JPCERT Coordination Center

JPCERT CC®

CSIRTマテリアル 構築フェーズ 「組織内CSIRT構築の実践」

一般社団法人
JPCERTコーディネーションセンター

本資料について

- 本資料は、CSIRTの構築のプロセスと作業項目の概要について簡潔に説明する資料として作成したものです。CSIRT構築を任された担当者が構築プロセスを理解し実作業を進める際の参考として頂くことを意図しています。
- 「CSIRTマテリアル」内の他の文書とあわせてご利用ください。
  - 構築フェーズ：「組織内CSIRTの理解」
    「組織内 CSIRT の実作業　フォームと作成例」
  - 運用フェーズ：「CSIRTガイド」「インシデントハンドリングマニュアル」

目次

1. 組織内CSIRTの構築プロセス
- 1-1. 経営層から理解を得る
- 1-2. 組織内の現状を把握する
- 1-3. 組織内CSIRT構築チームを結成する
- 1-4. 組織内CSIRTの設計と計画
- 1-5. 予算とリソースを獲得する
- 1-7. 組織内CSIRT関連規則類を整備する
- 1-8. CSIRT要員（スタッフ）への教育
- 1-9. CSIRTの告知と活動の開始

2. 組織内CSIRT構築の実作業
- 2-1. CSIRT構築の流れについて
- 2-2. キックオフ、スケジューリング
- 2-3. ゴールの設定とタスクの細分化
- 2-4. CSIRT関連知識・ノウハウ等の勉強会
- 2-5. 組織内の現状把握
- 2-6. 組織内CSIRTの設計
- 2-7. 組織内CSIRT設置に必要な準備
- 2-8. 組織内CSIRTの設置
- 2-9. 組織内CSIRT運用の訓練

１．組織内CSIRTの構築プロセス

1-1. 経営層から理解を得る

- 経営層に組織内CSIRTの必要性を理解させ、組織内CSIRT構築プロジェクトを開始することの承認を得る
  - 経営層向けにCSIRTを説明するための資料の作成
    - 十分な情報収集と分析に基づいて文書をまとめる
      - CSIRTのコンセプト
      - CSIRTの必要性とメリット、既存の組織内機能との違い
      - CSIRTがないことによる問題点
      - CSIRTの設置と運用に必要なコスト　など
  - 組織内CSIRTの必要性を理解する同僚や上司を増やして外堀を埋める

1-2. 組織内の現状を把握する

- 業務を把握する
  - 各部署の業務フロー
  - 部署間の情報共有と連携
  - 各部署の責任者やキーパーソン
- 責任者やキーパーソンへのヒアリングを行う
  - 各部署のインシデント対応の責任者
  - 関連する知見を持つ有識者
    - 過去のインシデント対応に関与したことのある人
    - 情報セキュリティに明るい人
    - 業務システムの運用と維持管理に明るい人
  - 情報セキュリティに関する業務の職責を持つ人
- インシデント対応に関係する規則類の把握する
  - インシデント対応に関係する条項を洗い出す

1-3. 組織内CSIRT構築チームを結成する

- 組織内の現状把握の結果から
  - インシデント対応のスキルと能力のある人を特定する
  - 組織内CSIRTの要員の候補者を洗い出す
- 組織内CSIRT構築チームメンバーを選定しチームを結成する
  - インシデント対応が可能な人
  - 情報セキュリティや業務システムに明るい人
  - 情報セキュリティに関する職責を持つ人
  - 組織内の業務に詳しい人、経験豊富な人
- 活動を推進する責任を持つリーダーを指定する
  - 推進者がいなければ、構築活動は停滞する

1-4. 組織内CSIRTの設計と計画

- 以下の項目を検討し決定する
  - 活動の対象（サービス対象）
  - 責任と使命
  - 活動内容とそのレベル
    - サービス対象に提供するサービス
  - 組織における位置づけ
    - インシデント報告の窓口、各部署との調整役など
    - サービス対象に対する権限
  - サービス対象の中で特に重要なポイント
    - インシデントが発生しやすい部署、重要な情報資産を扱う部署など
- これらの情報を文書化する
  - これから構築する組織内CSIRTの基礎となる

