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

構築に必要な現状把握

（バージョン 1．0　　2021 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

Version 2.1

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。*
(例) ➢ 既存のインシデントの対応状況は、以下の通り。 ✧ ほとんどのインシデントについては、「各部署内」での対応になっている。 ● 部署でのインシデント対応に関するノウハウは、他の部署に共有されていない。 ✧ 会社全体で対応したのは、過去に 2 件のみで、事実上の対策室が設けられ、CIO が直接指示を取った。 ● その都度の対応で、その対応体制や手順などについては、文書化されていない。 ✧ ビジネス的に直接影響するインシデントは把握されているが、軽微なインシデントについては、把握されていない。 ✧ 簡単な調査により、これまでの発生インシデントの分類は、「お客様 ID の不正使用」、「情報漏えい(ノート PC 紛失を含める)」、「原因不明のネットワークトラフィックの急増による、Web サービス不能状態の発生」などが見られる。

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）

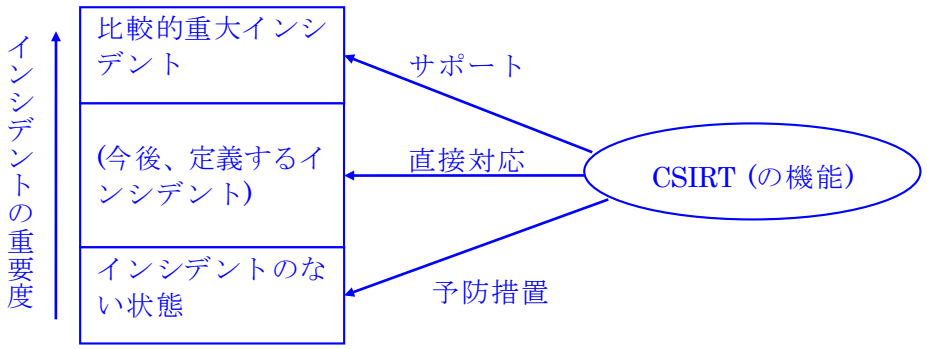
***ポイント**:*
CSIRT を計画し実装するために必要な情報を、組織内のステークホルダーから引き出す。各ステークホルダーとの個別のインタビューやディスカッションにより、誰が情報を何の持っているのかを認識し、その情報を最大限に引き出すことを図る。

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*

(例)

- CIO に対するインシデント対応の専門組織(CSIRT)の理解は得られている。
- 経営層全体からは、各部署(IT 部門、総務部門)で実施されているインシデント対応の切り分けが懸念されている。
- 経営層によるインシデント対応の意思決定にかかわるのは、「比較的重大なインシデント」とされているが、具体的な評価基準は定められていない。
- 経営層から現場に対する「インシデント対応にかかる」意思決定の権限委譲が十分ではない。
- 経営層による CSIRT（の機能）の設置認識は、以下のとおり。

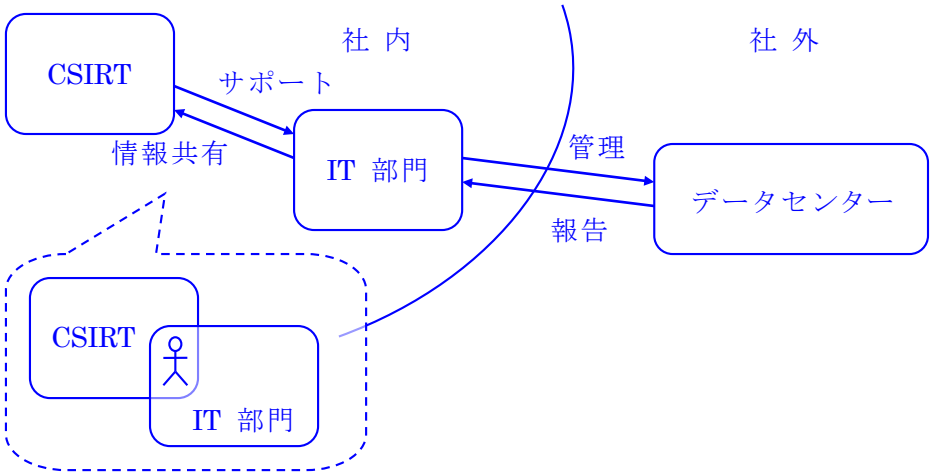


2. IT 部門

- *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*

(例)

