

ISMS の PDCA サイクル

形骸化を防ぐ実務のコツ

回し続けることが本当の価値？

4 段階の中身・ISO 条項対応・形骸化防止・GRC 案件単価を解説



形だけになってるでしゅ…

回してこそだ。仕組みを学べ。



【解説に入る前に】サービスのご紹介



セキュリティプロ・フリーランス

セキュリティに特化したフリーランス案件の
マッチングサービス

- ✓ 最高月収 150 万円・月額 80 万円以上の案件が 80% 以上
- ✓ リモート率 80% 以上、フルリモート案件多数
- ✓ セキュリティに精通した専任エージェントが営業・単価交渉・契約を代行

[詳細を見る →](#)



セキュリティプロ・テンショク

セキュリティエンジニア / コンサルタントに
特化した転職エージェント

- ✓ 最高想定年収 1,200 万円・利用者の 85% 以上が年収アップ
- ✓ 取扱求人の約 7 割が非公開求人
- ✓ 技術がわかるアドバイザーが書類添削・面接対策・年収交渉を代行

[詳細を見る →](#)



どちらも登録・利用は完全無料。在職中・フルリモート希望でも相談できます。
まずは市場価値の無料相談から。

● ISMS の PDCA サイクル：4 段階の全体像

1

Plan（計画）

情報セキュリティ方針の策定・リスクアセスメント・対応計画の作成

2

Do（運用）

規程に沿った運用・従業員教育・インシデントの管理と記録

3

Check（点検）

監視・測定・内部監査・マネジメントレビューで実態を確認

4

Act（改善）

不適合への是正処置・再発防止・次の Plan への反映

4 つがつながって初めて輪になる。



● ISO27001 の条項と PDCA の対応関係

4 ～ 7 章（Plan）

土台づくりフェーズ

- ・ 4 章 組織の状況
- ・ 5 章 リーダーシップ
- ・ 6 章 計画
- ・ 7 章 支援

VS

8 ～ 10 章（DCA）

運用・点検・改善フェーズ

- ・ 8 章 運用（Do）
- ・ 9 章 パフォーマンス評価（Check）
- ・ 10 章 改善（Act）



条項の核心

章番号と PDCA を結べば、どこが遅れているか一目でわかる。

● Plan ・ Do 段階の具体タスク

Plan : 土台をつくる



適用範囲の決定

守る情報資産・部門・拠点を明確化する



方針と目標の策定

Check で達成度を測る基準になる



リスクアセスメント

脅威・脆弱性を洗い出し優先順位を決定

Do : 計画を現場に落とす



規程に沿った運用

手順書どおりの日常業務を徹底する



教育・訓練の実施

標的型メール訓練などを定期実施する



記録を残す習慣

ログ・対応経緯が審査の証跡になる

記録が命！



● Check ・ Act 段階の具体タスク

Check : 運用実態を点検する



内部監査（9.2）

規程どおりか独立した立場で客観確認



マネジメントレビュー（9.3）

経営層が ISMS 全体の有効性を評価する



ログ・監視基盤

有効性の測定を感覚から数値へ変える

Act : 課題を次のサイクルへ渡す



是正処置の実施

原因を分析し対症療法で終わらせない



再発防止策

同じ不適合を繰り返さない仕組みを作る



次年度 Plan へ反映

ここまでやって初めて 1 周が完結する

Act で 1 周完結



● 形骸化の 3 つの典型パターン



文書だけ立派

分厚いマニュアルを作って満足し、現場運用が伴っていない



儀式化した監査

チェックリストを埋めるだけで、実態確認が形式的になっている



審査直前だけ稼働

普段は放置し、更新審査の前だけ帳尻合わせをしている状態

共通点は Do ・ Check の欠落だ。文書 ・ 審査だけでは情報は守れない。



● 形骸化を防ぐ：回し続けるための工夫



担当と責任を明確化

誰がいつ何をやるかを決め、善意頼みを脱却する



小さいサイクルで回す

四半期ごとに点検しズレを早く見つける



継続の核心

仕組みで回る運用へ移すことが形骸化を防ぐ鍵だ。

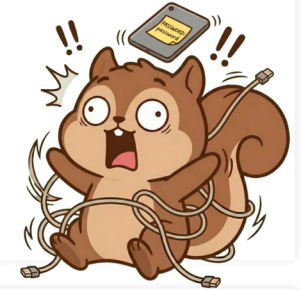


● 認証審査と 3 年更新サイクルの関係



1・2年目：維持審査

サーベイランスで日常の運用状況を継続確認



3年目：更新審査

3年間の運用実績を精査。書類より中身が問われる



審査の核心

3年間ずっと見られている。付け焼き刃は審査官に見抜かれる。

● PDCA の記録が審査対応をラクにする

1

内部監査の記録

規程どおりに運用されていたかを示す最重要の証跡

2

是正処置の記録

課題を発見し対処した事実を証明するための記録

3

マネジメントレビュー

経営層が ISMS を評価・判断した議事録が証跡になる

都度残す習慣が審査をラクにする。



● GRC ・ ISMS 運用スキルの市場価値

求められる案件の傾向



GRC ・ ISMS 構築

内部監査・リスクアセスメント経験が評価軸



PMO ・ 上流工程

仕組みを設計し回す力が直接武器になる



ガバナンス強化

体制整備・ルール策定を専門に進める動き

武器になる！



単価感（公開案件データ）



全体中央値

月額 92.5 万円（50 ～ 180 万円）



PMO ポジション

中央値 100 万円（65 ～ 130 万円）



要件定義フェーズ

中央値 115 万円（70 ～ 180 万円）

● 会社員とフリーランスの働き方の違い

会社員

組織の ISMS を継続的に育てる

- ・ 社内調整も含めて担う
- ・ 1つの組織を深く理解できる
- ・ 継続的な改善が積み上がる

VS

フリーランス

専門性を軸に複数現場を渡る

- ・ ガバナンス構築・ PMO に参画
- ・ 横断的な視点が強みになる
- ・ 複数業界の経験が蓄積される



選択の核心

ISMS を回した経験は、どの道でも通用する。選択肢を知れ。

● まとめ



ISMS の PDCA は Plan ・ Do ・ Check ・ Act の 4 段階を止めずに回し続けることが価値になる



形骸化の根本原因は Do と Check の欠落。担当を決め、小さいサイクルで日常に混ぜて回すことが処方



ISMS 運用 ・ GRC 経験はフリーランス市場でも評価され、PMO ・ 上流工程の高単価案件に直結する

NEXT ACTION

まずは市場価値の無料相談・登録

[セキュリティプロ・フリーランス >](#)

[セキュリティプロ・テンショク >](#)

