JPCERT CC®

組織内における CSIRT の形態

一般社団法人
JPCERT コーディネーションセンター

目 次

- 組織内における CSIRT の形態の分類
  - セキュリティチーム
  - 分散型 CSIRT
  - 集中型 CSIRT
  - 統合（分散／集中）型 CSIRT
  - 調整役 CSIRT
- 組織の実情に合わせた CSIRT の選択

（参考）さまざまな CSIRT の名称

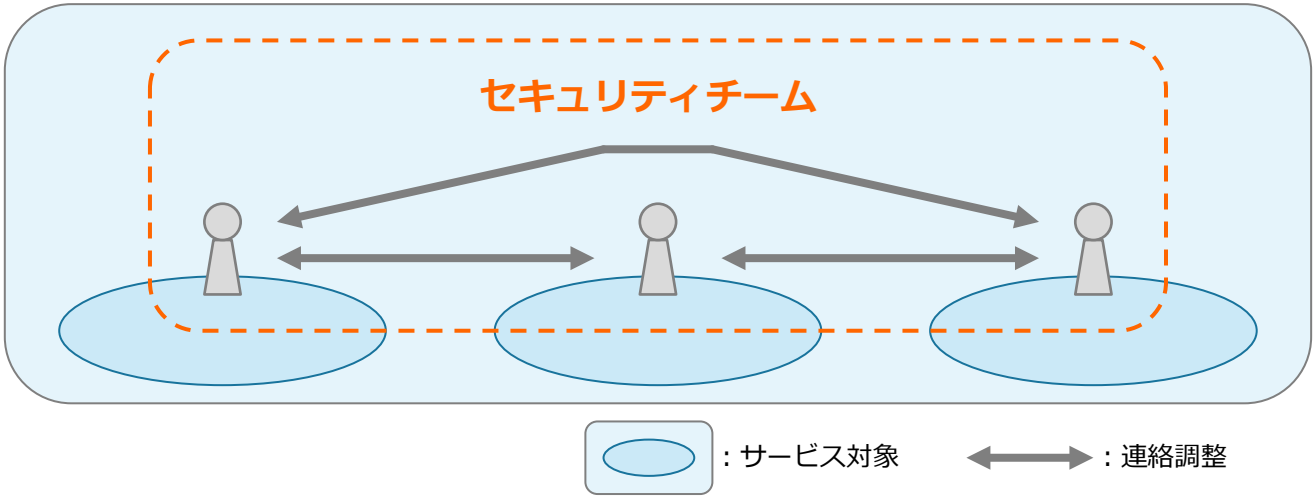
組織内における CSIRT の位置づけの分類

- セキュリティチーム
  - Security Team
- 分散型 CSIRT
  - Internal Distributed CSIRT
- 集中型 CSIRT
  - Internal Centralized CSIRT
- 統合（分散／集中）型 CSIRT
  - Internal Combined Distributed and Centralized CSIRT
- 調整役 CSIRT
  - Coordinating CSIRT

※参照元：*Organizational Models for Computer Security Incident Response Teams (CSIRTs)*
http://www.cert.org/archive/pdf/03hb001.pdf