1-5. 予算とリソースを獲得する

- 組織内CSIRTの設立・運営に必要な予算を獲得
- 組織内CSIRTに必要な要員の確保
  - 構築プロジェクトチームのメンバーがそのまま要員となることが多い
- 組織内CSIRTの運営に必要な設備等の準備
  - 専用のセキュアなネットワークとサーバー
  - 日常業務用のPC、分析・検証・開発用の機材等
  - 他部署と分離された専用のオフィススペース、会議室など
  - 専用のメールアドレス（チームアドレス）
  - その他

1-6. 組織内CSIRT関連規則類を整備する

- 活動に関連する規則類を整備する
  - ポリシー
    - インシデント対応に関するポリシー
    - 情報セキュリティに関するポリシー
    - その他、業務活動に必要なポリシー
  - 手順
    - インシデント対応に関する手順
    - 情報セキュリティ活動に関する手順
    - その他、業務活動に必要な手順

1-7. CSIRT要員（スタッフ）の教育

- CSIRT要員（スタッフ）の教育
  - ポリシーおよび手順
  - 情報セキュリティ全般に関する知識
  - その他、業務に必要な知識

- インシデント対応のための訓練と演習
  - 模擬のインシデントによる対応訓練
    - CSIRTの業務や、インシデント発生時の組織全体の対応プロセスの評価
    - 習熟度を把握
    - 不足している能力・スキルの強化

1-8. CSIRTの告知と活動の開始

- CSIRTの設置について告知する
  - サービス対象、情報共有・連携する関連部署と外部組織に向けて発信する
  - ミッションステートメント、活動内容（提供するサービス）、報告先の窓口と報告手段などについて告知する
- フィードバックを得る
  - 告知した相手からの反応や意見を収集する
  - インシデント対応を実施した相手からのフィードバックを得る
- 得られたフィードバックをもとに活動を改善する
  - フレームワーク、ポリシー・手順、活動内容などの見直しを継続して実施する

参考資料

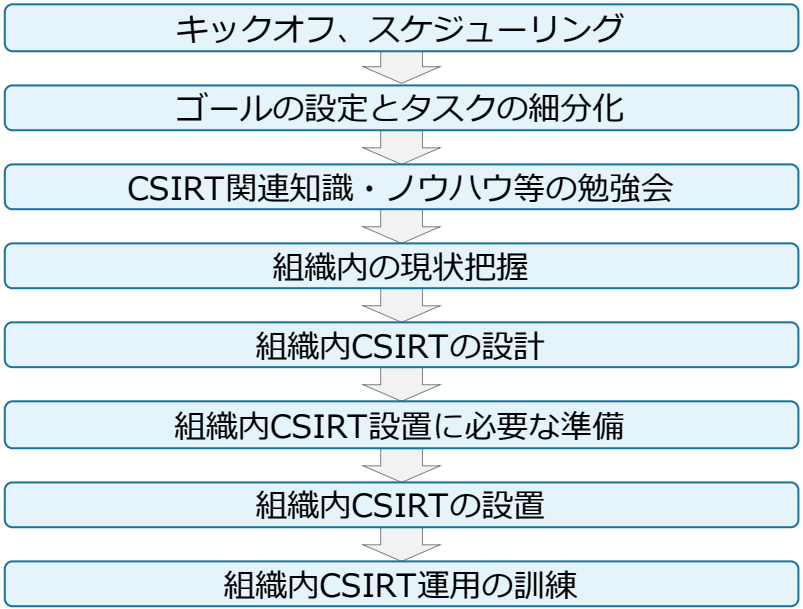
- 日本シーサート協議会「CSIRTスターターキット」
  https://www.nca.gr.jp/imgs/CSIRTstarterkit.pdf

  CSIRTを構築する際に注意し取り組むべき課題や定義すべき事項、および、組織におけるインシデントレスポンスの計画を構築する際に取るべき手順について説明している文書

