サイバーセキュリティ
フレームワーク完全ガイド

主要 7 種の比較・選び方から実務活用まで

年収 600 万〜 1,500 万円キャリアへの近道

どれを選べばいいでしゅ？

全体像から整理していこう

セキュリティエンジニア/コンサルタント特化型

セキュリティプロ・フリーランス

登録・利用 完全無料

最高月収150万円

月額80万円以上の案件が
80%以上を占める高単価

リモート率80%以上

フルリモート対応可能案件多数
自由な働き方を実現

専門特化サポート

セキュリティ領域に精通した
専任エージェントが伴走

フリーランス案件マッチング

- 高単価案件から長期安定稼働の案件まで多数保有
- 脆弱性診断、SOC構築、ゼロトラスト導入など幅広い専門案件
- 面倒な営業活動・単価交渉・契約手続きは全て代行

キャリアサポート

- 業界に精通したエージェントがあなたの市場価値を最大化
- 独立支援（会社員から個人事業主、法人設立までサポート）
- 定期的な技術情報共有会、起業支援パックの提供

支払サイト
月末締め翌月払い (30日サイト)

案件参画スピード
2週間〜1カ月程度

詳細を見る →

フレームワークが今注目される背景

攻撃の高度化

ランサムウェア・サプライチェーン攻撃が過去最大規模に拡大

法規制の急速な整備

経済安全保障推進法・サイバー対処能力強化法など規制が強化

本質

フレームワークは「あると望ましい」から「なければ経営リスク」へ

フレームワーク導入前後の変化

導入前

場当たり的な対策

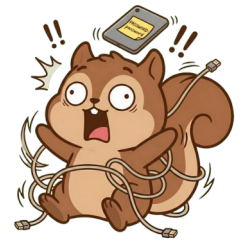
・リスクが属人的・断片的
・投資がインシデント後対応
・経営層に技術語が伝わらない
・監査のたびにゼロから準備

VS

導入後

体系的なリスク管理

・リスクが組織横断で可視化
・リスクベースの優先順位づけ
・共通フレームで経営層と対話
・証跡蓄積で監査対応を効率化



差のポイント

「不足が不明」から「優先順位が明確」な状態へ移行できる

代表的フレームワーク 4 選

1

NIST CSF 2.0

世界最普及・ 6 機能で全業種に適用可能なリスク管理フレーム

2

ISO 27001

国際認証規格・第三者認証で取引先への信頼性を対外的に証明

3

CIS Controls

技術的対策の優先順位リスト・中小企業は IG1 の 56 項目から着手

4

MITRE ATT&CK

攻撃者の TTPs 体系化・ SOC や脅威分析の現場で活用される参照モデル

軸となる 2 つから始めよ

業種・用途別フレームワーク 3 選

PCI DSS v4.0

カード決済事業者向け。違反で月額最大 10 万ドルの罰金リスクあり

経産省ガイドライン

日本の経営者向け。 3 原則・ 10 項目で経営層の理解を得やすい指針

SP800-171/CMMC

防衛調達・サプライチェーン向け。日本の防衛産業基準の元となる

PCI DSS v4.0.1 は 2025 年 3 月に全 64 要件が完全適用済み

NIST CSF 2.0 の 6 つのコア機能

1
ガバナンス (GV)
セキュリティ方針の経営承認・リスク委員会の設置（新設の司令塔）

2
識別 (ID)
情報資産台帳の整備・リスクアセスメントで守るべき対象を把握

3
防御 (PR)
アクセス制御の標準化・教育訓練の体系化で保護策を実装

4
検知 (DE)
SIEM 導入・異常検知ルール整備で潜在的な侵害を発見・分析

5
対応 (RS)
インシデント対応手順書の整備・机上演習で即応体制を構築

6
復旧 (RC)
バックアップ戦略の策定・復旧訓練で影響を最小化して復元

ティアで自組織の成熟度を測る

4 段階のティアレベル

Tier1→4 の順で成熟度が上がる 4 段階の自己評価軸

ギャップ分析の 4 ステップ

As-Is 評価→ To-Be 設定→差分特定→優先順位づけで改善計画を策定

重要原則

全て Tier 4 を目指す必要はない。リスクに応じた目標ティアを設定する

フレームワーク導入３ステップ

1

資産棚卸し

ハード・ソフト・データ・人的資産を整理してリスクを見える化する

2

ギャップ分析

ティアで As-Is と To-Be の差を把握し優先して強化する領域を特定

3

ロードマップ策定

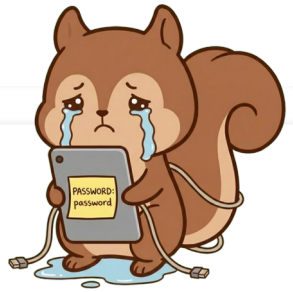
経営層を巻き込み短期・中期・長期の KPI で段階的な改善計画を立てる

全部やらないのが成功の秘訣だ

導入の典型的な失敗パターン３つ

形だけの導入

認証取得がゴールになり実際のリスク管理に活かされない状態



現場が回らない

理想的な対策を盛り込みすぎて日常業務と両立できなくなる

経営層の理解不足

セキュリティをコストと捉え投資判断が先送りされ続ける

経産省ガイドライン３原則を経営層と共有し経営リスクとして認識させる

フレームワーク人材の年収相場

正社員・コンサルタント

セキュリティエンジニア

500 万〜 900 万円（経験・企業規模による）

セキュリティコンサルタント

600 万〜 1,500 万円（ GRC ・ CSF 知識で上振れ）

CISO ・セキュリティ責任者

1,000 万〜 2,000 万円（経営視点が必須）

フリーランス・独立

月額平均単価

70.4 万円 / 月（年収換算 844 万円）

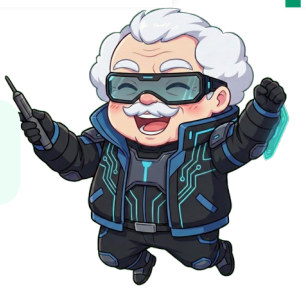
ISMS 審査員・ CSF 導入支援

月額 100 万円超の独立案件あり

実装のみ vs フレームワーク

年収差 100 万〜 300 万円のケースも

知識が年収を上げる



フレームワーク知識で開くキャリアパス

コンサルタント・ GRC 専門家

NIST CSF ・ ISMS 導入支援で年収 1500 万円レンジへ到達できる

フリーランスアドバイザー

ISMS 審査員や CSF 導入支援で月額 100 万円超の独立も可能

市場価値の源泉

「実装できる」から「経営層にリスクを語れる」への進化が年収差を生む

まとめ｜フレームワークを使いこなす人材へ

フレームワークは場当たり対策から脱却する設計図。 NIST CSF と ISMS を軸に理解する

NIST CSF 2.0 でガバナンス機能が新設。経営層の関与がセキュリティの中心になった

フレームワーク知識は年収 600 万〜 1,500 万円のキャリアレンジを開く実践的な武器

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 ＞