プロジェクト名：

組織内CSIRT構築

CSIRTの基本的な枠組み

（バージョン 　　　　年　　月　　　日）

|  |  |
| --- | --- |
| 担当部署 | 作成者 |
|  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 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、CSIRTとの関係を明示する*     - *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* |
|  |
| **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*     - *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* |
|  |
| **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つのカテゴリー（「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、組織の経営層からの期待が強く影響する。* |
|  |

|  |
| --- |
| **組織内の位置づけ** |
| * + *ポイント*     - *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。* |
|  |
| **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。* |
|  |
| **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）* |
|  |