JPCERT CC®

組織内 CSIRT の活動

一般社団法人
JPCERT コーディネーションセンター

目 次

- インシデントの定義の詳細について
- 組織内 CSIRT によるインシデント対応活動
- 組織内 CSIRT の活動の設定について
- 組織内 CSIRT の活動の設定ポイント

（参考） CSIRT の活動内容（サービス）の分類について

- 組織内 CSIRT の活動のフレームワーク
  - 「ミッションフレームワーク」の定義方法
  - 「サービス対象者」の定義方法
  - 「組織内の位置づけ」の定義方法
  - 「他のチームとの関係」の定義方法

（参考） CERT/CC におけるサービスの分類の例

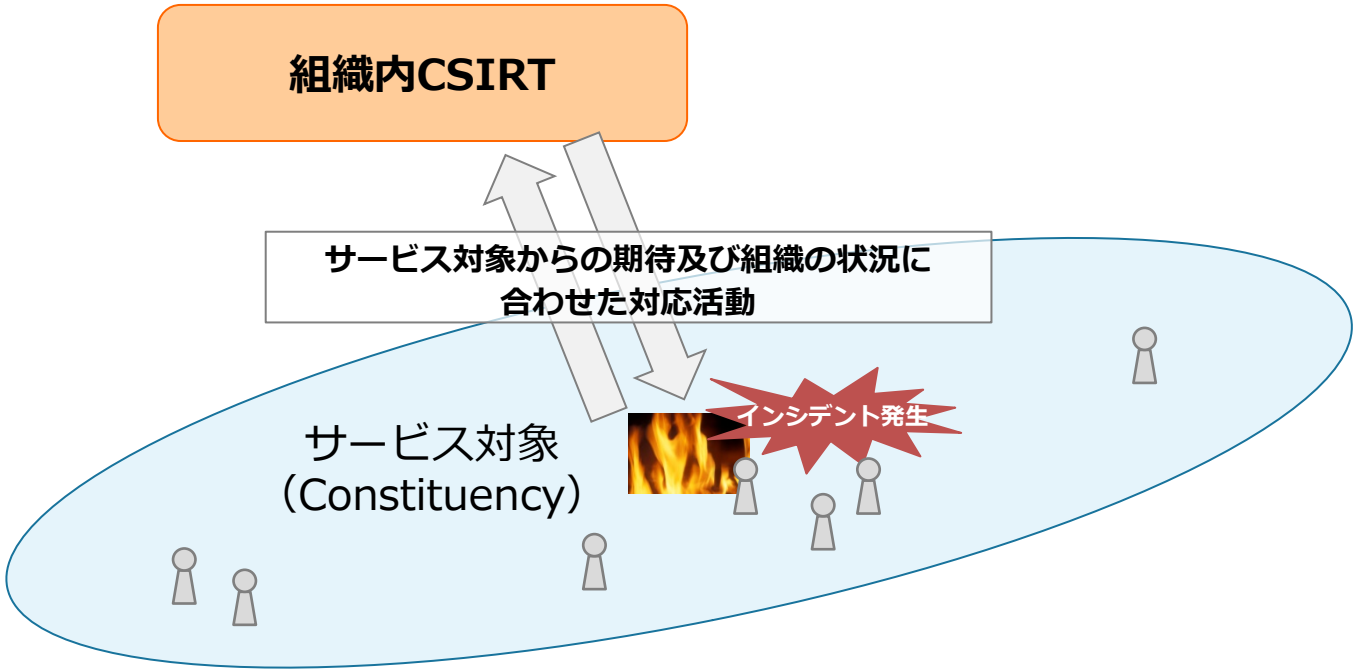
（参考） 「インシデント」「攻撃」「事象（イベント）」の定義の例

（参考） IT 部門の活動範囲の違いの例

インシデントの定義の詳細について

- 組織の事業内容、規模、部門構成、業務遂行形態、事業に対する脅威やリスクの定義により、組織内 CSIRT のインシデントの定義の詳細は異なる
  - 多く見られる定義
    - システムあるいはネットワークのセキュリティに関連した、実際に発生した有害な事象、または、その疑いがある事象
    - 明示的または暗黙的に示されているセキュリティポリシーの違反行為
  - JPCERT/CC による定義
    - コンピュータセキュリティに関係する人為的事象で、意図的および偶発的なもの
    - リソースの不正使用、サービス妨害行為、データの破壊、意図しない情報の開示など