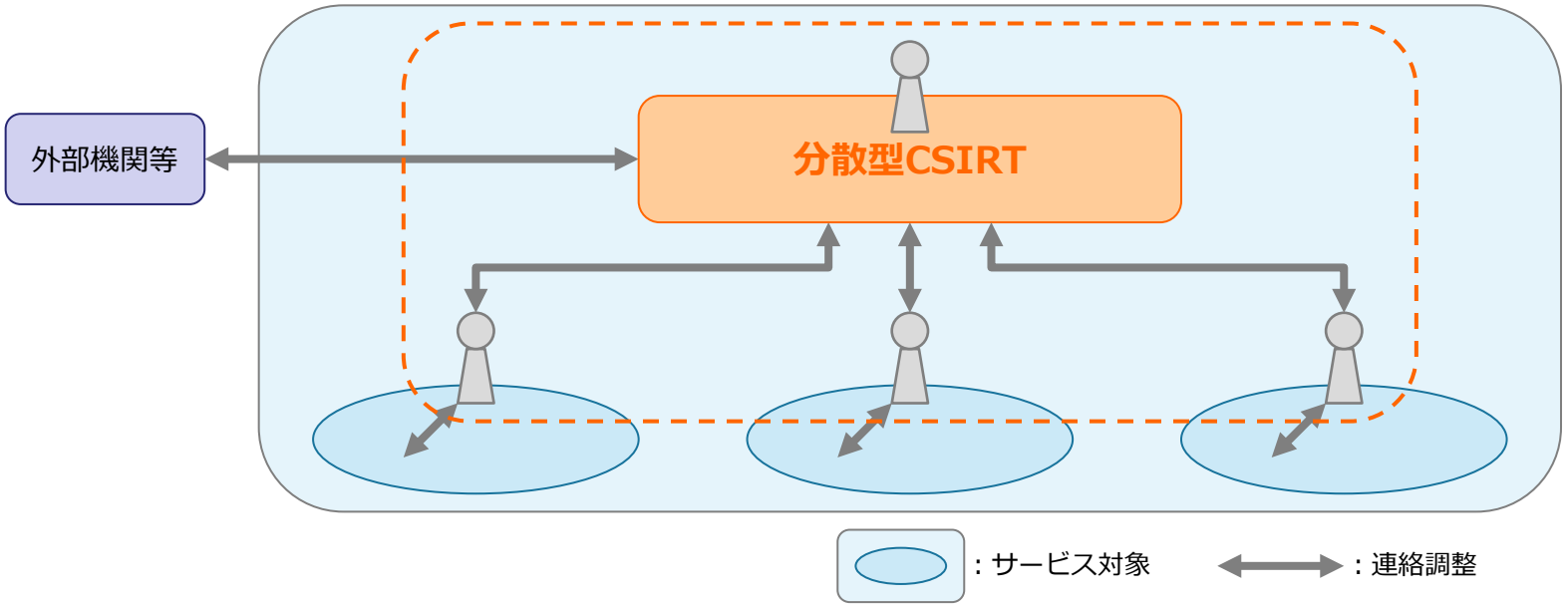
セキュリティチーム

- 正式な CSIRT の組織体ではない（既存のＩＴエンジニア等を活用）
- システム管理者、ネットワーク管理者、セキュリティ管理者などの職務の一部として、セキュリティインシデントに関する対応をとる
- 組織全体におよぶインシデントへの対応が難しい
- 復旧のために組織全体から情報を集めたり、最新の脅威情報を収集し、所属組織への影響度を考察し、報告するような組織ではない
- “Business as usual”（いつもどおり）のアプローチであり、インシデント対応としては極めて限定的な活動となる
- 組織内において、CSIRT として認知されていないことが多い



