SOC と CSIRT

違いと使い分け

「検知の目」と「指揮の司令塔」は何が違うのか？

役割・連携フロー・スキル・資格・案件単価を解説

どっちも同じでしゅ…？

見張りと指揮官くらい違う。

【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。**

SOC と CSIRT の根本的な違い

SOC

検知・分析の部隊

・攻撃の兆候を見つける「検知の目」
・ 24 時間 365 日の常時監視
・技術（監視・分析）中心

VS

CSIRT

対応・指揮のチーム

・見つかった後に動く「指揮の司令塔」
・インシデント発生時に対応
・技術＋経営・法務・広報

役割の核心

優劣ではない。見張りと消防指揮官の分担だ。

SOC とは監視・分析の専門部隊

常時監視とトリアージ

ログ・アラートを 24 時間監視し本物の脅威を選別

SIEM と EDR の運用

監視ツールのチューニングで検知精度を高め続ける

SOC の核心

見つける精度が、その後の対応速度を決める。

CSIRT とは対応を指揮するチーム

対応方針の決定・指示

SOC からの報告を受け隔離・復旧・再発防止を指揮

組織横断で動く

経営層・法務・広報まで巻き込んで組織を動かす

CSIRT の核心

技術屋の集団ではない。組織そのものを動かす役だ。

MDR と PSIRT の位置づけを整理する

SOC/CSIRT

組織が持つ機能・役割そのもの。内製か外部かは形態の話

MDR

SOC 機能を外部委託で調達するサービス形態。調達方法の区分

PSIRT

自社製品の脆弱性に対応するチーム。守る対象が製品・サービス

MDR は組織ではなくサービス。 PSIRT は守る相手が違う。混ぜるな。

インシデント発生時の対応フロー

1. **SOC が異常を検知**
   ログ・アラートを分析し、インシデントかどうかを判断する
2. **CSIRT へ報告**
   脅威と判断したらエスカレーションして引き継ぐ
3. **対応方針を決定**
   CSIRT が指示を出し、封じ込めの判断を下す
4. **隔離・復旧を進める**
   封じ込め・復旧まで指揮しながら対応を完結させる
5. **原因分析・再発防止**
   事後に SOC と CSIRT が共同でレビューし次に備える

平常時と有事でどう役割が分かれるか

平常時

準備・積み上げの時間

- SOC: 常時監視・精度チューニング
- CSIRT: 手順書・訓練の整備
- 地味な準備が有事の速度を決める

VS

有事（発生時）

即応・指揮の時間

- SOC が異常を検知・分析
- CSIRT に報告し対応方針を指示
- 平時の型通りに動けるかが勝負

準備の核心

平時の質が有事のスピードに直結する。手を抜くな。

なぜ今 SOC と CSIRT 両方が必要か

攻撃は「起きる前提」に変わった

ランサムウェア・サプライチェーン攻撃で防ぎきれなくなった

制度・商流からの圧力

取引先からのセキュリティ体制確認が広まり整備が必須に

需要の核心

「起きる前提」に立てば、両輪が必要なのは自然な流れだ。

SOC と CSIRT で求められるスキルの違い

SOC アナリスト

監視・分析が軸

・ログ分析・異常の読み取り
・ SIEM ・ EDR の運用スキル
・トリアージと影響範囲の見極め

VS

CSIRT メンバー

技術＋マネジメント

・フォレンジック・マルウェア解析
・関係部署との調整・意思決定
・広報・法務との連携スキル

スキルの核心

SOC で見つける力を磨き、 CSIRT で動かす力に広げろ。

両者に効く資格の当たり

情報処理安全確保支援士

IPA 認定の国家資格。国内で最も評価が高い入り口

CISSP と CompTIA

CISSP= 国際資格、 Security+/CySA+= 実務寄りの入門

資格の核心

取って終わりではない。実務でどう使うかまで踏み込め。

キャリアパスとフリーランス単価の実際

正社員のキャリアパス

SOC アナリスト
監視・一次分析でトリアージ精度を磨く

上位アナリスト・ SOC リード
分析の深掘りとチーム牽引へ

CSIRT マネジメント
対応の指揮・体制運営へ広げる

案件単価公開中

フリーランス月額単価

全体中央値
92.5 万円（ 50 ～ 180 万円）

要件定義・ PMO
100 ～ 115 万円（上流は高い）

運用・保守
90 万円（ 50 ～ 130 万円）

まとめ

SOC は検知、 CSIRT は指揮。優劣ではなく役割分担の関係だ

連携してこそ機能する。片方だけでは必ず穴が空く

SOC で土台を固め、 CSIRT で指揮する側へ広げていけ

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 ＞