

情報セキュリティ管理

発表者 大東

目次

- ISMS
- PDCAサイクル
- 情報セキュリティ継続
- リスクマネジメント
- 情報セキュリティポリシー
- 認証の3要素
- 情報セキュリティ組織,機関

ISMS

- ISMS ... 情報セキュリティマネジメントシステム
組織で情報セキュリティを管理する仕組み
- ISMSの構築方法や要求事項は,JIS Q(ISO)27001に示されている.
- また,実践の規模はJIS Q(ISO)27002に示されている.

PDCAサイクル

ISMSでは,PDCAサイクルが繰り返し行われている.



情報セキュリティのPDCAサイクル

情報セキュリティ継続

- 組織は非常事態に備えて、継続した情報セキュリティの運用をしなければならない。

→そのために、**情報セキュリティ継続**を策定しておく必要がある。

具体例として、コンジエンシープラン(緊急時対応計画),復旧計画,バックアップ対策,などが挙げられる。

リスクマネジメント

- **リスク分析**を行うことで、リスクの大きさを算出する。**(リスクアセスメント)**
- リスクの大きさは、リスクの発生確率と発生した際の**影響**の大きさを組み合わせて算出される。
- リスク分析を行った後で、それぞれのリスクに対して、**リスク評価**を行う。

リスク評価

- 定性的評価

リスクの大きさを金額以外の尺度で評価する.

- 定量的評価

リスクの大きさを金額で評価する.

リスク対応

①リスク最適化(低減)

リスクの発生確率や被害額を減少させる対策を取る.

例.セキュリティ対策

②リスク回避

リスクの根本的原因を排除してリスクを取り除く仕組み.

例.運用サーバーの除去

リスク対応

③リスク移転

リスクを第三者に移す.

保険をかけて外部に費用負担を転嫁する方法などがある.

④リスク保有(受容)

特にリスクに対応しない.

残ってしまったリスクを**残留リスク**と呼ぶ

問題

個人情報の漏えいに関するリスク対応のうち、リスク回避に該当するものはどれか。

- ア 個人情報の重要性と対策費用を勘案し、あえて対策をとらない。
- イ 個人情報の保管場所に外部の者が侵入できないように、入退室をより厳重に管理する。
- ウ 個人情報を含む情報資産を外部のデータセンタに預託する。
- エ 収集済みの個人情報を消去し、新たな収集を禁止する。

(平成29年春 情報処理安全確保支援士試験 午前Ⅱ 問9)

解説

リスク回避とは、リスクの根本原因を排除することでリスクを処理することです。新たな収集を禁止し、収集済みの個人情報を消去することで、情報漏えいのリスクを回避できます。したがって、エが正解です。

アはリスク保有、イはリスク最適化、ウはリスク移転に該当します。

《解答》エ

情報セキュリティポリシー

- 組織の情報資産を守るための方針や基準を明文化したもの.

①情報セキュリティ基本方針

②情報セキュリティ対策基準

情報セキュリティ基本方針

- 情報セキュリティに対する組織の考え方や方針を示すもの.
- 経営陣によって承認される.
- 目的や対象範囲,管理体制や罰則について記述されており,全従業員及び関係者に通知される.

情報セキュリティ対策基準

- 情報セキュリティ基本方針とリスクアセスメントの結果に基づき,対策基準を決める.
- 適切な情報セキュリティレベルの維持,確保のための遵守事項や基準を定める.

問題

ISMSにおいて定義することが求められている情報セキュリティ基本方針に関する記述のうち、適切なものはどれか。

- ア 重要な基本方針を定めた機密文書であり、社内の関係者以外の目に触れないようにする。
- イ 情報セキュリティの基本方針を述べたものであり、ビジネス環境や技術が変化しても変更してはならない。
- ウ 情報セキュリティのための経営陣の方向性及び支持を規定する。
- エ 特定のシステムについてリクス分析を行い、そのセキュリティ対策とシステム運用の詳細を記述する。

(平成25年秋 応用情報技術者試験 午前 問40)

解説

情報セキュリティ基本方針は、経営陣によって承認されるもので、情報セキュリティのための経営陣の方向性及び支持を規定します。したがって、ウが正解です。

ア 機密文書とするのではなく、全社員に公開し、必要なら外部関係者にも通知します。

イ 「変更してはならない」は誤りです。ISMSの一環として整備されるものなので、PDCAサイクルに則って定期的に改善する必要があります。

エ 基本方針ではなく、情報セキュリティ対策実施手順、規程類のことです。

《解答》ウ

認証の 3 要素

- ・ **知識** …… ある情報をもっていることによる認証
例：パスワード, 暗証番号など
- ・ **所持** …… あるものをもっていることによる認証
例：ICカード, 電話番号, 秘密鍵など
- ・ **生体** …… 身体的な特徴による認証
例：指紋, 虹彩, 静脈など

それぞれの認証を 1 つずつ使うのではなく, 複数組み合わせで認証することが重要. (**多要素認証, 二要素認証**)

情報セキュリティ組織,機関

①情報セキュリティ委員会

組織内における情報セキュリティ管理責任者
(**CISO**:Chief Information Security Officer)などの意思決定組織

②SOC(セキュリティオペレーションセンター)

セキュリティ監視の拠点.

セキュリティ管理サービスを提供する企業が,複数の顧客へ対応を集中して行うために用意される.

情報セキュリティ組織,機関

③CSIRT(Computer Security Incident Response Team)

コンピュータやネットワークを監視し,問題が発生した際に,その原因の解析や調査を行う組織.

日本には他のCSIRTと情報連携や調整を行う
JPCERT/CC(Japan Computer Emergency Response
Team Coordination Center)がある.

情報セキュリティ組織,機関

④IPAセキュリティセンター

IPA(情報処理推進機構)内に設置されているセキュリティセンター.

⑤JVN(Japan Vulnerability Notes)

日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供する脆弱性対策情報ポータルサイト.

JPCERT/CCとIPAが共同運営している.

情報セキュリティ組織,機関

⑥内閣サイバーセキュリティセンター

内閣官房に設置された組織.

サイバーセキュリティ戦略の立案,実施の推進を行っている.

⑦ホワイトハッカー

コンピュータやネットワークに関する高い技術を持つハッカーと呼ばれる人の中で,その技術を善良な目的に活かす人.