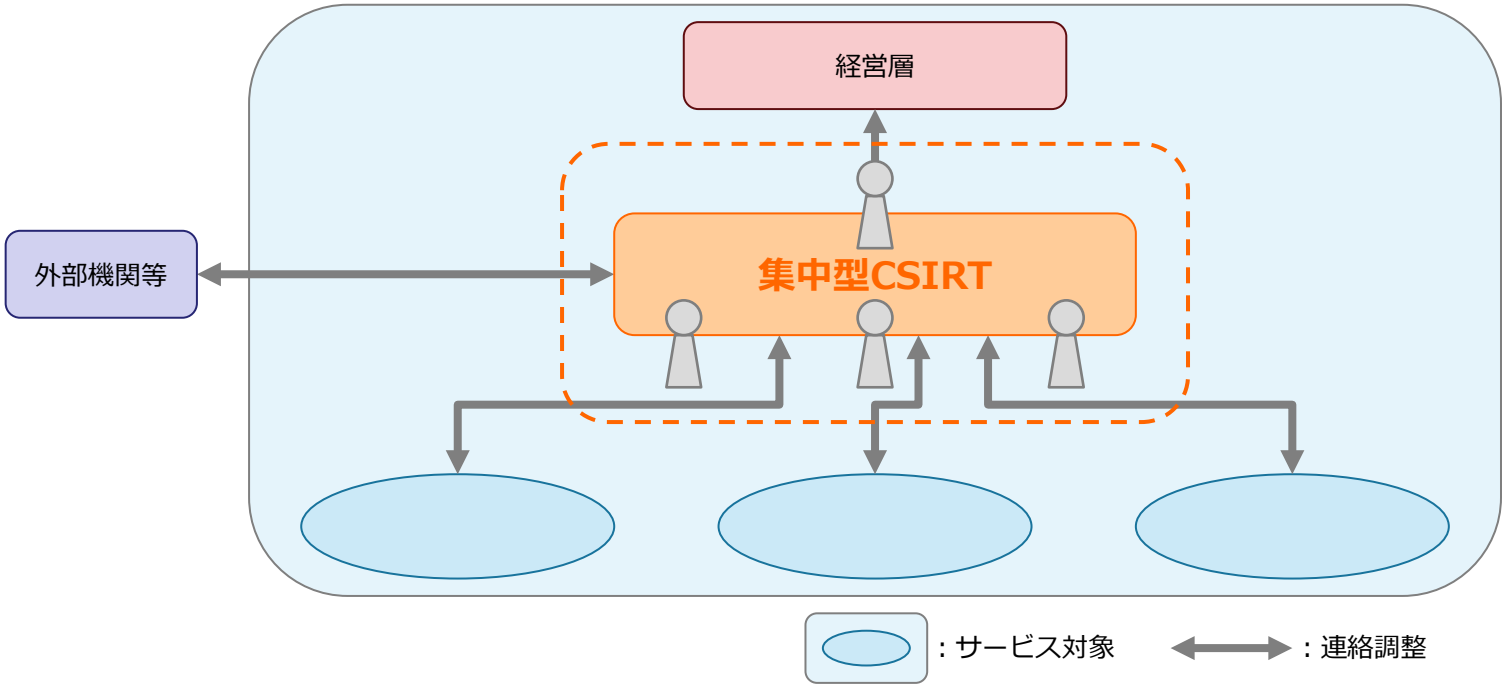
分散型 CSIRT

- 一部またはすべての下位組織の中に、仮想的に（場合によっては兼務で）CSIRT のスタッフを指定する
- 一人の責任者（マネージャ）が、監督及び調整役を担う
- スタッフは、それぞれのエリア担当をベースにしながら、インシデント発生時には、CSIRT のスタッフとして活動をする。また、何人かは、CSIRTの業務のみを専門にする
- このタイプの CSIRT は、外部から見たこの組織の SPOC（Single Point of Contact:単一窓口）としての機能を持つ



