5分でわかる CSIRT と SOC

NTTセキュリティ・ジャパン株式会社
羽田 大樹

NTT Security

CSIRT と SOC （Wikipedia より）

NTT Security

CSIRT（Computer Security Incident Response Team、シーサート）とは、コンピュータやネットワーク（特にインターネット）上で何らかの問題（主にセキュリティ上の問題）が起きていないか[1]を監視すると共に、万一の問題が発生した場合にその原因解析や影響範囲の調査を行ったりする組織の総称。

CSIRT ⇒ 組織を守るための組織

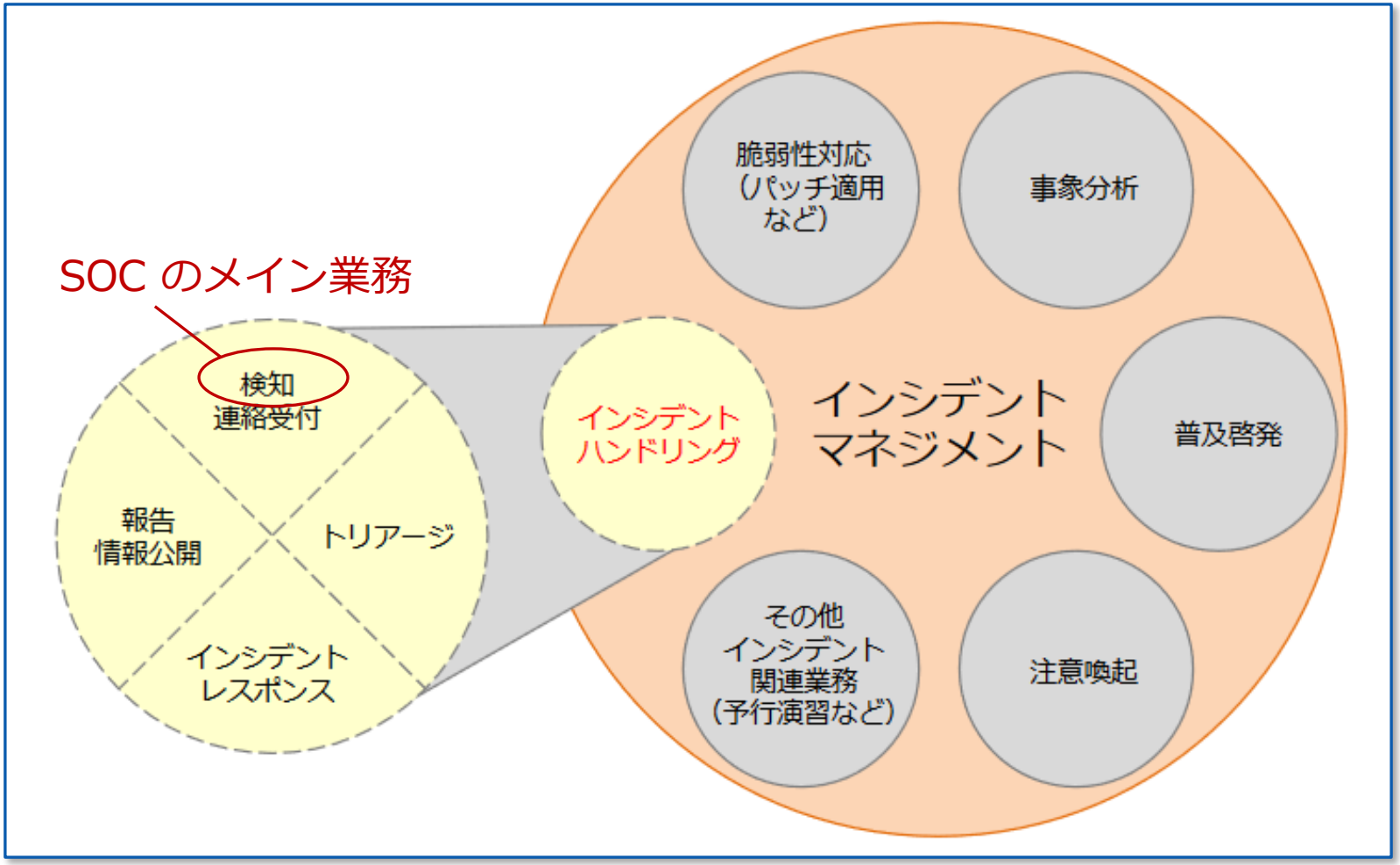
セキュリティオペレーションセンター（英: Security Operation Center）とは、顧客または自組織を対象とし、[illegible]器、サーバーコンピュータ[illegible]が生成するログを監視・分析し、サイバー攻撃の検出・通知を行う組織である[1]。

SOC ⇒ 脅威を見つけるための組織

CSIRT と SOC の業務 (1)

NTT Security

- JPCERT/CC 「インシデントハンドリングマニュアル」より

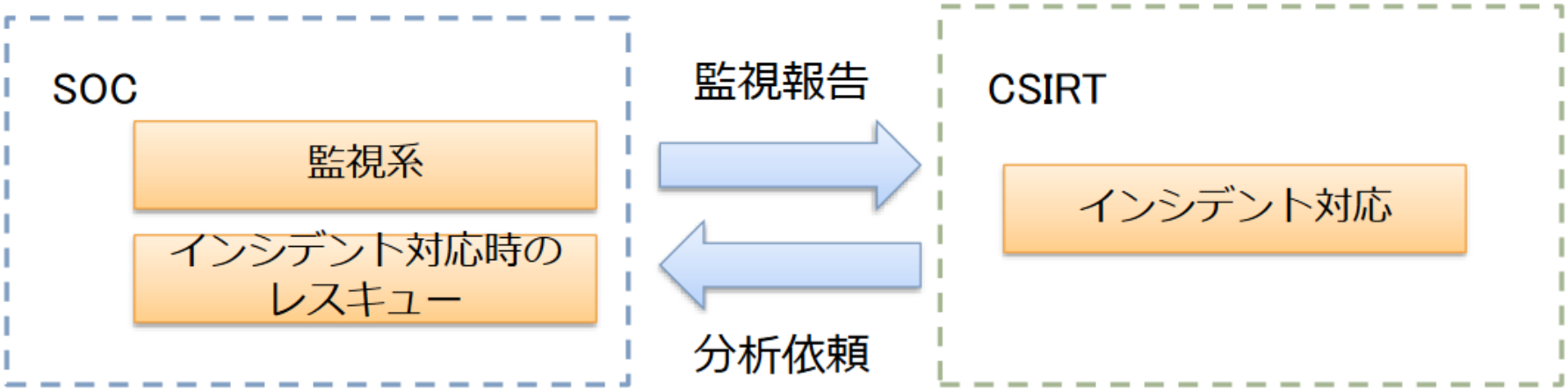


CSIRT と SOC の業務 (2)

NTT Security

・ISOG-J 「SOCの役割と人材のスキル」より

- 日本においては、監視やインシデント対応時のレスキューサービスをSOC、インシデント対応をする組織をCSIRTと呼称する場合が多い。



CSIRT と SOC のやりがい（個人的見解）

NTT Security

- CSIRT
  - インシデント対応を最後まで手当てできること
  - 自組織に最適なセキュリティ対策を立案から実装まで実行できること

- SOC
  - セキュリティ技術に特化した分析や解析ができること
  - 広いフィールド情報に触れられること