サイバーだより

栃木県警察
サイバー対策センター
令和７年４月

◆ CSIRTのススメ ◆

●CSIRT（シーサート）＝Computer Security Incident Response Team

セキュリティインシデント（マルウェアの感染や不正アクセス、機密情報の流出など、セキュリティ上の脅威となる事象）が発生した際に対応するチーム。各組織の実情に応じて様々な形態がある。（独立部署が担当、部署横断的に組織、個人がCSIRTを担当等）

CSIRT
部署横断で
構築する例


システム部門


事業部門


広報部門


法務部門

◎事後対応
・アラートと警告
・インシデントハンドリング
・脆弱性ハンドリング
等々

◎事前対応
・技術動向監視
・セキュリティ情報の提供
・セキュリティ監査
等々

◎セキュリティ品質管理
・リスク分析
・事業継続計画
・啓発、教育、トレーニング
等々

インシデントが発生したときは、さまざまな社内調整や、広報対応など会社全体を巻き込んだ対応が発生します。
これらを完全に外注（アウトソース）することは難しいので、自社組織内でCSIRTを運営・運用する体制を構築する企業が増えています。

【CSIRT構築の留意点～形だけのCSIRTは意味がありません～】

各組織の実情に応じて構築されるため、一つとして同じものは存在しません。機能するCSIRTを実現するに当たっては、まず**既存の体制を整理、見直したうえで、大きく作り変えるのではなく、足りない機能を付け加えて体制を構築する**ことが肝要です。

CSIRT構築の参考資料

① 一般社団法人日本シーサート協議会
・「CSIRT構築ガイド」
② JPCERTコーディネーションセンター
・「CSIRTマテリアル（構想・構築・運用フェーズ）

①

②

栃木県警察
Tochigi Police

栃木県警察ＨＰ(サイバーだより)
https://www.pref.tochigi.lg.jp/keisatu/n14/seikatu/cyber_cyber_dayori.html