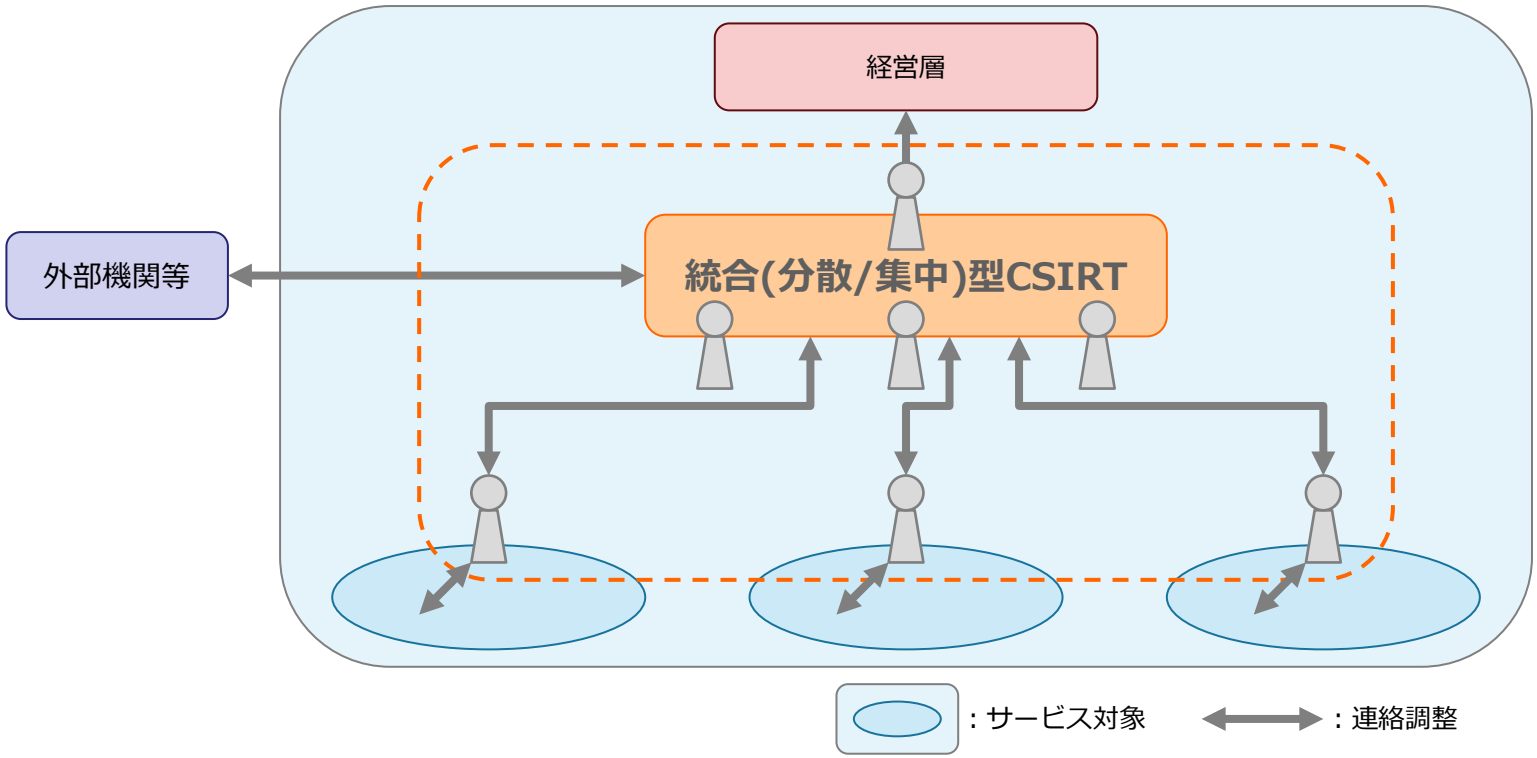
集中型 CSIRT

- 専属のスタッフで構成されているが、何人かは、下位部署との兼務やローテーションで活動する場合がある
- 責任者（マネージャ）や組織の経営層（CIO など）に対する報告義務を伴う
- 正式に組織化され、組織内で発生するすべてのインシデンへの対応に責任を持つ
- このタイプの CSIRT は、外部から見たこの組織の SPOC としての機能を持つ