- 外部のお客様に提供しているシステムは、外部のデータセンターに存在しており、その管理責任は、IT 部門となっている。
- 社内用のシステムに関する管理は、IT 部門が直接担当している。
- 現状では、IT 部門が実施するインシデント対応と、情報セキュリティ本部が実施するインシデント対応の連携はされていない。
- CSIRT と IT 部門のとの予想関係図は、以下のとおり。(IT 部門の人員を CSIRT に入れるかどうか検討中)

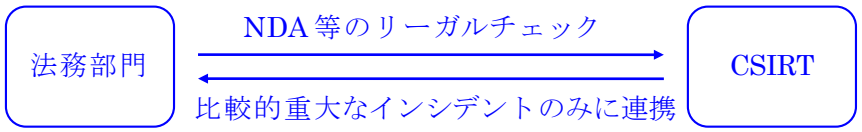


3. 法務部門

- *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*

(例)

- 比較的重大なインシデントについては、法務部門が関わることになっている。
- 通常のインシデントについては、事後に確認をすることがある。
- 通常は、契約書等の内容のチェックを担当してもらう。
- 法務部門との CSIRT とのかかわりを示した概念図は以下のとおり。

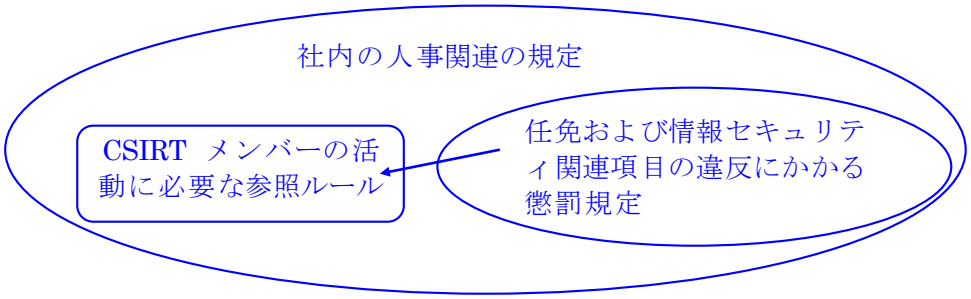


4. 人事部門

- *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*

(例)

- CSIRT メンバーの懲罰規定は、社内の就業規則に定められているものに従う。
- 機微な情報と取り扱う CSIRT メンバーへの特別な規定については、現時点では検討していないが、運用開始時に、必要性が出れば検討をする。

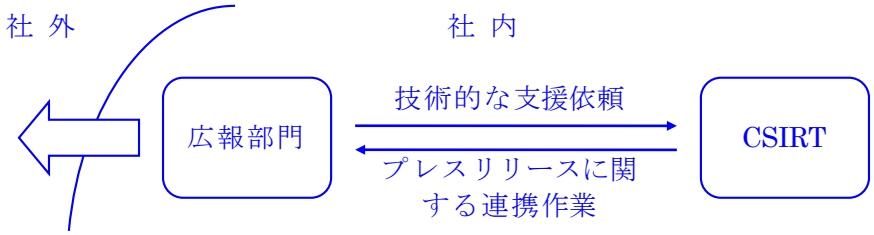


5. 広報部門

- *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*

(例)

- インシデント対応の一つで、プレスリリースが必要なときは、必ず広報を通すことになっている。
- 広報部門からは、プレスリリース文を作成する際、技術的な内容を記述する際、インシデント対応を担当した人からの支援が必要なときが出てくる。
- 広報部門と CSIRT の連携図は、以下のとおり。



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*

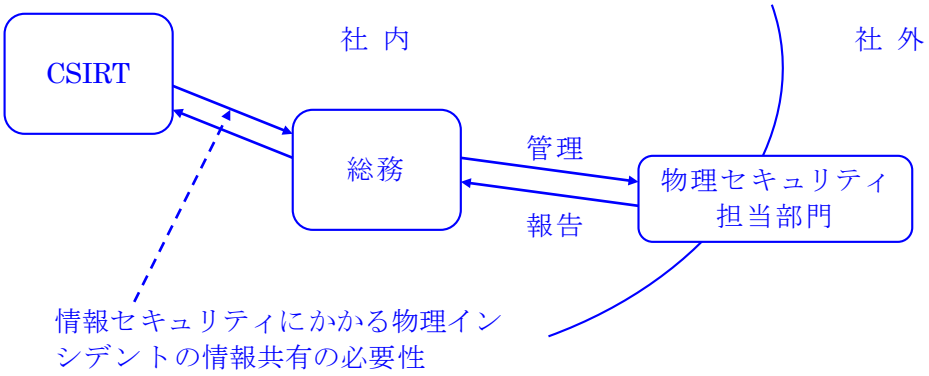
(例)

