備の計画、昼休みはこの時間に含まれません。

学習時間の目安

60 時間、個人が習得している知識によります。

認定教育機関

認定教育事業者のリストを www.exin.com で参照できます。

2. 試験の要件

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	試験の仕様	ウェイト
1 情報とセキュリティ		**10%**
	1.1 情報の概念	2.5%
	1.2 情報の価値	2.5%
	1.3 信頼性の側面	5%
2 脅威とリスク		**30%**
	2.1 脅威とリスク	15%
	2.2 脅威、リスク、情報の信頼性の関係	15%
3 アプローチと組織		**10%**
	3.1 セキュリティ基本方針とセキュリティ組織	2.5%
	3.2 構成要素	2.5%
	3.3 インシデント管理	5%
4 対策		40%
	4.1 対策の重要性	10%
	4.2 物理的セキュリティ対策	10%
	4.3 技術的対策	10%
	4.4 組織的対策	10%
5 法律と規制		**10%**
	5.1 法律と規制	10%
	合計	**100%**

試験の仕様

1　情報とセキュリティ

1.1　情報の概念

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　基本インフラの一部を形成する記憶媒体について説明する。

1.2　情報の価値

次のことが行える。

1.2.1　組織にとってのデータ／情報の価値を説明する。

1.2.2　データ／情報の価値が組織にどのように影響するかを説明する。

1.2.3　情報セキュリティの概念を適用することでデータ／情報の価値がどのように保護されるかを説明する。

1.3　信頼性の側面

次のことが行える。

1.3.1　情報の信頼性の側面を挙げる。

1.3.2　情報の信頼性の側面について説明する。

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、およびリスク分析の概念について説明する。

2.1.2　脅威とリスクの関係を説明する。

2.1.3　さまざまな種類の脅威について説明する。

2.1.4　さまざまな種類の損害について説明する。

2.1.5　さまざまなリスク戦略について説明する。

2.2　脅威、リスク、情報の信頼性の関係

次のことが行える。

2.2.1　さまざまな種類の脅威の例を認識する。

2.2.2　さまざまな種類の脅威が情報と情報処理に及ぼす影響について説明する。

3　アプローチと組織

3.1　セキュリティ基本方針とセキュリティ組織

次のことが行える。

3.1.1　セキュリティ基本方針の目的と内容の概要を説明する。

3.1.2　3.1.2　セキュリティ組織の目的と内容の概要を説明する。

3.2　構成要素

次のことが行える。

3.2.1　行動規範の重要性を説明する。

3.2.2　管理責任の重要性を説明する。

3.2.3　情報セキュリティ組織で最も重要な役割を挙げる。

3.3 インシデント管理

次のことが行える。

3.3.1 セキュリティインシデントの報告方法と必要な情報を要約する。

3.3.2 セキュリティインシデントの例を挙げる。

3.3.3 セキュリティインシデントを報告しない場合の結果について説明する。

3.3.4 エスカレーション（機能的、階層的）後の流れについて説明する。

3.3.5 組織内でのエスカレーションの影響を説明する。

3.3.6 インシデントサイクルについて説明する。

4 対策

4.1 対策の重要性

次のことが行える。

4.1.1 セキュリティ対策を体系化または整備するさまざまな方法について説明する。

4.1.2 セキュリティ対策の種類ごとに例を挙げる。

4.1.3 リスクとセキュリティ対策の関係を説明する。

4.1.4 情報分類の目的を説明する。

4.1.5 分類の効果を説明する。

4.2 物理的セキュリティ対策

次のことが行える。

4.2.1 物理的セキュリティ対策の例を挙げる。

4.2.2 物理的セキュリティ対策が不十分な場合のリスクについて説明する。

4.3 技術的対策

次のことが行える。

4.3.1 技術的セキュリティ対策の例を挙げる。

4.3.2 技術的セキュリティ対策が不十分な場合のリスクについて説明する。

4.3.3 暗号技術、ディジタル署名、および認証の概念を理解する。

4.3.4 オンライン・バンキングの3つのステップを挙げる（PC、ウェブサイト、支。

4.3.5 さまざまな種類の悪意のあるソフトウェアを挙げる。

4.3.6 悪意のあるソフトウェアに関して使用できる対策について説明する。

4.4 組織的対策

次のことが行える。

4.4.1 組織的セキュリティ対策の例を挙げる。

4.4.2 組織的セキュリティ対策が不十分な場合の危険性とリスクについて説明す。

4.4.3 職務の分離、パスワードの使用などのアクセスに関するセキュリティ対策。

4.4.4 アクセスマネジメントの原則について説明する。

4.4.5 識別、認証、認可の概念について説明する。

4.4.6 組織にとっての、適切に整備された事業継続管理の重要性を説明する。

4.4.7 演習実施の重要性を明示する。

5 法律と規制

5.1 法律と規制

次のことが行える。

5.1.1 法律と規制が情報の信頼性にとって重要な理由を説明する。

5.1.2 情報セキュリティに関する法律の例を挙げる。

5.1.3 情報セキュリティに関する規制の例を挙げる。

5.1.4 法律と規制の要件を満たすために取ることができる対策を示す。

3. 用語の一覧

本章では、受験者が知っておくべき用語を記載します。用語はアルファベット順に列挙しています。一覧で略語と正式名称が併記されている概念は、いずれも試験で使われる可能性があります。

