

ISMS は意味がないのか を徹底検証

形骸化と実質運用、何が違う？

定義・4つの理由・登録数・案件単価を解説



ISMS って本当に意味ないでしょ？

意味を持たせられるかが問題だ。



【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 が意味を失う瞬間と持つ瞬間

形骸化した ISMS

認証がゴールになった状態

- ・書類だけ更新、実態は放置
- ・審査前だけ帳尻合わせ
- ・PDCA が止まっている

VS

実質運用する ISMS

PDCA を実務として回す状態

- ・自社のリスクを言葉で評価
- ・管理策を現場に翻訳する
- ・改善を制度として説明できる



ISMS の核心

制度でなく運用が意味を決める。回せる人が鍵だ。

● ISMS ・ ISO27001 ・ JIS Q 27001 の違い



ISMS

情報セキュリティを回し続けるマネジメントの仕組み



ISO/IEC 27001

ISMS が満たすべき要求事項を定めた国際規格



JIS Q 27001

ISO/IEC 27001 を日本語化した国内版の規格

認証取得と ISMS の運用は別物だ。この違いを見失うと形骸化が始まる。



● 最新改訂で変わった 3 つのポイント



管理策を 114 から 93 に再編

4 テーマ（組織的・人的・物理的・技術的）に整理



11 の管理策を新設

脅威インテリジェンス・クラウドセキュリティを追加



改訂の核心

数は減った、やることは増えた。旧版のままで止めるな。

● 「意味がない」と言われる 4 つの理由

1

認証取得が目的化

取得後に PDCA が止まり、書類だけが残る形骸化

2

文書負担の肥大化

記録づくりが審査のための作業になり現場が疲弊する

3

インシデント誤解

ISMS はリスクゼロではなくリスクを管理する枠組み

4

経営層の不関与

チェックリスト対応と捉えると運用が現場丸投げになる

制度の欠陥ではない。運用の失敗だ。



● 形骸化はこうして起きる（担当者・文書編）



担当者不在で更新審査だけ残る

リスクアセスメントが毎年コピーで済まされる



是正処置が文書上だけで完結

審査前に帳尻を合わせ、終わればまた放置する



形骸化の核心

認証マークがあっても中身が止まれば意味はない。回し続けることだ。

● 形骸化はこうして起きる（経営・誤解編）



投資判断が後回しで責任者が曖昧

権限もリソースもないまま現場が丸投げされる



インシデント防止への誤解

ISMS はリスクゼロでなく管理プロセス。防止と管理は別物



根本の核心

形骸化の根は人材不足と経営の無関心だ。そこを変えろ。

● 認証登録数が増え続ける 2つの理由



登録 8,000 件超を突破

約 2 年 3 か月で 1,000 件超が増加。運用人材の不足も深刻化



取引条件・入札要件として定着

大手取引・官公庁入札で ISMS 認証が参加前提になる場面が増加



市場の核心

登録数が増えるほど運用人材の不足は深刻になる。需要は止まらない。

● 企業が ISMS を手放せない実利

取引・入札の要件



新規取引の条件

大手との契約で ISMS 認証が前提になる



官公庁入札の資格

参加条件として認証を求める案件が増加中



サプライチェーン加点

委託先選定で認証有無が評価に直結

インシデント時の説明責任



管理状況の記録提示

発生時に運用記録で対応の裏づけを示せる



監査・点検への一貫対応

資料が属人化せず制度として説明できる



再発防止の制度的説明

個別対応でなくプロセスで語れる強みになる

● 市場で評価される ISMS 関連スキル



リスクアセスメントの設計と実行

自社の文脈でリスクを評価し管理策に落とせる力



GRC の統合的な視点

ガバナンス・リスク・コンプライアンスを一つの軸で動かす



評価の核心

資格より実務。PDCA を回せた証明が最大の武器だ。



● フリーランス案件での ISMS 経験の価値

PMO 型案件



中央値

100 万円 / 月



上限

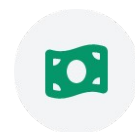
130 万円 / 月



主な業務

セキュリティガバナンス・ISMS 施策推進

要件定義型案件



中央値

115 万円 / 月



上限

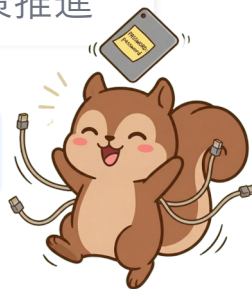
180 万円 / 月



主な業務

セキュリティ要件の定義・設計支援

公開案件 118 件



● まとめ



ISMS が意味を失うのは形骸化した時。制度でなく運用と人が価値を決める



認証登録数は 8,000 件超で増加中。運用できる人材の不足は深刻になり続けている



ISMS ・ GRC 経験者の PMO 案件中央値は 100 万円。今すぐ市場で自分の価値を確かめろ

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 >](#)

