プロジェクト名：

組織内CSIRT構築

構築に必要な現状把握

（バージョン 　　　　年　　月　　　日）

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 審議欄 |  |  |  |  |  | 承認者 |
|  |  |  |  |  |

現状把握のためのヒアリングシート

**目的：**

組織が必要とするインシデント対応およびサービスを決定するための情報を収集する

|  |
| --- |
| **既存のインシデントに関する検討** |
| ***ポイント****：**これまでにサービス対象者から報告されたインシデントを分析し、組織内のインシデントを定義する。これによりCSIRTが提供するサービスの種類をすぐに決めることはできないが、CSIRTスタッフが必要とするスキルや専門的知識の種類を決めることはできる。* |
| *アドバイス：**例えば、もし組織がマルウェア感染の被害を受けた場合、マルウェア感染への対応経験を持つスタッフが必要となります。また、適切なツールを活用して、感染を検知し、除去し、復旧するための手順も必要になります。感染を防止するための事前準備としてユーザーへの啓発を行うために、CSIRTスタッフにはトレーニング企画と文書作成の能力が必要となります。* |

|  |
| --- |
| **インシデントハンドリングに必要な情報の所在に関する検討****（利害関係者からのインタビュー／ディスカッションによるアプローチ）** |
| ***ポイント****：**CSIRTを計画し実装するために必要な情報を、組織内のステークホルダーから引き出す。各ステークホルダーとの個別のインタビューやディスカッションにより、誰が何の情報を持っているのかを認識し、その情報を最大限に引き出すことを図る。* |
| **1. 経営層** |
| * + *ポイント*
		- *経営層はCSIRTとは何かを理解しているか*
		- *経営層はCSIRTがどのようにビジネスプロセス支援に役立つかを理解しているか*
		- *基幹システムの停止やネットワークの遮断をするような場合に誰が意思決定をするのか、また、CSIRTにどこまで権限を持たせることができるか*
 |
|  |
| **2. IT 部門** |
| * + *ポイント*
		- *IT部門のスタッフとCSIRTとの関係を確認する*
		- *インシデント対応における IT部門スタッフとCSIRTスタッフのアクションを確認する*
		- *CSIRTが分析の目的のために（IT部門が管理する）ログを閲覧することの同意と、手順・環境を確認する*
 |
|  |

|  |
| --- |
| **3. 法務部門** |
| * + *ポイント*
		- *インシデント対応活動に対する法務部門の関わり方を確認する*
		- *インシデント対応に係る他組織との機密保持契約やその他の契約行為に関する支援*
		- *コンピューターセキュリティインシデントに関する法的責任の検討の支援*
 |
|  |
| **4. 人事部門** |
| * + *ポイント*
		- *CSIRTスタッフを雇用するための職務内容の記述*
		- *許可のないアクセスや違法行為に対する懲罰等に係るポリシーや手続きを作成*
 |
|  |
| **5. 広報部門** |
| * + *ポイント*
		- *メディアからの質問への対応*
		- *情報公開ポリシーの作成と業務手順の構築*
 |
|  |

|  |
| --- |
| **6. 物理セキュリティを担当する部門** |
| * + *ポイント*
		- *責任範囲が明確になっているかを確認する*
 |
|  |
| **7. 既存のセキュリティチーム** |
| * + *ポイント*
		- *コンピューターセキュリティインシデントへの対応について、どのようなノウハウを持っているかを確認する*
 |
|  |
| **8. 監査部門およびリスクマネージメントの専門家** |
| * + *ポイント*
		- *脅威分析や脆弱性評価についての支援が期待される*
		- *サービス対象者または組織全体に対して、コンピューターセキュリティにかかる最善策の推進に関する支援*
 |
|  |

