

ASM 勉強会 主催者向け資料

1 勉強会実施要領

目的

【主目的】

1. 未把握 IT 資産の特定
2. セキュリティ意識の向上

【副次的目的】

- ・ シャドーIT 対策の必要性理解
- ・ 適切な報告体制の構築

達成すべき目標

- ・ 自発的な報告体制の確立
- ・ セキュリティ意識の向上
- ・ 部門間の情報共有促進

主催に際してのポイント

- ・ セキュリティ部門ないしはシステム部門の有識者を説明担当者としてアサインする
- ・ 適当な要員がない場合は外部への依頼を検討する。

【注意】

外部の講師へ依頼を検討する場合、自社の IT 資産の情報、技術情報などへのアクセス、情報流出や勉強会の内容に関してトラブルが起こる可能性があるため、業務委託契約および秘密保持契約などの締結を法務部または総務部が検討することを推奨する。

[参考文献]

純行政書士事務所. (2024). 【研修会社向け】外部講師との業務委託契約で頻発するトラブル事例 9 つと対策条項を解説 <https://jun-gyosho.com/training-outsourcing/> (アクセス日: 2024 年 11 月 28 日)

進行のポイント

【説明時の注意点】

- ・ 責めない、追及しない
- ・ 退屈にさせないようにディスカッションなどを挟む
- ・ 建設的な議論の促進
- ・ 参加者の発言を促す

【タイミング別の対応】

開始時：

- ・ 心理的安全性の確保
- ・ 目的の明確な説明

実施中：

- ・ 参加者の反応観察
- ・ 理解度の確認
- ・ 適切な指示

終了時：

- ・ 重要ポイントの確認
- ・ アンケート回答の促進

2. 収集情報の管理

アンケート実施要領

【実施のポイント】

- ・ その場での回答を促す
- ・ 匿名性の確保
- ・ 回答のしやすさ重視

【回答の分析ポイント】

- ・ 未申告システムの特定
- ・ 使用頻度の高いサービス
- ・ リスクの高い利用形態
- ・ 部門特有の課題

要注意回答と対応方法

【要注意となる回答例】

1. 機密データの非承認サービスでの処理
2. 個人アカウントでの業務利用
3. 未承認の外部サービス利用

(外部からアクセス可能となっている情報の管理)

【対応手順】

1. 事実確認
2. リスク評価
3. 対策検討
4. 改善指導

3. リスク管理

想定される質問への回答

Q1: 「報告により自身に不利益はあるか？」

A1: 報告自体による不利益はなし。改善が目的

Q2: 「既存の業務効率が下がるのでは？」

A2: 適切な代替手段を提供する

インシデント対応

【発見時の対応フロー】

1. 情報の切り分け
2. 影響範囲の特定
3. 緊急対応の判断
4. 是正措置の実施

【報告経路】

緊急時: セキュリティ担当 (内線 XXXX)

平常時: 所属部門長→システム管理者

4. 評価基準

勉強会効果測定

【評価項目】

1. 参加率
2. アンケート回答率
3. 未把握資産の報告数

【長期的評価項目】

- ・ シャドーIT 減少率
- ・ セキュリティインシデント数
- ・ 自主報告件数

アンケート分析手法

【分析の視点】

- ・ 部門別の特徴
- ・ 共通する課題
- ・ リスクの高い利用形態
- ・ 優先度の判断

【データの活用方法】

- ・ セキュリティ対策の改善
- ・ 管理体制の見直し
- ・ 教育計画への反映

5. 運営チェックリスト

事前準備

- ☐ 会場・機材の確認
- ☐ 資料の準備
- ☐ アンケートシステムの動作確認
- ☐ 参加者リストの確認
- ☐ ネットワーク環境の確認

当日確認事項

- ☐ 機材の動作確認
- ☐ 配布資料の確認
- ☐ 出席者の確認
- ☐ アンケート回答状況の確認
- ☐ 質問・意見の記録

フォローアップ

- ☐ アンケート結果の集計
- ☐ 報告された資産の検証
- ☐ 必要な個別ヒアリングの実施
- ☐ 報告書の作成
- ☐ 次回への改善点整理

※本資料は機密情報を含むため、取り扱いには十分注意してください。