JPCERT CC®

組織内 CSIRT 構築の実作業

一般社団法人
JPCERT コーディネーションセンター

概要

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

（参考）リスク許容度の評価

CSIRT 構築の流れについて

- 組織内に CSIRT を構築する場合は、以下のようなプロセスで構築することが望ましいが、組織の事業内容により、省略できるプロセスや順序が異なる場合がある

1. キックオフ・スケジューリング

- 目的
  - 組織内 CSIRT 構築活動の開始
- 内容
  - 構築プロセス全体の事前準備
    - 組織内 CSIRT 構築担当者の選定
  - 組織内 CSIRT 構築の担当者及び関係者の顔合わせと意識合わせ
    - 本構築活動の目的、位置づけの共有
    - 構築活動にかかるポリシー及び制約事項
  - プロジェクト体制の説明
  - プロジェクト活動内容の説明
  - プロジェクトの進め方に関する検討
    - 詳細なゴール設定
    - プロセス
    - 打ち合わせの頻度
- 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）＋打ち合わせに１～２時間（１日程度）
- スタイル
  - 担当者による文書作成後、関係者との打ち合わせ
- 成果物
  - CSIRT 構築活動のためのプロジェクト憲章（A4 縦型文書１ページ程度）

2. 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の明確化
- 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
    - 具体的な目的と目標の設定
    - 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
  - 関係者との打ち合わせ後、担当者による文書作成
- 成果物
  - CSIRT 構築活動のためのスコープ記述書（A4 縦型文書１ページ程度）

3. 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 に関する歴史
  - CSIRT の基本的な枠組み
    - CSIRT のサービス対象者
    - 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）
    - CSIRT の組織内の位置づけと外部組織との連携
  - CSIRT の運用について（業務プロシージャについて）
  - 他の CSIRT の事例と現状の紹介
  - その他、CSIRT にかかるさまざまな情報の共有
- 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
  - 担当者のプレゼン資料作成後、関係者間の勉強会や議論の実施
- 成果物
  - CSIRT に関する資料（マテリアル）

4. 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に関する対応履歴と問題点
    - 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
  - 組織内におけるインシデント対応に必要な連携
  - 組織内の規則類の中のインシデント対応に関係する記述の調査と分析
  - 組織内のインシデント対応に関する経営層からの期待
  - 組織内におけるインシデント対応に関するサービス対象（従業員等）からの要望の取りまとめ
  - リスクアセスメント及びリスク許容度の評価の実施（スライド12を参照）
- 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
  - 担当者による関係部署に対するヒアリング後、担当者による文書作成
- 成果物
  - 構築に必要な現状把握（Ａ４縦型文書１３ページ程度）

5. 組織内 CSIRT の設計

- 目的
  - インシデント対応に必要な、基本的な枠組みと CSIRT の活動の流れの設計
- 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
    - 組織内の位置づけ
    - 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及び手順（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後、担当者による文書作成
- 成果物
  - CSIRT の基本的な枠組み（A4 縦型文書３ページ程度）
  - CSIRT 記述書（A4 縦型文書８ページ程度）
  - インシデント対応のポリシー及びマニュアルの文書

6. 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 のメンバ要員の確保
  - 組織内 CSIRT メンバ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ヶ月間程度＋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の打ち合わせ後、担当者による文書作成
- 成果物
  - 組織内 CSIRT の設置に必要な文書（稟議書、各見積書等）

7. 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及び関係者との打ち合わせ等
- 成果物
  - 「組織内 CSIRT 構築」を経営層やサービス対象者に対して説明するための概要資料（A4 縦文書３～４ページ程度）

8. 組織内 CSIRT 運用の訓練

- 目的
  - CSIRT 運用訓練の企画と実施
  - セキュリティ基本方針・インシデント対応計画の検証
- 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
    - 演習の参加者、役割、責任、権限の明確化
    - 実施スケジュールの決定
    - 事前告知するかを決定
    - 結果をAPTに対する能力評価とするか
    - 関連する全部門を演習に関与させるよう企画
    - 組織内外へ情報共有できるかの検証
  - 演習後の対応
    - 実施報告書の作成
    - セキュリティ基本方針・インシデント対応計画改善の検討
- 工数
  - 訓練・演習のタイプ、規模、実施内容等により大きく変動する。数週間から数か月程度。
- 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）組織のリスク許容度の評価と管理策の実装

APTなどの高度なサイバー攻撃に対応していくために、組織のプロファイル、攻撃がもたらすビジネスインパクト、リスクを緩和するための管理策の実装状況について、現状分析と整理をおこない、組織がどこまでのリスクを許容できるかを把握しておく。

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
  - サーバログ
  - ホストログ