組織内 CSIRT の要員

一般社団法人
JPCERT コーディネーションセンター

目 次

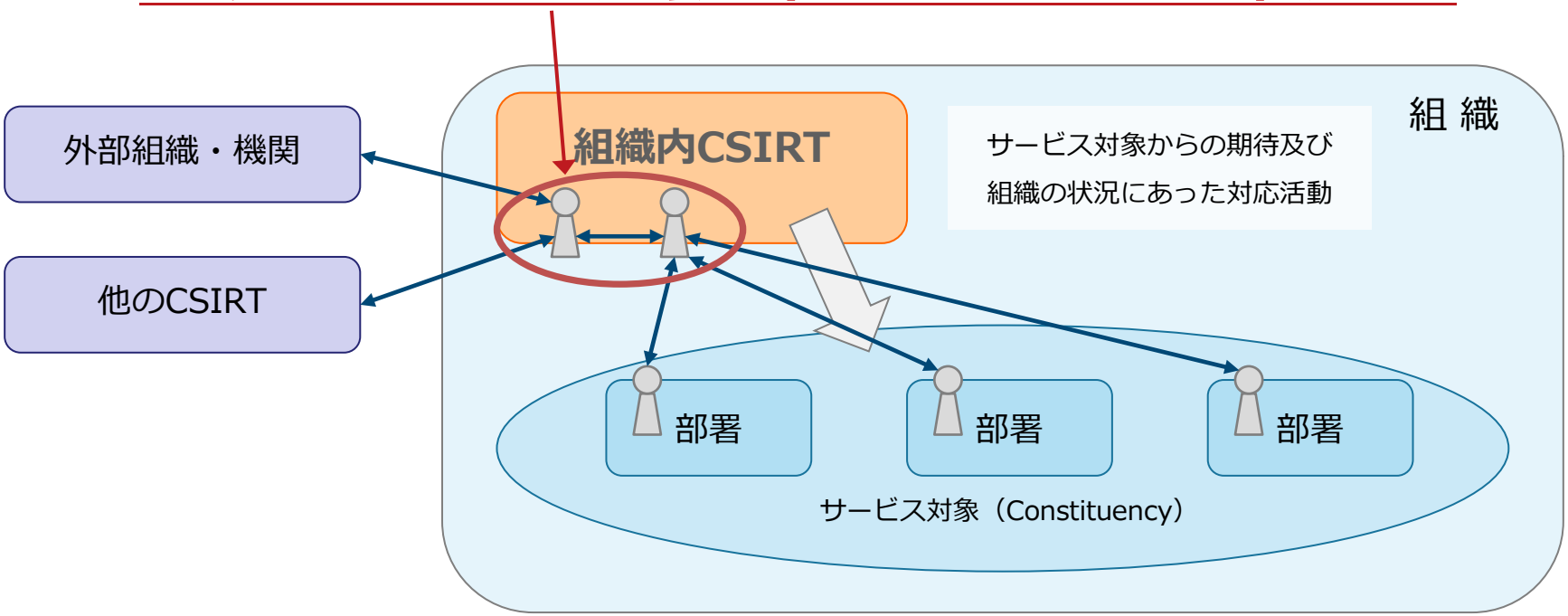
- CSIRT 要員の重要なスキル
- CSIRT 要員に必要なヒューマンスキル
- CSIRT 要員に必要なテクニカルスキル
- CSIRT 要員へのトレーニング

