プロジェクト名：

\_Label\_Keyword\_公開情報\_Keyword\_\_Label\_Keyword\_社外向け文書\_Keyword\_\_Label\_Keyword\_個人情報を含まない\_Keyword\_

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、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
 |
|  |
| **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
 |
|  |
| **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。
 |
|  |

|  |
| --- |
| **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。
 |
|  |
| **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）
 |
|  |