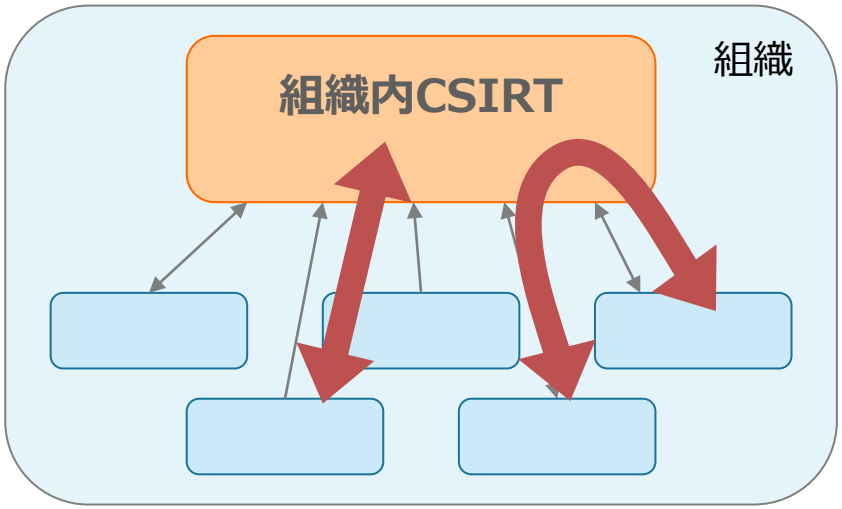
組織内 CSIRT によるインシデント対応活動



- あらかじめ定義されたサービス対象（Constituency）に関わるインシデントが発生した場合に、サービス対象からの期待および組織の状況にあわせた対応活動をする
- 対応活動の例としては、報告窓口の提供と告知、問題の切り分け、技術的支援、解決策の情報提供、被害の抑制策の実施、復旧に必要な支援などがある