2．組織内CSIRT構築の実作業

2-1. CSIRT構築の流れについて

- 組織内CSIRTの構築作業は以下のような手順で進めることが望ましいが、組織の状況に応じて手順の一部省略や順序の変更をしてもよい



2-2. キックオフ、スケジューリング

- 目的
  - 組織内CSIRTの構築活動を開始する
- 内容
  - 構築プロジェクトメンバーの選定
  - プロジェクトメンバーの意識合わせ
    - 構築活動の目的とスコープ、構築活動におけるポリシーと制約事項
  - プロジェクト体制と活動内容の説明
  - プロジェクトの進め方に関する検討
    - ゴール設定、作業プロセス、打ち合わせの頻度など
- 工数（期間）
  - 構築プロセス全体の事前準備に5～10時間程度（2～3日程度）
  - キックオフ会議に1～2時間（1日程度）
- スタイル
  - プロジェクト開始のための関連文書を作成し、メンバーを招集してキックオフ会議を開催する
- 成果物
  - CSIRT構築活動のためのプロジェクト憲章
    （参考：「構築活動のためのプロジェクト憲章」URL表示）

2-3. ゴールの設定とタスクの細分化

- 目的
  - 組織内CSIRT構築のための活動範囲を明確化する
- 内容
  - 外部の組織内CSIRT構築経験者などのアドバイスを参考にしながら、以下の項目を決定する
    - 目的と目標の設定
    - マイルストーンの設定
    - 構築活動に必要な作業の洗い出し
    - 作業範囲の定義
    - 作業計画の概要作成
- 工数（期間）
  - 打ち合わせに2～3時間程度（1日程度）＋事後作業1～2時間程度（1日程度）
- スタイル
  - プロジェクトメンバー＋外部の助言者との打ち合わせを行い、文書化する
- 成果物
  - CSIRT構築活動のためのスコープ記述書
    （参考：「構築活動のためのスコープ記述書」URL表示）

2-4. CSIRT関連知識・ノウハウの勉強会

- 目的
  - 組織内CSIRTスタッフ候補者に対するCSIRTに関する理解の促進
- 内容
  - CSIRTの歴史
  - CSIRTの基本的な枠組み
    - CSIRTのサービス対象
    - CSIRTのミッションステートメント
    - CSIRTが提供するサービス（活動内容）
    - 組織内でのCSIRTの位置づけと外部組織との連携
  - CSIRTの運用、業務手順
  - 他のCSIRTの事例紹介　など
- 工数（期間）
  - 事前準備に5～10時間程度（2～3日程度）＋　勉強会に2～3時間（1日程度）
- スタイル
  - 資料を作成し、勉強会を実施する
- 成果物
  - CSIRTに関する資料

2-5. 組織内の現状把握

- 目的
  - 組織内CSIRTの設立と活動に必要な情報の収集と整理
- 内容
  - 過去に組織内で発生したインシデントの対応履歴と問題点
    - 現状のインシデント対応の流れと、意思決定要素の分析
  - 各部署のインシデント対応の実態調査
  - インシデント対応に必要な組織内連携
  - 組織の規則類における、インシデント対応に関係する記述の調査と分析
  - インシデント対応に関する経営層からの期待
  - インシデント対応に関するサービス対象（従業員等）からの要望の収集
  - リスクアセスメントおよびリスク許容度の評価の実施
- 工数
  - ヒアリングに10～20時間程度（6～9日程度）＋まとめに6～9時間程度（2～3日程度）
- スタイル
  - 関係部署にヒアリングし、文書化する
- 成果物
  - 構築に必要な現状把握

    （参考：CSIRTマテリアル 構築フェーズ「構築に必要な現状把握」）

2-6. 組織内CSIRTの設計

- 目的
  - 組織内CSIRTの基本的な枠組みと活動手順の設計
- 内容
  - 基礎的なCSIRTの枠組みの作成
    - ミッションステートメント
    - サービス対象
    - 組織における位置づけ
    - 他の部署／組織との連携
  - CSIRTの運用に必要な情報の作成
  - インシデント対応のためのポリシーおよび手順（マニュアル）の作成
- 工数
  - 打ち合わせに2～3時間程度（1日） ＋ まとめに4～5時間程度（1日）
- スタイル
  - 関係者との打ち合わせを行い、文書化する
- 成果物
  - CSIRTの基本的な枠組み（参考：CSIRTマテリアル 構築フェーズ「CSIRTの基本的な枠組み」）
  - CSIRT記述書（参考： CSIRTマテリアル 構築フェーズ「CSIRT 記述書」）
  - インシデント対応ポリシーおよび対応マニュアル

