

CSIRT とは？

役割・作り方・キャリア

専任ゼロでも動く？対応力の作り方

定義・SOC 比較・4 ステップ・案件単価を一挙解説



CSIRT って何でしゅか？

定義から始めれば全部つながるぞ



【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。

● CSIRT の定義と読み方



正式名称の意味

「シーサート」と読む対応専門チーム



専任部署は不要

兼任メンバーが機能を担う形も有効



定義の核心

対応機能があれば CSIRT と呼べる

● 設置が広がる 3つの背景



攻撃の深刻化

ランサム・サプライチェーン攻撃が IPA 脅威の上位に



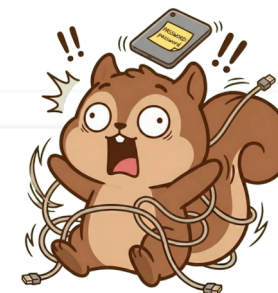
法規制の強化

改正個人情報保護法で漏えい報告が義務化された



取引先からの要求

セキュリティ対応体制の証明を求められる場面が増加



3つの圧力が重なり CSIRT は任意から必須へと変わりつつある



● 事後対応（リアクティブ）の流れ



検知・トリージ

優先順位を即断し対応方針を決める



封じ込め・復旧

被害拡大を止めシステムを正常化



対応の核心

トリージの精度が初動の成否を決める

● 事前対応（プロアクティブ）の役割



脅威情報の収集

インテリジェンス収集と社内への注意喚起



訓練と外部連携

JPCERT/CC など外部組織との情報共有



備えの本質

事前対応が有事の被害を最小化する



● SOC と CSIRT の役割比較



● PSIRT ・ 情シスとの役割分担

PSIRT



対象

自社製品・サービスの脆弱性対応



主な業務

脆弱性報告受付とパッチ提供調整

情報システム部門



対象

社内 IT 基盤の構築と運用保守



主な業務

システム開発とインフラ管理

役割を分けて機能させろ



● CSIRT の 4 タイプ

1

組織内 CSIRT

自社の従業員とシステムを守る最も一般的な形態

2

国内調整 CSIRT

JPCERT/CC のように国全体のインシデント調整を担う

3

ベンダー CSIRT

自社製品に関するセキュリティ対応を専門に担う

4

サービス提供型

他組織へ CSIRT 機能を提供するプロフェッショナル集団

まず自組織がどの型か把握しろ



● CSIRT 構築の 4 ステップ

1

経営層の合意

目的と権限を明確にしトップダウンで動き出す

2

範囲と体制図

対象システムと役割分担を文書化して共有する

3

手順の整備

インシデントハンドリング手順を最初に固める

4

訓練で検証

実際に動かして穴を塞ぐ。机上論では不十分だ

経営の合意なき体制は動かんぞ



● 中小企業でも回す外部活用



MSSP 委託

監視・運用を専門業者に委託し自社の負荷を削減



仮想 CSIRT

法務・広報・人事などの兼任メンバーで構成する形



外部専門人材

フリーランスや支援会社で専門スキルを補完する



連絡網ひとつでも無いより何倍もマシだ。まず動ける形を作れ



● CSIRT に求められるスキル

技術スキル



ログ分析

インシデントの原因と経路を特定



脆弱性の理解

既知の攻撃手法と対策を熟知する

ソフトスキル



経営層への報告

非技術者に状況を伝える力



部門間の調整力

法務・広報・人事を動かす力

技術と調整の両輪が必要だ

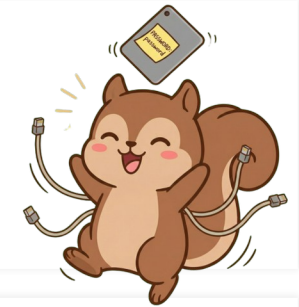


● CSIRT で評価される資格



情報処理安全確保支援士

国内認知度が高い国家資格



CISSP ・ Security+

国際的マネジメント ・ 基礎資格



資格の本質

資格は実務経験との掛け合わせで生きる

● CSIRT キャリアとフリーランス



キャリアの4段階

アナリスト→シニア→マネージャー→CISO



フリーランス単価

上流は中央値 92.5 万～ 115 万円、運用・保守は 90 万円



単価の核心

実務経験が深いほど市場評価は上がる



● まとめ | CSIRT の本質とキャリアの活かし方



CSIRT は専任不要・兼任と外部活用で構築できる対応機能



SOC は検知・CSIRT は対応—連携が初動の速度を決める



実務経験 × 資格がフリーランス単価を押し上げる

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 >](#)