|  |
| --- |
| **9. サービス対象の代表者** |
| * + *ポイント*
		- *サービス対象におけるニーズや要求事項を確認する*
 |
|  |
| **10. 外部（組織外およびサービス対象外）の利害関係者** |
| * + *ポイント*
		- *インシデントハンドリングのプロセスにどのような立場で関与するか*
		- *過去のインシデント経験より、(外部の）誰に通知すべきであったか*
		- *CSIRTに対して通知をする人はいるか*
		- *CSIRTと情報を共有する人はいるか*
		- *外部ベンダー等（脆弱性評価、侵入検知、ネットワーク監視など）は含まれるか*
 |
| *アドバイス：**「CSIRTのすべき事」を理解すると、手順の作成に関わるべき人を見出すことに役立ちます。* |
| **11. その他の利害関係者** |
| * + *ポイント*
		- *CSIRTが提供するサービスをすでに提供している部署を見つける*
		- *そのサービスをその部署でそのまま継続すべきなのか、あるいはCSIRTに委譲すべきなのかを決める*
 |
| *アドバイス：**計画段階でこの検討をしておくと、CSIRTの責任範囲の大枠や必要な情報収集の見極めに役立ちます。* |

|  |
| --- |
| **インシデントハンドリングに必要な情報の所在に関する検討****（文書レビューによるアプローチ）** |
| ***ポイント****：** *既存の文書をレビューすることは、「利害関係者、情報源、システムの所有者の特定」および「CSIRT が遵守すべき既存のポリシーの概要の準備」の目的に適う。*
* *文書には、CSIRTが従わなければならないポリシーや手順が存在する。*
* *文書には、CSIRTのポリシー、手順、その他の文書の作成時に使用しなければならない文言が含まれる。*
* *CSIRT活動に必要な連絡先リストも含まれている可能性がある。*
 |
| 1. **事業や特有の事業機能のための組織図**
 |
| * + *ポイント*
	+ *組織における CSIRT の位置づけを見つける。*
 |
|  |
| 1. **組織またはサービス対象のシステムとネットワークの形態（トポロジー）**
 |
| * + *ポイント*
		- *機微な情報を扱う CSIRT に必要なネットワークの確保*
		- *CSIRT が権限を有する範囲の特定（他の担当部署との切り分け）*
 |
|  |

|  |
| --- |
| 1. **重要なシステムと資産目録**
 |
| * + *ポイント*
		- *想定されるインシデントによって影響を受ける情報資産の把握*
 |
|  |
| 1. **既存の災害復旧計画と事業継続計画**
 |
| * + *ポイント*
		- *関連するインシデント対応に関する既存の規定との整合性*
 |
|  |
| 1. **既存の物理セキュリティ侵害を対策する組織への通知に関するガイドライン**
 |
| * + *ポイント*
		- *インシデント対応にかかる物理セキュリティに関する外部との連携状況の把握*
 |
|  |

|  |
| --- |
| 1. **既存のインシデント対応計画**
 |
| * + *ポイント*
		- *インシデント対応に関する既存の計画との整合性*
 |
|  |
| 1. **親組織等の規則**
 |
| * + *ポイント*
		- *CSIRTの運営に必要な規則体系（親組織から影響を受ける範囲）の把握*
 |
|  |
| 1. **既存のセキュリティポリシーと手順**
 |
| * + *ポイント*
		- *策定すべきインシデント対応のポリシーや手順と、既存のセキュリティポリシーや手順との整合性*
 |
|  |

*アドバイス：*

* *他組織のCSIRTの情報の活用*
	+ *他組織のCSIRTの活動を調査する*
	+ *そのCSIRTに直接連絡できる場合は、設立の経緯を尋ねる*
	+ *そのCSIRTのWebサイトから、使命、憲章、資金計画、サービスリストを調べる*
	+ *CSIRTに関する書籍や公開文書を読む*

*これらにより、CSIRTを構築する上での良いアイディアが得られる*

*アドバイス：*

* *カンファレンスやワークショップの活用*
	+ *CSIRT 構築に関するセッションを含んだカンファレンスに参加する*
	+ *カンファレンス会場において、互いのアイディアを交換し、協力関係を築く機会を得る*