

ISMS リスクアセスメント

手順と 4 つの対応

リスクはどこまで下げればいい？

3 ステップ・4 アプローチ・4 対応・案件単価を解説



どこから始めればいいでしゅ？

型を知れば誰でも回せる。



【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。

● リスクアセスメントの目的



CIA の 3 要素を守る

機密性・完全性・可用性が損なわれると事業に響く



目的はゼロでなく許容水準

影響の大きい資産から優先的に手を当てる



目的の核心

ゼロを目指すな。許容水準まで下げる判断が優先順位を生む。



● リスク管理 3 概念の包含関係



リスクアセスメント

特定・分析・評価で「測るまで」の工程



リスク対応

評価後に具体的な手を打つ「動く」工程



リスクマネジメント

両者を計画・運用・見直しで回す管理全体の枠組み

3つは対立しない。アセスメントと対応を包む枠組みがマネジメントだ。



● リスクアセスメントの3ステップ

1

リスク特定

情報資産・脅威・脆弱性を洗い出す。網羅性が後工程を左右する

2

リスク分析

発生可能性 × 影響度でリスク値を算定。評価基準は先に決める

3

リスク評価

受容基準と照合し、対応が必要なリスクの優先順位を決める

順番に意味がある。飛ばすな。



● リスク特定の 3 つの視点



情報資産

顧客データ・サーバー・PC など守るべき対象を一覧化



脅威

不正アクセス・マルウェア・内部不正など害を与える要因



脆弱性

パッチ未適用・弱いパスワードなど脅威に付け入られる弱点



この 3 軸の抜け漏れが後工程の精度を直接左右する。棚卸しを甘く見るな。

● リスク分析の 2 つの手法



定性的アプローチ

高・中・低で評価。手軽で全体把握に向く



定量的アプローチ

金額・確率で精緻算出。工数は大きい



分析の核心

基準を先に決めろ。後出しにすると恣意的な判断が入り込む。

● リスク分析 4 つのアプローチ

1

ベースライン

既存ガイドラインをもとに未導入の管理策を補強する

2

非形式的

専門家の知識と経験で素早く当たりをつける手法

3

詳細リスク分析

資産ごとに資産価値・脅威・脆弱性を精緻に識別

4

組み合わせ

重要資産は詳細に、その他はベースラインで効率化

重要資産だけ詳細に使い。



● 4つのリスク対応

1

リスク低減

管理策を導入して発生可能性・影響度を引き下げる

2

リスク回避

リスクの発生源となる活動そのものをやめる判断

3

リスク移転

保険や委託で影響の一部を外部と分担する

4

リスク受容

根拠と承認のうえで受け入れる意思決定。放置とは別物

4 択でなく組み合わせて使え。



● リスク受容と放置の決定的な違い

リスク受容

意識的な意思決定

- ・ 根拠を明確にして承認を得る
- ・ 受容内容を記録に残す
- ・ 定期的に妥当性を見直す

VS

放置

対応漏れの状態

- ・ なぜ対応しないかが不明
- ・ 責任者の承認がない
- ・ 審査で厳しく問われる



受容の核心

根拠と承認のない放置は言い訳が効かない。

● 形骸化させる 3つの失敗パターン



洗い出して終わり

対応に結びつかず台帳作りが目的化する



評価基準が曖昧

担当者ごとに結果がぶれ説明責任が果たせない



更新されない

環境が変わってもリスク一覧が去年のまま止まる

トリガーを仕組みにしないと形骸化は必ず起きる。善意だけでは回らない。



● GRC ・ ISMS 運用で高まる市場需要



設計できる人材が不足

リスクを測る仕組みを作れる層が慢性不足



GRC を横断して見られる

ガバナンス・リスク・コンプライアンスを一体で担う



希少性の核心

手を動かす人はいる。設計できる人間が少ない。そこが市場価値だ。



● フリーランス案件の単価目安

対象となる工程



要件定義

ISMS 基準・リスク評価プロセスの設計



PMO

ISMS 認証プロジェクトの進捗・体制管理



設計

管理策の選定・SoA 策定・実装計画立案

月額単価の目安



要件定義工程

中央値 115 万円



PMO 工程

中央値 100 万円



設計工程

中央値 92.5 万円

設計力が単価を上げる



● まとめ



3 ステップ（特定・分析・評価）で進め、評価基準を先に定める



4 つの対応（低減・回避・移転・受容）は状況に応じて組み合わせる



リスク設計を担える人材は上流工程で高く評価される

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 >](#)