2-7. 組織内CSIRT設置の準備

- 目的
  - 経営層の理解の獲得
  - 関係部署との調整に必要な情報源の整理
- 内容
  - 経営層の承認を得る
  - 組織内CSIRT設置や活動継続のための予算の獲得
  - 組織内CSIRTに必要な設備等の準備
  - 組織内CSIRTの要員の確保
  - 組織内CSIRTメンバーの役割と責任の定義
  - その他、組織内CSIRTの設置に必要な準備のための活動
- 工数
  - 準備にかかる調整に1～2カ月間程度＋打ち合わせに4～5時間程度（2～3日）
- スタイル
  - 関係部署や関係者と打ち合わせを行い、文書化する
- 成果物
  - 組織内CSIRTの設置に必要な文書（稟議書、見積書等）

2-8. 組織内CSIRTの設置

- 目的
  - CSIRTの設置、活動の開始
- 内容
  - 組織内外への組織内CSIRTの設置に関する告知
  - 組織内の関係部署との連携と共通認識の確保
  - CSIRTの試行運用
  - 他組織のCSIRTとの連携や適切なコミュニティー等への参加
- 工数
  - 準備に２～３週間程度
- スタイル
  - 関係部署やサービス対象への連絡および関係者との打ち合わせ等
- 成果物
  - 「組織内CSIRT」を経営層やサービス対象者に対して説明するための資料

2-9. 組織内CSIRT運用の訓練・演習

- 目的
  - インシデント発生時の対応に関する、CSIRTおよび関連部署を含む、要員の理解度と対応能力の検証
  - セキュリティ基本方針・インシデント対応計画の実効性の検証
- 内容
  - 演習の準備
    - 演習の目的、スコープ、目標値、評価方法を定める
    - 演習のタイプ、実施スケジュールを決定する
    - 関連するすべての部門へ演習への参加を要請
    - 演習シナリオ作成、演習のファシリテーションとロジスティクスの準備
  - 演習後の対応
    - 評価結果を収集し、実施報告書を作成する
    - セキュリティ基本方針・インシデント対応計画における改善点を特定する
- 工数
  - 訓練・演習のタイプ、規模、内容等により大きく変動する。数週間から数カ月程度。
- 成果物
  - 演習企画書、演習実施手順書、演習実施報告書、改善検討結果報告書
    （参考： CSIRTマテリアル構築フェーズ「CSIRTマテリアル付録　インシデント対応演習プログラム」）

組織のリスク許容度の評価

組織の特徴

- 組織の規模
- 組織の複雑さ
- 保有する知的財産の価値
- ITへの依存度
- システムダウンが与える影響
- システムエラーが与える影響
- 組織的な変化の度合い
- 多国籍企業かどうか
- 利害関係者/株主の期待の度合い
- 規制のレベル
- 評判への依存度
- 外部委託の依存度
- 事業所の地域的な不安定さ

リスク判断

- セキュリティ防衛能力
- 守るべき製品/サービス
- 資産を防御する理由
- 潜在的なリスク
  - リスクの対処に必要なコスト
  - リスクによる減損の許容範囲
  - 対処後の残存リスク

取り組み方法

- 組織の管理策の有効性/生産性を把握
- 組織の対外的な評価を維持/向上
- 企業の回復力を維持
- 内外を問わず悪意ある攻撃から防御
- 例外条件を極少化したアクセスコントロールリストを作成
- ISO/IEC27001におけるセキュリティ管理策に準じて行動
- 予防的なログを保持
  - DNSログ
  - プロキシログ
  - ファイアウォールログ
  - NetFlowログ
  - サーバーログ
  - ホストログ