サイバーセキュリティ経営ガイドライン実践についてのアンケート結果

2020年6月3日

独立行政法人　情報処理推進機構

調査概要

- 期間：2019年3月25日～2019年10月25日
- 回答者：プラクティス第1版に興味をもって頂いた方
- 回答数：4286件（自由記述の有効回答数691件）
- 設問：

  ①経営ガイドライン重要10項目の実践で困っていること(選択式)

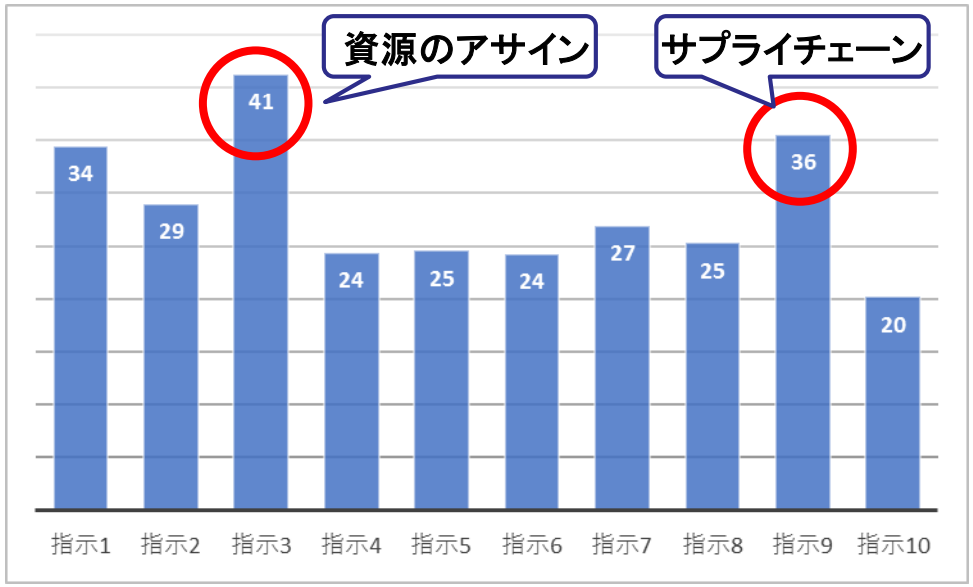
  ②プラクティス第1版3章の内容で共感できる課題(選択式)

  ③セキュリティ対策で必要と思われる情報(自由記述)

①重要10項目実践で困っていること

【設問1】サイバーセキュリティ経営ガイドラインに記載の重要10項目について、あなたもしくはあなたの組織で実践に困っていると思われる項目はありますか？（複数回答可）

指示1 サイバーセキュリティリスクの認識、組織全体での対応方針の策定	34.48%
指示2 サイバーセキュリティリスク管理体制の構築	28.98%
指示3 サイバーセキュリティ対策のための資源（予算、人材等）確保	41.25%
指示4 サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	24.36%
指示5 サイバーセキュリティリスクに対応するための仕組みの構築	24.55%
指示6 サイバーセキュリティ対策におけるPDCAサイクルの実施	24.22%
指示7 インシデント発生時の緊急対応体制の整備	26.92%
指示8 インシデントによる被害に備えた復旧体制の整備	25.29%
指示9 ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握	35.58%
指示10 情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	20.16%

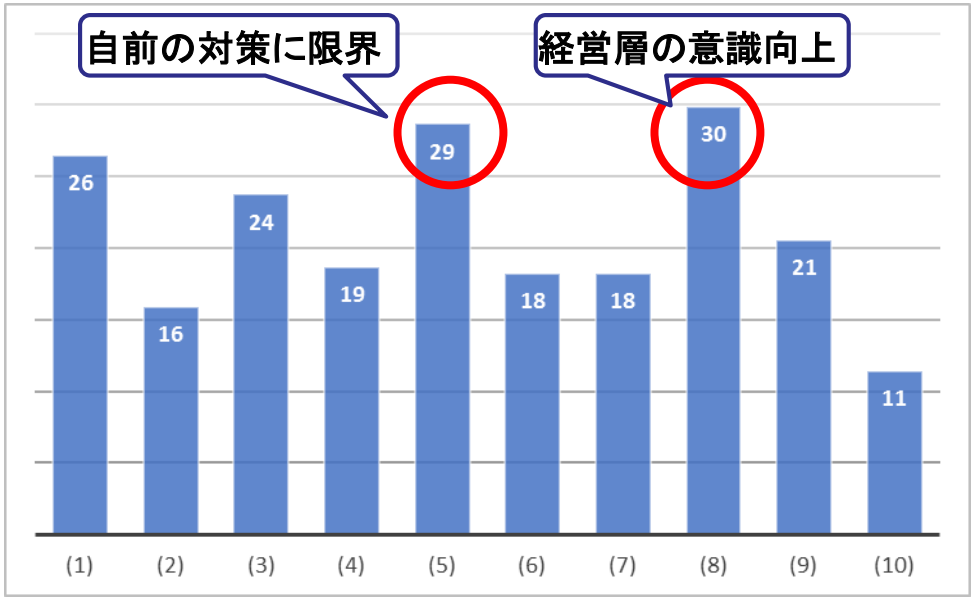


②プラクティスの内容で共感できる課題

【設問2】あなたもしくはあなたの組織において、困っていることや共感できる課題はありますか？（複数回答可）

選択肢(1)~(10)は2019年3月公開のプラクティス集第1版3章悩みのトピックを流用

(1)	インシデント対応経験がない要員でCSIRTを組成したが対応に不安がある	26.48%
(2)	標的型攻撃メール等のインシデントに関する報告が行われにくい	15.91%
(3)	インシデントが起きた際の財務面のリスクヘッジが十分でない	23.75%
(4)	IoT機器が「シャドーIT」化している	18.69%
(5)	自前でのセキュリティ対策は負担が大きく、現状運用に限界を感じる	28.67%
(6)	遠隔拠点のセキュリティ管理状況が把握できない	18.20%
(7)	外部サービスの選定にコストがかかる	18.22%
(8)	経営層のセキュリティ意識をどのように向上させればよいかわからない	29.86%
(9)	従業員向けに実施している教育の効果が感じられない	20.56%
(10)	新興企業のセキュリティ管理体制に不安を感じ、取引先として推奨できない	11.43%



③ サイバーセキュリティ対策で必要と思われる情報(自由記述):有効回答数691

- 自由記述回答で出現頻度の高いキーワードから回答例を抽出

必要と思われる情報の主な回答例	自由記述回答中のキーワード※	キーワード出現頻度
攻撃と対策の事例、侵入口事例、攻撃の兆候事例、インシデント対応手順ひな形、攻撃者情報	攻撃・インシデント	111
予算確保の方法、予算例、インシデント対応コスト、外部ベンター活用ノウハウ、採用・育成方法	予算・人材	68
経営層の意識向上施策、対策導入の訴求方法	経営層	57
教育方法、教育資料、教育効果測定とフィードバック方法、演習シナリオ	教育、演習・訓練	51
対策導入状況、セキュリティ管理/成熟度レベル、クラウドのセキュリティ対策、失敗事例	他社事例	47
リスク評価方法、リスク軽減策、リスクレベル別対応策例	リスク	46

※類似の文言はまとめて集計。例えば、インシデントは、「事故」や「被害」を含む。予算は、「コスト」を含む。

・その他、「具体的」を含む回答数136。例えば「具体的な攻撃と対策の事例」、「具体的な行動指針」、「具体的な意識向上施策」など。