✧ 物理セキュリティにかかる器材を担当しているのは、総務である。

✧ ビル管理のセキュリティについては、外注業者に委託している。

✧ 物理的なインシデント（不審人物侵入など）の情報は、総務に一報されることになっている。

✧ CSIRT と物理セキュリティ部門が連携する場合の概念図は以下のとおり。



7. 既存のセキュリティチーム

➢ *ポイント*

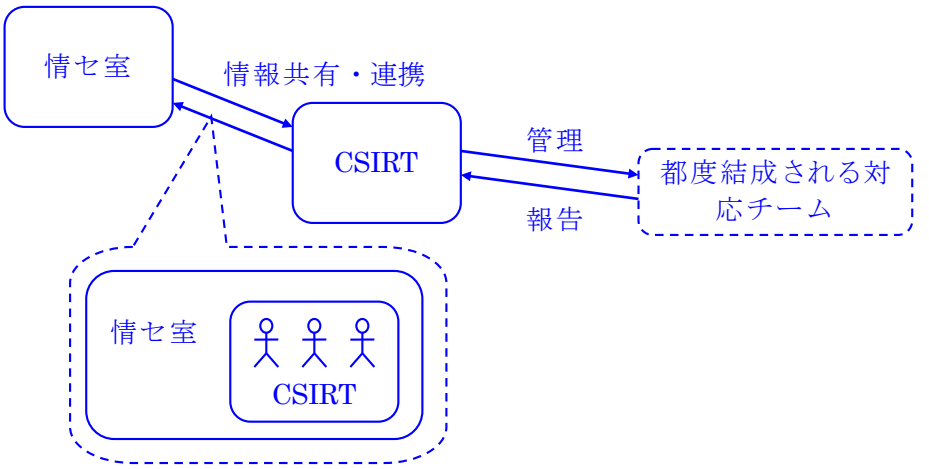
✧ *コンピューターセキュリティインシデントへの対応について、どのようなノウハウを持っているかを確認する*

(例)

✧ 会社全体のセキュリティポリシーは、情報セキュリティ室が担当し、比較的重大なインシデントを担当することがある。

✧ しかし、各部署で扱うインシデントについては、その都度、関係者が集まり事実上の対応チームが結成されるが、インシデントが解決されると、すぐに解散される。

✧ 情報セキュリティ室内に CSIRT を構築することを検討中であり、その概念図は、以下のとおり。



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*

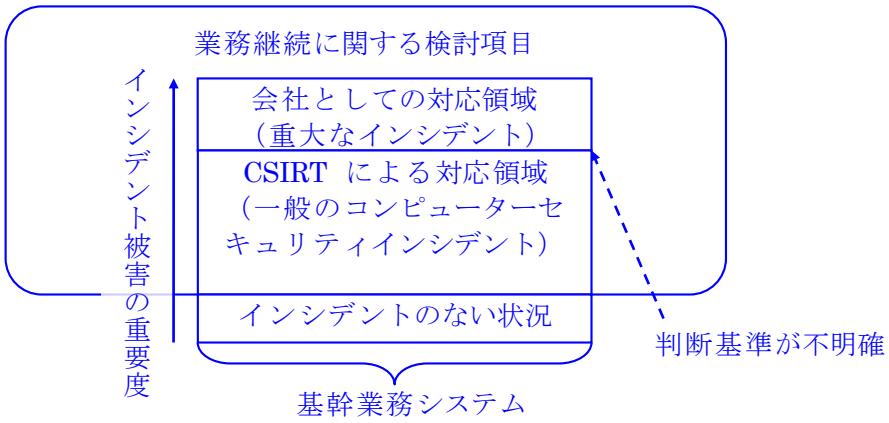
(例)

✧ 現在、どこの部署も BCP の作成はしていない。

✧ 業務基幹システムの IT 依存度が高いため、業務継続性の観点から、コンピューターセキュリティインシデントによる被害からの復旧については、経営層が強い関心を示しているが、被害の重要度の違いによる担当部署が明確ではない。

✧ 業務基幹システムにおける不正なデータ改ざん等を発見する仕組みについて、監査部門が強い関心を示している。

✧ 業務継続に関するヒアリングの結果、得られた傾向は以下のとおり。



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*

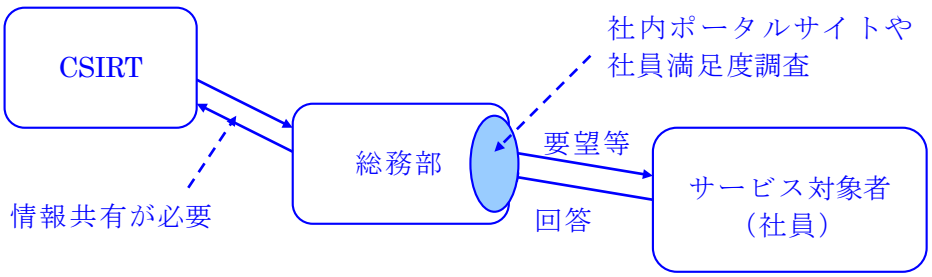
(例)