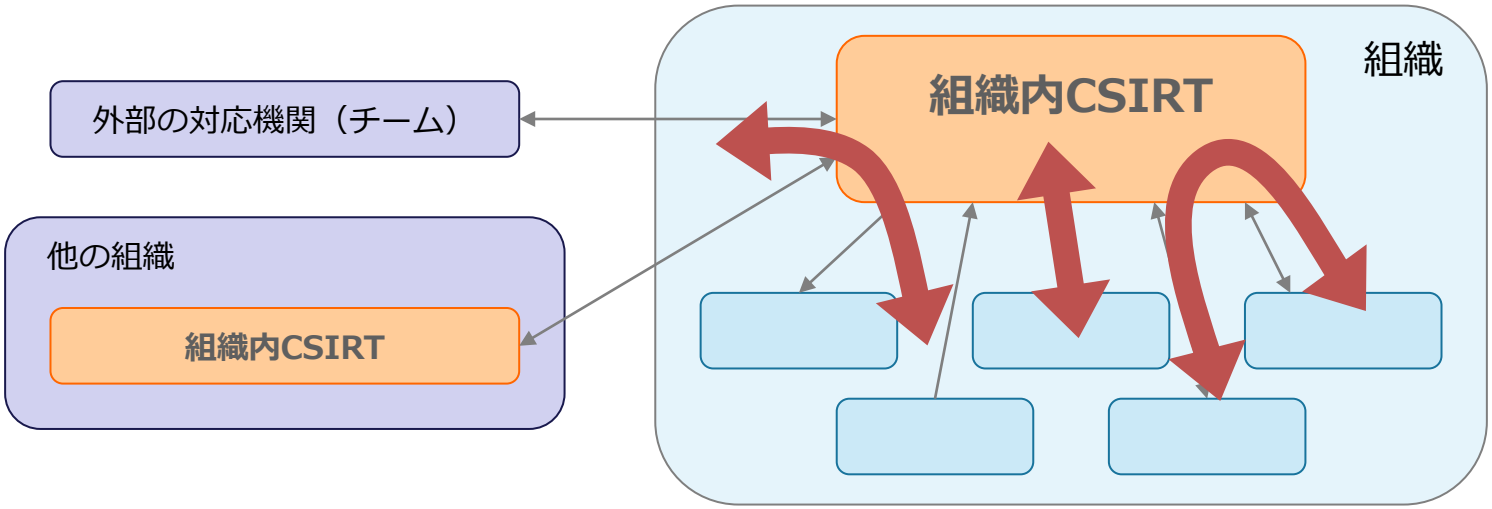
組織内 CSIRT の活動設定 1

- 組織内のみの活動に限定される場合：
  - サービス対象との良好な関係を構築する
    - 適切にインシデント報告がされるように、サービス対象に対して啓発をするとともに、インシデントの報告先、報告内容、そして手順などを周知する
    - 強制の有無にかかわらず、サービス対象からの協力が得られるような啓発をする
    - どの部門と連携できるのかを周知する
  - サービス対象における状況を把握する
    - 特にネットワークやホストに関する技術情報を把握する



組織内 CSIRT の活動設定 2

- 外部と関係をもつ（調整を含む）活動をする場合：
  - 外部に対する POC（Point of Contact：連絡窓口）を設ける
    - 外部に対して、連絡先（メールアドレスや電話番号など）をメールや Web 等で周知する
  - 外部との良好な関係を構築する
    - 外部とコミュニケーションをとり、何かできるのか等について相互理解する
  - 前ページ「組織内のみの活動に限定される場合」の活動内容すべて
    - （POC を通じて組織内に来る情報は、「組織に対して」来ることが多いため、サービス対象との良好な関係と状況の把握は必須）

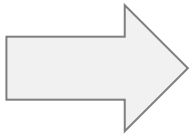


組織内 CSIRT の活動設定のポイント 1

- CSIRTに対し次のような「求められる役割」が示された場合

> 組織内において、発生したインシデントに対して、
> 適切な対応活動を実施し、速やかな復旧の支援をする。

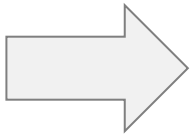
- 考察すべきポイント 1
  - この組織における「インシデント」の定義
    - これまで発生したインシデントを把握し傾向分析する
    - 同業他社で発生しているインシデントを把握し発生可能性を検討する
    - 経営層や現場の社員が認識しているインシデントを把握し傾向分析する
    - 予測されるインシデント発生場所を把握し傾向分析する
    - 可能であれば、インシデントの分類を検討する



「インシデント」が定義されることによって、組織内 CSIRT の活動の基本方針が決まる。極めて重要な定義である。

組織内 CSIRT の活動設定のポイント 2

- 考察すべきポイント 2
  - 「適切な対応」をする手段と、事前準備の定義
    - 発生したインシデントが適切に報告されるかどうかの確認
      - サービス対象者へのインシデント報告窓口と手順の周知徹底を事前に行う
    - 「サービス対象」と「組織の位置づけ」の定義を考慮し、何ができるのか／何ができないのかを把握し検討する
    - 組織内だけでは対応できないものを把握し検討する
      - 組織内だけでできない場合の外部との連携について、事前に検討する
    - 経営層やサービス対象が、どのような「適切な対応」を期待しているのか把握し検討する
    - インシデントが発生した際、「直ちに排除する」か「範囲を特定する」かの判断ができるように、組織のリスク許容度を評価する



