JPCERT CC®

組織内 CSIRT の構築プロセス

一般社団法人
JPCERT コーディネーションセンター

目次

1. 経営層から理解を得る
2. 組織内の現状把握
3. 組織内 CSIRT 構築活動のためのチーム結成
4. 組織内 CSIRT の設計と計画
5. 必要な予算やリソースの獲得
6. 組織内 CSIRT 関連規則類の整備
7. CSIRT 要員（スタッフ）への教育
8. CSIRT の告知と活動開始

（参考） 組織内 CSIRT に関して検討すべき事項一覧

1. 経営層から理解を得る

- 経営層が CSIRT を理解していない場合は、CSIRT に関する説明資料の作成が必要になる

- 最初に経営層からの理解を得るのが難しい場合には、十分な情報収集および検討した結果をまとめた文書にして伺いを立てる

- まずは、CSIRT の必要性を理解する同僚と上司を増やしていくことが重要である

2. 組織内の現状把握

- 組織内における業務の把握
  - 各部署の業務フロー
  - 部署間の情報共有及び連携の状況
  - 各部署の責任者及びキーパーソン
- 主要な人物に対するヒアリングの実施
  - 各部署のインシデント対応の責任者
  - インシデント対応時に関わったことのある人
    - 情報セキュリティに明るい人
    - 業務システムの運用及び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
  - インシデント対応に関係する項目や文言の列挙

3. 組織内 CSIRT 構築活動のためのチーム結成

- 組織内の現状把握により
  - インシデント対応のスキルと能力のある人を見出すことができる
  - 組織内 CSIRT に必要な要員の候補者を見出すことができる
- 組織内 CSIRT 構築の活動をする人を選定しチームとして結成する
  - 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、経験の豊富な人
- 必ず活動を推進する選任を持つリーダーを指定する
  - 推進していく人が不在だと、構築活動は停滞する

4. 組織内 CSIRT の設計と計画

- 活動チームにおいて「組織内 CSIRT」に関する以下の項目を検討し、決定する
  - 活動の対象（サービス対象）（Constituency）
  - 責任と使命
  - 活動内容とそのレベル
    - 活動の対象に対して、提供するサービス
  - 組織内における位置づけ
    - インシデント報告の窓口、各部署との調整役などのための位置づけ
    - 活動の対象に対する権限
  - サービス対象の中で、他に重要なポイント
    - お客様窓口、インシデントが発生しやすい部署など
  - サービス対象に対する責任と権限
- 以上の情報を文書で記述する
  - 基礎的な組織内 CSIRT の枠組みとなる

5. 必要な予算やリソースの獲得

- 組織内 CSIRT の設立・運営に必要な予算の獲得
- 組織内 CSIRT に必要な要員の確保
  - 構築活動のチームのメンバが、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
  - 個人の PC
  - 専用のセキュアなネットワークとサーバ
  - デスク及び椅子
  - 専用のメールアドレス（チームアドレス）
  - SIEM
  - その他

6. 組織内 CSIRT 関連規則類の整備

- 以下の規則類の整備が必要
  - 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

7. CSIRT 要員（スタッフ）への教育

- CSIRT 要員（スタッフ）の以下の項目に関する教育
  - 各ポリシー及び手順
  - 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事前訓練
  - 模擬のインシデントによる対応訓練
    - 業務に関するプロセスの評価
    - 習熟度を把握
    - 不足している能力・スキルの再教育

8. CSIRT の告知と活動開始

- CSIRT に関する告知を実施する
  - サービス対象
  - 情報共有及び連携活動をする関連部署及び外部組織
  - 告知内容は、ミッションステートメントと活動内容（提供するサービス内容）、報告の手段など
- フィードバックを得る
  - 告知をしたところからの反応や意見
  - インシデント対応を実施したところからフィードバック
- 得られたフィードバックをもとに活動を改善する
  - ＰＤＣＡサイクルを活用し、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） 組織内 CSIRT に関して検討すべき事項一覧

- サービス対象者は？
- 経営層及びサービス対象者の期待は？（何が必要か？）
- 保護すべき重要な資産は何か？
- 情報セキュリティに関する既存の問題は？
- どのような種類のインシデントが報告されるか？
- どのような種類の調整と対応が求められているか？
- どのような能力やスキルが必要か？
- どのようなプロセスが必要か？
- エスカレーションする先はどこか？
- どのような人が関わるか？
- どのようなコンプライアンス、組織の事業、組織文化があるか？
- 誰が担当すべきか？他に担当できる人がいるか？
- 外部との連絡調整、情報共有、連携活動の必要性はあるか？
- 組織のリスク許容度はどうなっているか？
- その他