CSIRT 体制図の作り方

公式モデルで役割分担

自社に合う体制図、どう描く？

3 要素・ 5 形態・役割・ SOC/PSIRT ・運用を解説



箱を並べれば完成でしゅか？

線を決めるのが本題だ



セキュリティプロ

【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。**

© 2026 スプラッシュエンジニアリング

体制図を構成する３つの要素

役割（箱）

機能名で描く統括・窓口・実対応

指揮命令系統（縦線）

コマンダーを頂点にした判断と報告

連絡線（横線）

経営層・各部署・外部機関との接点

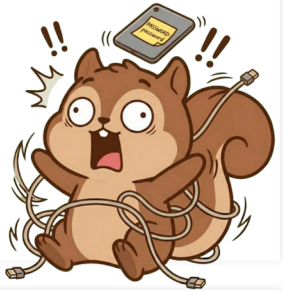
箱より線が本題



唯一の正解がない理由

JPCERT/CC の 3 実装例

独立部署・部署横断・個人が担う形



公式モデルを土台に

論点がそろい抜け漏れを防ぐ型

出発点の核心

規模に合わせて組み替える前提

JPCERT/CC の 5 つの CSIRT 形態



1. **セキュリティチーム**
   管理者などが職務の一部として対応する非公式な形
2. **分散型**
   下位組織の兼務スタッフを一人の責任者が監督・調整
3. **集中型**
   専属スタッフ中心で正式に組織化し全インシデントに責任
4. **統合型**
   中心の CSIRT が下位組織の CSIRT を調整
5. **調整役型**
   組織内外の対応調整や環境構築を担当

形態を選ぶ３つの問い

専任を置けるか

不可ならセキュリティチームから開始



拠点は分かれるか

各所に兼務者を置ける分散型が候補

まず何から始めるか

連絡だけか調査まで自社で担うか

回せる型から始める



指揮系統の中核となる 4 役割

指揮と報告（縦の線）

コマンダー

全体統括・意思決定・経営層との連携

インシデントマネージャー

対応状況の把握とコマンダーへの報告

連絡の窓口（横の線）

社内 PoC

法務・広報・各事業部と連携

社外 PoC

NCA ・ JPCERT/CC ・警察と連携

まず 4 つの箱から決めろ



実務を担う 4 つの役割

1. **トリアージ**
   届いた事象の優先順位を決定
2. **ハンドラー**
   現場監督とセキュリティベンダーとの連携
3. **フォレンジック**
   証拠保全・鑑識・足跡追跡・マルウェア解析
4. **脆弱性診断士**
   OS ・ネットワーク等の検査と結果の評価

自分はどの箱でしゅ？



少人数は兼任と外部委託で描く

自社に残す役割

コマンダーなど判断と社内調整



外部に委託する役割

フォレンジックなど専門性の高い作業

兼任の核心

兼任の組み合わせを先に決定

SOC と CSIRT の描き分け

SOC

検知の起点

・ログの監視・分析・検知
・ CSIRT へアラートを上げる
・外部サービスなら社外の箱

VS

CSIRT

判断と連絡のハブ

・インシデント対応の統括
・経営層・各部署・外部へ連携
・引き渡し条件を線に明記



線引きの核心

検知後の引き渡し線を明確化

PSIRT と外部機関への連絡線

PSIRT は別の箱

製品・サービスが対象で脆弱性情報を共有

外部窓口は一本化

社外 PoC から各機関へ線を伸ばす

連絡線の核心

窓口集約で勝手な連絡を防止

体制図を確定する 5 ステップ

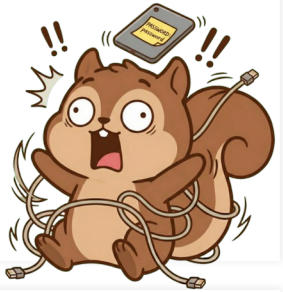
1. **資産の洗い出し**
   守る情報資産と想定インシデントの整理
2. **形態の選定**
   規模と専任人数から型を選択
3. **役割の割り当て**
   兼任・外部委託を含めて配置
4. **流れの決定**
   検知から報告・外部連絡までのエスカレーション
5. **経営層の承認**
   承認を得て正式なルールとして確定



形骸化を防ぐ運用のコツ

演習と見直し

検知から外部報告まで定期的に実施



経営層の巻き込み

判断者が流れを体験して意思決定を迅速化

運用の核心

訓練と図の更新をセットで実施

働き方別の相場の目安

正社員（転職）

CSIRT タグ付き求人

24 件を公開中

年収の中央値

665.0 万円（全体は 700.0 万円）

フリーランス（案件参画）

月額の中央値

90.0 万円（ 133 件）

上流役割の中央値

コンサル 115.0 万円・ PM110.0 万円

どの箱を担ったかが武器だ



まとめ｜型を土台に自社仕様へ落とす体制図

- 箱より指揮系統と社内外の連絡線が本題
- 5 形態と役割表を土台に自社の規模へ調整
- 訓練と見直しで図を現実に合わせて更新

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 ＞