「適切な対応」の活動リストと、それらを実現するため事前に準備しておかなければならない活動のリストが得られる。

（参考） 組織内 CSIRT の活動の分類について

- 組織内 CSIRT 活動は、以下のように分類できる
  - 事後対応型の活動
    - Reactive Service
    - 各インシデント報告や不正検知システムなどからの情報による活動
    - CSIRT の基本的な活動
  - 事前対応型の活動
    - Proactive Service
    - 事前にソフトウェアなどの脆弱性、脅威情報、攻撃予測情報などを提供する活動
    - 直接的にインシデント発生の抑制を図る
  - セキュリティ品質マネージメントに関する活動
    - セキュリティコンサルタント、教育など
    - 他のセキュリティ会社がすでに提供済みだが、CSIRT としての視点や専門知識での見識を提供できる。
    - 間接的にインシデント発生の抑制を図る

組織内 CSIRT の活動のフレームワーク

- 組織内 CSIRT の活動のフレームワークを整えるためには、以下の基本骨子を確実に定義しなければならない
  - ミッションステートメント
    - 大局的な目標、目的 – 何を果たすべきなのか
  - サービス対象（Constituency）
    - 誰のために活動するのか
    - サービス対象と、どのような関係なのか
    - サービス対象から、どのくらい認識されているのか
    - サービス対象との信頼関係
  - 組織内の 位置づけ
    - 組織内における CSIRT の位置
    - 組織内における CSIRT の役割
    - 各部署との相互関係
  - 他のチームとの関係
    - 他の CSIRT との協力及び連携

組織内 CSIRT の活動のフレームワーク
「ミッションステートメント」の定義方法

- 組織から求められる役割（インシデント対応など）を明確にする
- 組織の活動目的を補完するような組織内 CSIRT のミッションステートメントを作成する
- 組織内 CSIRT が所属する組織の経営層からの理解を得る

構築した組織内 CSIRT の役割、目的、活動を理解してもらうために、 をサービス対象者や他の CSIRT に対して、「ミッションステートメント」周知することが重要

組織内 CSIRT の活動のフレームワーク
「サービス対象」の定義方法

- 組織内 CSIRT がどの範囲を対象として活動するかを設定する
  - 「組織内 CSIRT が提供するサービスの対象範囲を設定する」と言い換えることができる
- 組織内 CSIRT がサービス対象に対してどの程度の権限を持つのか設定する
  - 強制的な権限があるのか、ないのか？
- サービス対象者に対して、組織内 CSIRT が何をするのかを周知する
  - インシデントの報告先として認知してもらう
- サービス対象者から信頼を得る
  - 信頼がなければ、インシデントは報告されない

組織内 CSIRT の活動のフレームワーク
「組織内の位置づけ」の定義方法

- 組織内 CSIRT が組織におけるリスク管理全体において求められている役割を明確にする
  - 主に、情報セキュリティ基盤に起因するリスクを管理する役割が多い
- 組織内に既に他のインシデント対応チームが存在している場合は、それぞれのミッションステートメント及びサービス対象の定義の区別を明確にする
- 組織における組織内 CSIRT の責任を明確にする