✧ CSIRT のサービス対象者である社員からは、社内のポータルサイトを通じて、ニーズを得ることができる。

✧ 社内のポータルサイトは、IT 部門がシステム自体管理し、総務部がコンテンツの管理をしている。

✧ 従業員満足度調査は、総務部が担当している。

✧ 現状、CSIRT がサービス対象者からのニーズを得るための概念図は以下のとおり。



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*

(例)

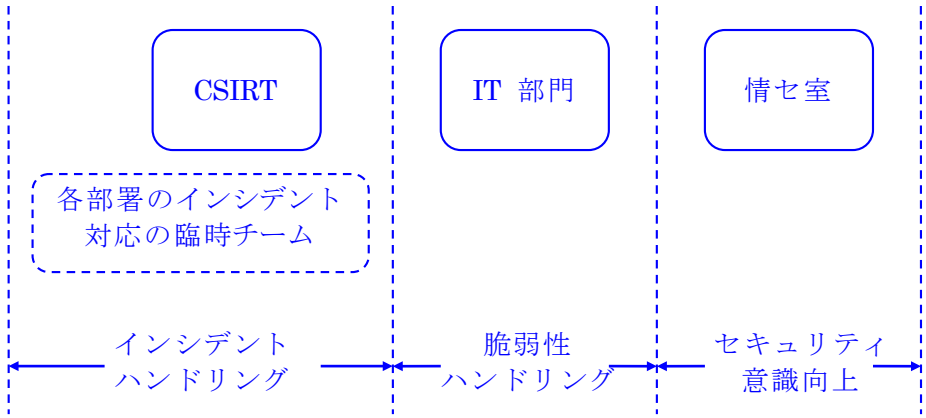
- 外部に公開しているお客様専用サーバー（外部のデータセンター内）の監視を、外部の SOC 事業者に委託している。
- 外部の SOC 事業者を管理しているのは、IT 部門である。
- IT 部門は、SOC 事業者および JPCERT/CC より情報収集をしている。
- APT などの外的要因によるインシデントが発生した場合は、JPCERT/CC に対応の依頼をしている。
- JPCERT/CC に対する連絡は、IT 部門が担当している。
- 警察に対しては、法務部門が主に担当している。
- インシデント対応にかかる外部との連携の概念図は以下のとおり。

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*

(例)

- 社員のセキュリティ啓発活動は、情報セキュリティ室が担当している。
- 各部署それぞれに特化したインシデントについては、各部署内でインシデント対応ができる能力があるが、そのチームの結成は、インシデントが発生してからとなる。
- 脆弱性の対応は、IT 部門が担当している。
- インシデントにかかるサービスをしている社内状況は、想定する CSIRT のサービスを含めると概念図は以下のとおり。



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**:*

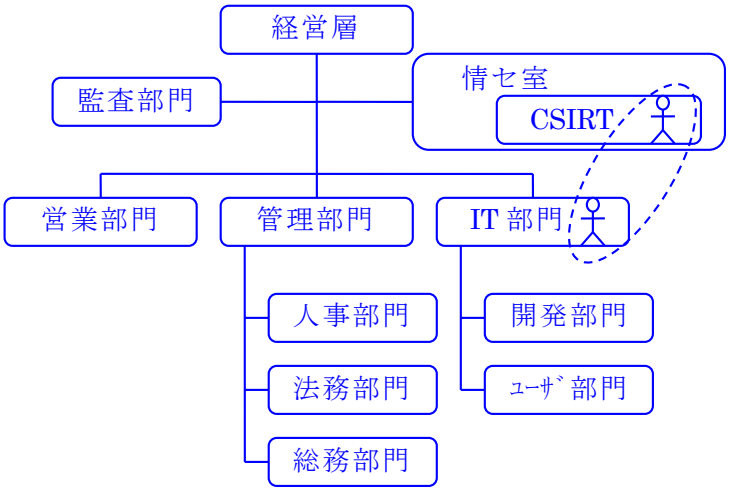
- *既存の文書をレビューすることは、「利害関係者、情報源、システムの所有者の特定」および「CSIRT が遵守すべき既存のポリシーの概要の準備」の目的に適う。*
- *文書には、CSIRT が従わなければならないポリシーや手順が存在する。*
- *文書には、CSIRT のポリシー、手順、その他の文書の作成時に使用しなければならない文言が含まれる。*
- *CSIRT 活動に必要な連絡先リストも含まれている可能性がある。*