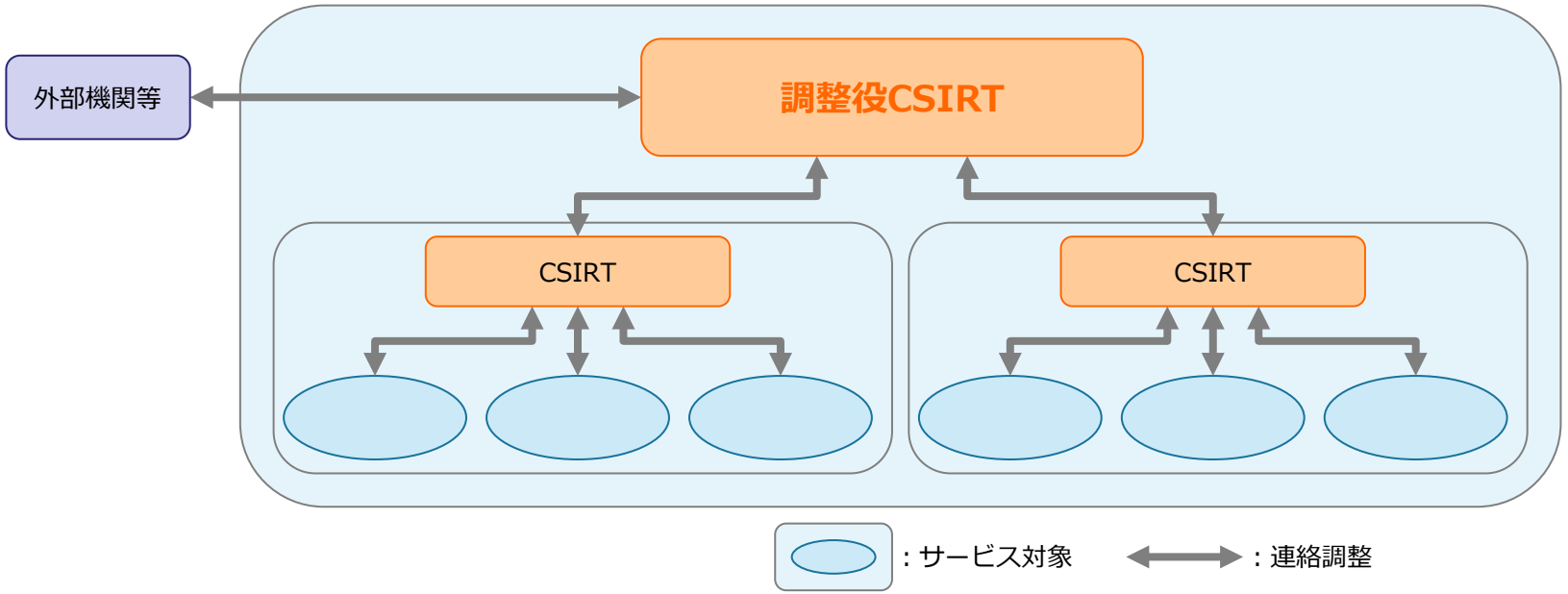
統合（分散／集中）型 CSIRT

- 分散型と集中型を合わせた CSIRT
- 組織全体におよぶセキュリティインシデントに対応できる体制を整えるため、既存の社員を最大限に活用する
- この CSIRT を中心に、下位組織の CSIRT を調整できる能力を持たせる
- このタイプの CSIRT は、外部から見たこの組織の SPOC としての機能を持つ



調整役 CSIRT

- 組織の内外に対するインシデントレスポンスの調整をしたり、その環境を構築する役割を担う CSIRT （組織外に関しては、他の組織の CSIRT との連携を指す）
- この CSIRT は広い範囲を対象とし、さまざまなサービス対象を持つ
- 他の組織のインシデントレスポンスを支援するための連絡調整もする



組織の実情に合わせた CSIRT の選択 1

「セキュリティチーム」を選択することが多い状況

- 組織内にインシデント対応を専門に担当している部署がない
- 既存の IT 部門やセキュリティグループ等のメンバが、通常業務の一部として、セキュリティインシデントを扱う
- インシデントが発生する都度、チームが結成され、比較的現場に近いところで対応をする

組織の実情に合わせた CSIRT の選択 2

「統合（分散／集中）型」を選択することが多い状況

- CSIRT がサービス対象と同じ組織内に存在している
- 最も優先すべき活動が、インシデント対応、あるいは、その支援である
- インシデント対応あるいはその支援に対して、特別な権限が与えられている

組織の実情に合わせた CSIRT の選択 3

「調整役」を選択することが多い状況

- CSIRT がインシデント対応に必要な情報を取りまとめ、調整することによって、実際のインシデント対応に役立つ情報の流通を図っている
- 事前に、インシデントに関する情報の調整やインシデント対応の活動に関するノウハウの提供などを実施している
- メンバは、実際のインシデントが発生した現場で対応することは少ない

（参考） さまざまな CSIRT の名称

- CSIRT
  - Computer Security Incident Response Team
- CSIRC
  - Computer Security Incident Response Capability
- CIRC
  - Computer Incident Response Capability
- CIRT
  - Computer Incident Response Team
- IHT
  - Incident Handling Team
- IRC
  - Incident Response Center
  - Incident Response Capability
- IRT
  - Incident Response Team
- SERT
  - Security Emergency Response Team
- SIRT
  - Security Incident Response Team