（参考） IT 部門の要員に求められるスキルとの違い

組織内 CSIRT 要員の重要なスキル

- CSIRT の要員は、サービス対象者や他の CSIRT を含む外部組織や機関との積極的な対話が最も重要

コミュニケーションスキル（対人能力とその意欲）が重要



※注意：図中の「組織内 *CSIRT*」の要員は専任であるとは限らず、他の業務と兼務している場合がある。

組織内 CSIRT 要員に必要なヒューマンスキル

- 組織内 CSIRT 要員のヒューマンスキルについては、以下の**能力及び意欲**を持っていることが求められる
  - 明確な指示や取り決めなどがなく、時間的制約がある状況下でも、必要なことを受け入れ、判断できること
  - 業務内容の異なる部署や、外部組織との対話を円滑にできること
  - 規則や取り決めなどに従うことができること
  - 強いストレスのある状況下で業務を遂行できること
  - チームの評判を守る大局的な視点と行動ができること
  - 勉強を続ける姿勢があること
  - 問題解決能力
  - 他のメンバとの連携能力
  - 時間管理能力

参考文献：コンピュータセキュリティインシデント対応チーム（CSIRT）のためのハンドブック
CERT/CC 発行 （翻訳：JPCERT/CC）

組織内 CSIRT 要員に必要なテクニカルスキル

- 組織内 CSIRT の活動領域であるサービス対象の範囲の業務、システム、ネットワーク、関連規則等の知識以外に、以下のテクニカルスキルを持っていることが求められる
  - インターネットに関する知識
  - ネットワークプロトコル （IPv4、IPv6、ICMP、TCP、UDP）
  - ネットワークインフラ （ルータ、スイッチ、DNS、メールサーバ
  - ネットワーク上のサービス及びその実装プロトコル
    （SMTP、HTTP、HTTPS、FTP、Telnet、SSH、IMAP、POP3）
  - セキュリティの三原則（機密性・完全性・可用性)、多層防御など
  - コンピュータ、ネットワークに対する脅威
  - 攻撃手法（IP スプーフィング、DoS、ウィルス、ワーム等）
  - 暗号化技術（3DES、AES、IDEA、RSA、DSA、MD5、SHA）
  - 運用上の問題（バックアップ、セキュリティパッチ、アップデート）
  - プログラミング及びコンピュータ管理能力

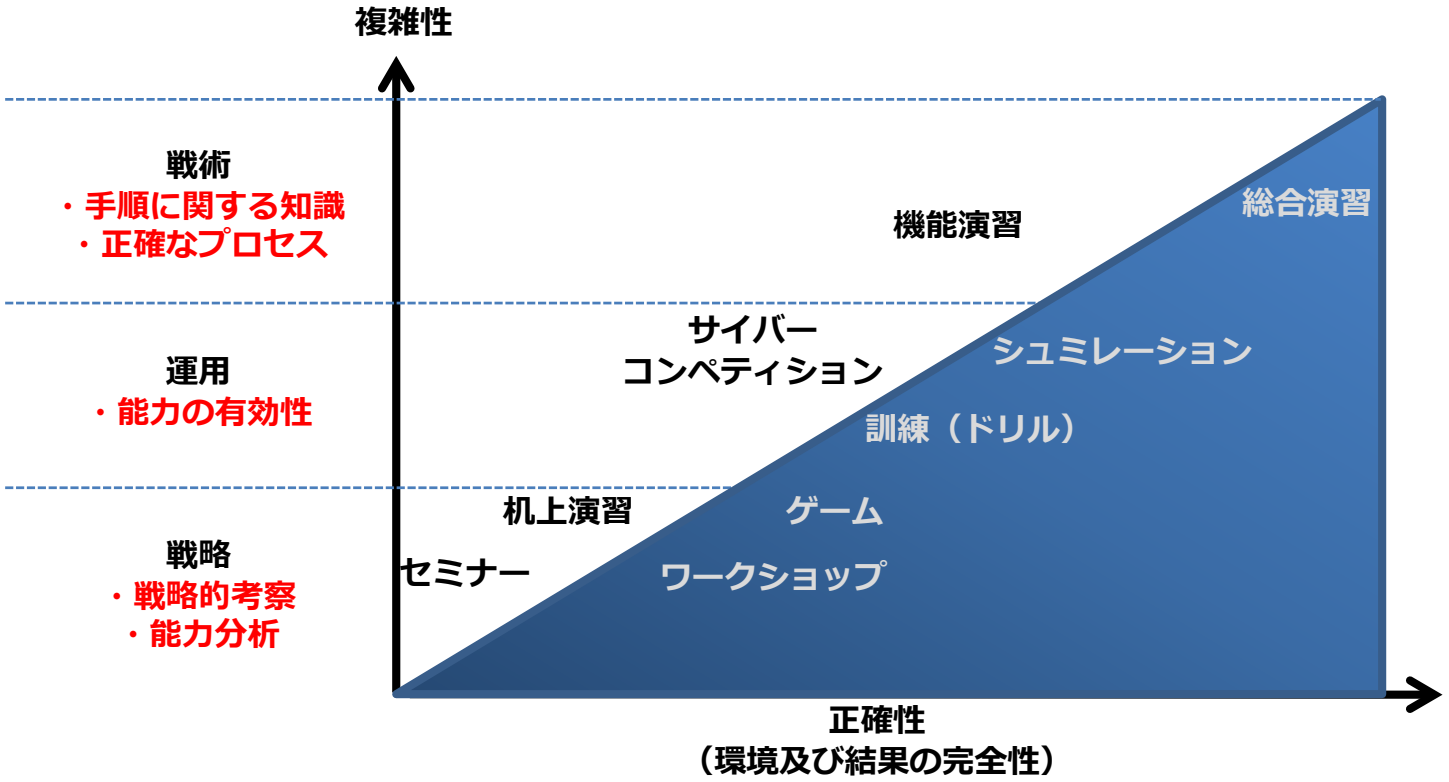
参考文献：コンピュータセキュリティインシデント対応チーム（CSIRT）のためのハンドブック
CERT/CC 発行 （翻訳：JPCERT/CC）

