

プロジェクト名: 〇〇〇CSIRT 構築プロジェクト

組織内 CSIRT 構築

CSIRT の基本的な枠組み

(バージョン 1.0 2021 年 X 月 X 日)

担当部署	作成者
〇〇〇部 〇〇課	〇〇 〇〇

	〇〇課	〇〇課	〇〇課	
審議欄				

承認者

CSIRT の基本的な枠組み

サービス対象者
<p>➤ ポイント</p> <ul style="list-style-type: none"> ◇ CSIRT は「誰のために」あるいは「どの範囲に対して」活動をするのか ◇ サービス対象者の定義と、その関係を明示する ◇ サービス対象者を定義しない場合、その理由を明確にする。例えば、顧客がサービス対象である場合は、顧客情報およびサービス提供の詳細な内容を秘密にする場合がある ◇ 定義したサービス対象者が、組織の他部門や他チームのサービス対象者と重複する場合があるが、その際は、それぞれの責任範囲や権限の違い、棲み分けについて明確にする
<p>(例)</p> <ul style="list-style-type: none"> ◇ 会社内および子会社の従業員および弊社インターネットサービスを契約している顧客
ミッションステートメント
<p>➤ ポイント</p> <ul style="list-style-type: none"> ◇ 上記で定義されたサービス対象者に対し何をするのかを記述する ◇ 組織のミッションに基づかなければならない、あるいは、その範囲内で解釈されるものでなければならない ◇ CSIRT の設立目的を併記することが多い
<p>(例)</p> <ul style="list-style-type: none"> ◇ 会社内および子会社の従業員に対し、コンピューターセキュリティインシデントによる被害が軽減されるための環境および仕組みの構築への支援をする。 ◇ 会社内および子会社の従業員に対し、インシデントが発生した場合の対応の支援をする。 ◇ インターネットサービスを契約している顧客が、弊社インターネットサービスを起因とするインシデントに巻き込まれた場合、その被害の軽減と、迅速な復旧をする。
提供するサービス
<p>➤ ポイント</p> <ul style="list-style-type: none"> ◇ 上記で定義されたサービス対象に対する直接のインシデント対応、あるいは、インシデント対応を実施する組織や部署に対する支援活動が、最低限必要である。 ◇ サービス分類の3つのカテゴリ（「事後対応型サービス」「事後対応型サービス」「セキュリティ品質管理サービス」）を参考にして記述する。 ◇ サービス対象者のニーズ、親組織の経営層からの期待が強く影響する。
<p>(例)</p> <ul style="list-style-type: none"> ◇ インシデント対応 ◇ インシデント対応の支援 ◇ インシデント対応の他の組織および部署との調整 ◇ 社内および顧客向けのシステムに関する脆弱性のハンドリング ◇ 技術動向の監視と社内へ適切な部署への展開

組織内の位置づけ
<p>➤ ポイント</p> <ul style="list-style-type: none"> ◇ 一部の特定インシデントへの対応能力をもった部署やチームが別に存在する場合、CSIRT との棲み分けが必要になる ◇ どの範囲に対して活動をするのか(サービス対象者)と、何のために活動するのか(ミッションステートメント)、どのような活動をするのか(提供するサービス)に基づいて、最適な組織内の位置づけを確定する。
<p>(例)</p> <ul style="list-style-type: none"> ◇ 経営層直下の情報セキュリティ室内に設置し、将来的に、独立した部署の設立を検討する。 ◇ サービス対象との関係については、サービス毎に異なり、別途定義をする。
必要なリソース
<p>➤ ポイント</p> <ul style="list-style-type: none"> ◇ サービスの提供を実現するために必要なスタッフ/設備/インフラ等を見積もる。 ◇ これらのリソースは、CSIRT のサービス品質に大きく影響する。
<p>(例)</p> <ul style="list-style-type: none"> ◇ CSIRT に所属するメンバーは、IT 部門を1年以上経験し、会社が認めたセキュリティ関連資格を取得あるいは情セ室長がその能力を有すると認めたものとする。(最初は、常勤2名、他の部署との兼務3名とする。) ◇ CSIRT の活動に必要な設備については、情セ室のものを活用するが、専用のファイル共有サーバーやメールサーバーを別途用意する。 ◇ ネットワークについては、情セ室のものを活用する。ただし、子会社に所属するCSIRT メンバーについては、別途、専用のVPNを用意し、本社のCSIRT 専用のファイル共有サーバーを別途用意する。
運営予算
<p>➤ ポイント</p> <ul style="list-style-type: none"> ◇ CSIRT を構築する際、既存の設備の活用だけでは難しい場合、どのくらいの追加コストが必要か? ◇ CSIRT の運用にはどのくらいの維持費が必要か?(設備の維持管理、他の組織やコミュニティとの継続的なコミュニケーションの維持、CSIRT スタッフの教育・訓練にかかる費用等)
<p>(例)</p> <ul style="list-style-type: none"> ◇ 必要なリソースから、以下のものを購入および設置するための費用が必要。 <ul style="list-style-type: none"> ● CSIRT 専用のメールサーバー、ファイル共有サーバー ● 子会社とのVPNを張るための器材 <ul style="list-style-type: none"> ➤ 常勤者CSIRT メンバーの業務に必要なノートPC、ネットワーク回線、デスクおよびその椅子、打ち合わせ用テーブルおよびその椅子、ホワイトボード、プロジェクターおよびそれらに必要な消耗品 ➤ 計〇〇〇〇円(見込み) ● 各カンファレンスおよびコミュニティ参加のための費用 <ul style="list-style-type: none"> ➤ 計〇〇〇〇円(見込み)