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　　2015 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

- *ポイント*
  - *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、顧客情報及びサービス提供の詳細な内容を秘密にする場合がある*
  - *サービス対象者が、他の組織によるサービス対象者と重複する場合があるが、その際は、サービス対象者に対する権限の違いを明確にする*

(例)
- 会社内及び子会社の従業員及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

- *ポイント*
  - *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*
  - *親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*

(例)
- 会社内及び子会社の従業員に対し、コンピュータ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及び仕組みの構築への支援をする。
- 会社内及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

- *ポイント*
  - *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。*

(例)
- 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及び部署との調整
- 社内及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

- *ポイント*
  - *一部のインシデントへの対応能力をもった部署が存在する場合、CSIRT との切り分けが必要になる*
  - *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。*

(例)

- 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、各サービス毎に異なり、別途定義をする。

必要なリソース

- *ポイント*
  - *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。*

(例)

- CSIRT に所属するメンバは、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或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やメールサーバを別途用意する。
- 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を別途用意する。

運営予算

- *ポイント*
  - *CSIRT を構築する際、既存の設備の活用だけでは実現が難しい場合、どのくらいの追加コストが必要か？*
  - *CSIRT の活動継続には、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コミュニケーション継続のためにかかる費用等）*

(例)

- 必要なリソースから、以下のものを購入及び設置するための費用が必要。
  - CSIRT 専用のメールサーバ、ファイル共有サーバ
  - 子会社との VPN を張るための器材
    - 常勤者 CSIRT メンバの業務に必要なノート PC、ネットワーク回線、デスク及びその椅子、打ち合わせ用テーブル及びその椅子、ホワイトボード、プロジェクター及びそれらに必要な消耗品
    - 計〇〇〇〇円（見込み）
  - 各カンファレンス及びコミュニティ参加のための費用
    - 計〇〇〇〇円（見込み）