組織内 CSIRT 要員へのトレーニング

- 組織内 CSIRT 要員へは、ヒューマン・テクニカルスキルと先進的な戦術に焦点を当てたトレーニングを実施する必要がある
  - ヒューマン・テクニカルスキル
    - CSIRT要員のベースラインを確保
  - 先進的な戦術
    - 高度サイバー攻撃(APT)に特徴的な攻撃手法、防御対策への理解（年１回以上）
    - 最新のツール(SIEM、UTM等)の知識
    - プロファイルやインディケータ等、外部連携に必要な情報
    - 高度サイバー攻撃(APT)とそれ以外での対応手順の違いへの理解
    - ログの取得や保存に対する理解

訓練・演習の実施

- 組織内CSIRTを含む、インシデント対応に関与する部門・部署を対象に、インシデント発生時を想定した訓練と演習を実施する
- 訓練と演習の実施により、トレーニングの成果を実践し、要員、プロセス、技術に求められるレベルと実際の能力とのギャップを認識することができる



（参考） IT 部門の要員に求められるスキルとの違い

- 組織内 CSIRT 及び IT 部門の要員が必要な能力・スキルに偏りがある
  - 組織内 CSIRT ： 他組織との連絡調整能力とセキュリティ関連スキル
  - IT 部門： 担当しているネットワークやシステムに関する設計・設定の知識

- 以下は、その一例 （※ 共通する部分はあるが、重要度が異なる ）

	組織内CSIRT	IT部門
ヒューマンスキル	1．各部署及び外部との、人との折衝能力及び調整能力 ・ ・ ・	1．チーム活動に必要な連携能力 ・ ・ ・
テクニカルスキル	1．セキュリティの概念 2．攻撃及び防御手法 3．ネットワーク・サーバ関連知識 ・ ・ ・	1．開発手法及び言語 2．ネットワーク設計・設定知識（ルータ、ファイアウォール等） ・ ・ ・
知識	1．最新のインシデント動向 2．組織内の事業に影響を与えるポイント ・ ・ ・	1．組織内ネットワーク及びシステムの構成 2．最新の製品知識 ・ ・ ・