ただし、これらの用語の知識だけでは試験に十分とは言えません。受験者はその理論を理解し、応用できなければなりません。

English	Japanese
Access control	アクセス制御
Asset	資産
Audit	監査
Authentication	認証
Authenticity	真正性
Authorization	認可
Availability	可用性
Backup	バックアップ
Biometrics	生体認証
Botnet	ボットネット
Business Continuity Management (BCM)	事業継続管理 (BCM)
Business Continuity Plan (BCP)	事業継続計画 (BCP)
Business Assets	ビジネスアセット
Category	カテゴリ(事業資産)
Certificate	証明書
Change Management	変更管理(格付け)
Classification (grading)	分類
Clear desk policy	クリアデスク方針
Code of conduct	行動規範
Code of practice for information security (ISO/IEC 27002)	情報セキュリティマネジメントの実践のための規範 (JIS Q 27002)
Completeness	完全さ
Compliance	法令遵守／遵守
Computer criminality legislation	コンピュータ犯罪関連法規
Confidentiality	機密性
Continuity	継続性
Controls	管理策
Copyright legislation	著作権法
Corrective	是正的
Correctness	正確性
Cryptography	暗号技術
Damage	損害
Data	データ
Detective	検知的
Digital signature	ディジタル署名

Direct damage	直接的ダメージ
Disaster	災害
Disaster Recovery Plan (DRP)	災害復旧計画 (DRP)
Encryption	暗号化
Escalation	エスカレーション
Functional escalation	XX 機能的エスカレーション
Hierarchical escalation	XX 階層的エスカレーション
Exclusivity	排他性
Hacking	ハッキング
Hoax	デマウィルス
Identification	識別
Impact	影響
Incident cycle	インシデントサイクル
Indirect damage	間接的ダメージ
Information	情報
Information analysis	情報分析
Information architecture	情報アーキテクチャ
Information management	情報マネジメント
Information security review	情報セキュリティのレビュー
Information system	情報システム
Infrastructure	インフラ
Integrity	完全性
Interference	干渉
ISO/IEC 27001	JIS Q 27001
ISO/IEC 27002	JIS Q 27002
Key	かぎ
Logical access management	論理アクセスマネジメント
Maintenance door	メンテナンスドア
Malware	マルウェア（悪意のあるソフトウェア）
Managing business assets	ビジネスアセット(事業資産)管理
Non-disclosure agreement	秘密保持契約 (NDA)
Non-repudiation	否認防止
Patch	パッチ
Personal data protection legislation	個人情報（データ）保護関連法規
Personal firewall	パーソナルファイアウォール
Phishing	フィッシング
Precision	精度
Preventive	予防的
Priority	優先度
Privacy	プライバシ
Production factor	生産要素
Public Key Infrastructure (PKI)	公開かぎ基盤 (PKI)
Public records legislation	公的記録関連法規
Qualitative risk analysis	定性的リスク分析
Quantitative risk analysis	定量的リスク分析

Reductive	低減的
Redundancy	冗長性
Reliability of information	情報の信頼性
Repressive	制止的
Risk	リスク
Risk analysis	リスク分析
Risk assessment (Dependency & Vulnerability analysis)	リスクアセスメント（依存関係およびぜい弱性分析）
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	リスク負担
Risk neutral	リスク中立
Robustness	堅牢性
Rootkit	ルートキット
Secret authentication information	秘密認証情報
Security event	セキュリティ事象
Security in development	開発におけるセキュリティ
Security incident	セキュリティインシデント
Security measure	セキュリティ対策
Security Organization	セキュリティ組織
Security Policy	セキュリティ基本方針
Security regulations for the government	政府（行政）機関向け特別情報関連セキュリティ法規
Segregation of duties	職務の分離
Social engineering	ソーシャルエンジニアリング
Spam	スパム
Spyware	スパイウェア
Stand-by arrangement	スタンバイ
Storage medium	記憶媒体
System acceptance testing	システム受入れテスト
Threat	脅威
Timeliness	適時性
Trojan	トロイの木馬
Uninterruptible Power Supply (UPS)	無停電電源装置（UPS）
Urgency	緊急
User access provisioning	ユーザアクセスのプロビジョニング
Validation	妥当性検証
Verification	検証
Virtual Private Network (VPN)	仮想私設網（VPN）
Virus	ウィルス
Vulnerability	ぜい弱性
Worm	ワーム

4. 文献

試験の参考文献

A. Hintzbergen, J., Hintzbergen, K., Smulders, A. and Baars, H.
Foundations of Information Security - Based on ISO 27001 and ISO 27002
Van Haren Publishing, 3rd edition, 2015
ISBN 978 94 018 0012 9
eBook 978 94 018 0541 4

文献の概要

試験要件	試験の仕様	文献
1 情報とセキュリティ		
	1.1 情報の概念	3 章、4.10 項
	1.2 情報の価値	3 章、4 章
	1.3 信頼性の側面	3 章、4 章
2 脅威とリスク		
	2.1 脅威とリスク	3 章
	2.2 脅威、リスク、情報の信頼性の関係	3 章、11 章
3 アプローチと組織		
	3.1 セキュリティ基本方針とセキュリティ組織	3 章、5 章、6 章
	3.2 構成要素	6 章、7 章、8 章、13 章
	3.3 インシデント管理	3 章、15 章、16 章
4 対策		
	4.1 対策の重要性	3 章, 8 章、16 章
	4.2 物理的セキュリティ対策	3 章、11 章
	4.3 技術的対策	6 章、11 章、12 章
	4.4 組織的対策	3 章、6 章、9 章、17 章、18 章
5 法律と規制		
	5.1 法律と規制	18 章

EXIN の連絡先

www.exin.com

YOUR ICT COMPETENCE PARTNER