組織内 CSIRT の活動のフレームワーク
「他のチームとの関係」の定義方法

- 組織内 CSIRT が他の（外部の） CSIRT との調整及び連携するという役割を明確する

- 他の CSIRT が何ができ、どんな調整及び連携ができるのかを把握する
  - 逆に、自らが出来ることを、他の CSIRT に伝えることも重要である

- 他の CSIRT との連携に必要なことを定義する
  - 他の CSIRT に対する対応依頼は、自発的で非公式な場合が多いため、信頼関係の構築が必要となる

（参考）CERT/CC におけるサービスの分類の例

事後対応型サービス

・アラートと警告

・インシデントハンドリング
- インシデント分析
- オンサイトでのインシデント対応
- インシデント対応支援
- インシデント対応調整

・脆弱性ハンドリング
- 脆弱性分析
- 脆弱性対応
- 脆弱性対応調整

・アーティファクトハンドリング
- アーティファクト分析
- アーティファクト対応
- アーティファクト対応調整

事前対応型サービス

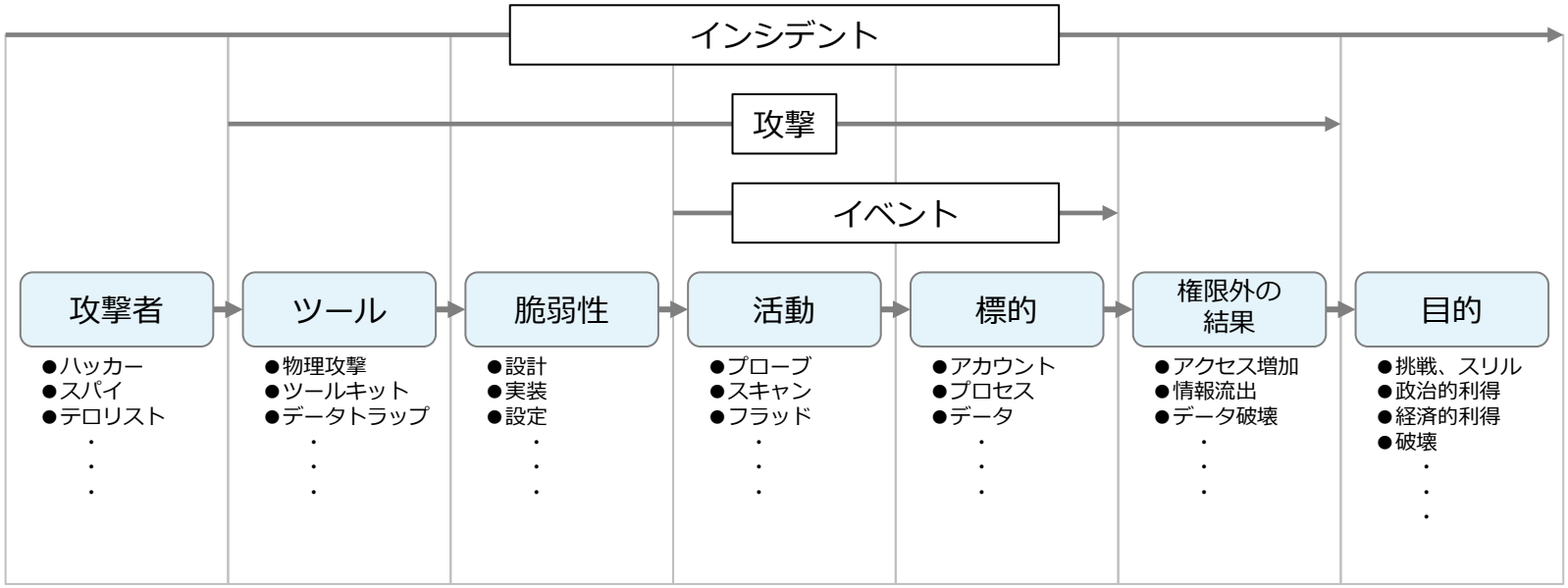
・告知
・技術動向監視
・セキュリティ監査または審査
・セキュリティツール、アプリケーション、インフラ、およびサービスの設定と保守
・セキュリティツールの開発
・侵入検知サービス
・セキュリティ関連情報の提供

セキュリティ品質管理サービス

・リスク分析
・ビジネス継続性と障害回復計画
・セキュリティコンサルティング
・意識向上
・教育 / トレーニング
・製品の評価または認定

（参考）「インシデント」「攻撃」「事象（イベント）」の定義の例

- 用語としての「インシデント」、「攻撃」、「事象（イベント）」の使い分けの例については、以下の報告書で記述されている。
  - 米国 Sandia National Laboratories の報告書
    “A Common Language for Computer Security Incidents”
    http://www.cert.org/research/taxonomy_988667.pdf



（参考）IT 部門との活動範囲の関係の例