12. 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。*

(例)

✧ CSIRT の設置すべき場所を情報セキュリティ室内に配置し、そのチーム内には、パートタイムあるいは兼務で IT 部門の人を参加させる形態となる。



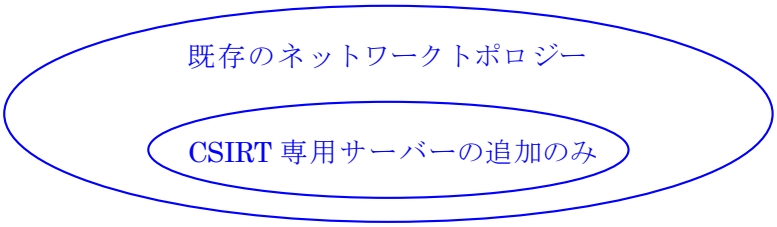
13. 組織またはサービス対象のシステムとネットワークの形態（トポロジー）

- ➢ *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）*

(例)

✧ CSIRT が使用するネットワークは、既存のものを活用するが、機微な情報の共有のために、専用のサーバーを設置する。

✧ クライアントは、既存のものを活用し、新しく設けることはない。

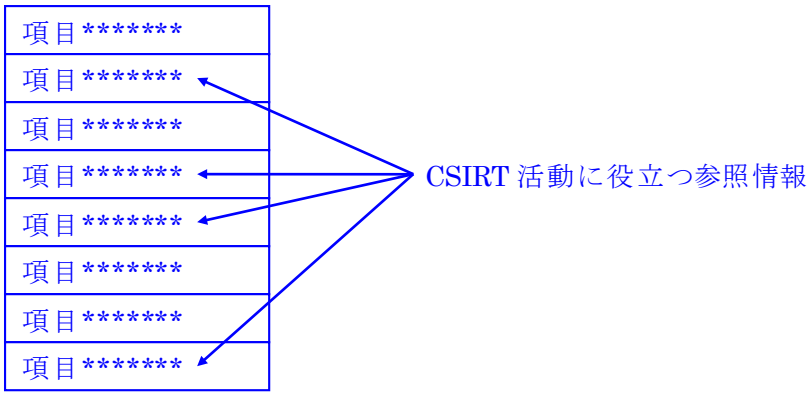


14. 重要なシステムと資産目録

- *ポイント*
  - *想定するインシデントに影響する情報資産の把握*

(例)

- インシデント発生時における初期の被害対象の重要度および被害程度の目安として活用できる項目を抽出する。

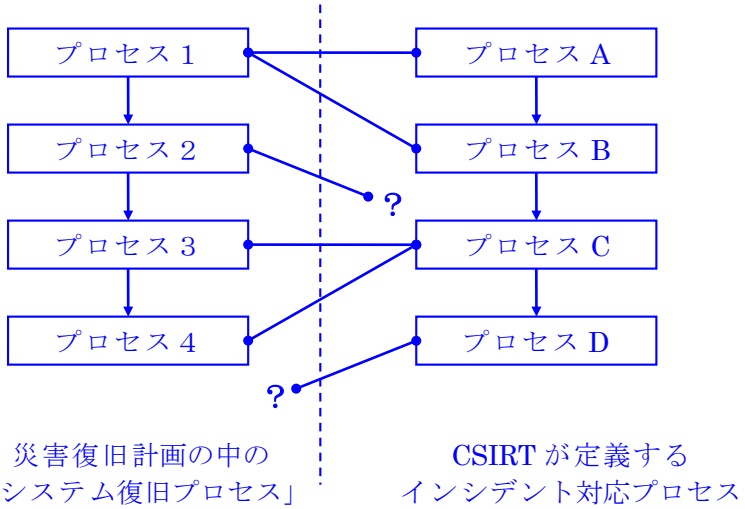


15. 既存の災害復旧計画と事業継続計画

- *ポイント*
  - *既存の関連するインシデント対応に関する規定との整合性*

(例)

- 災害復旧計画等に「システムの復旧」の項目が抽象的に記述されており、それとの整合性を考慮する。
- 「事故」や「インシデント」等の定義を明確にする必要がある。



Version 2.1

16. 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*

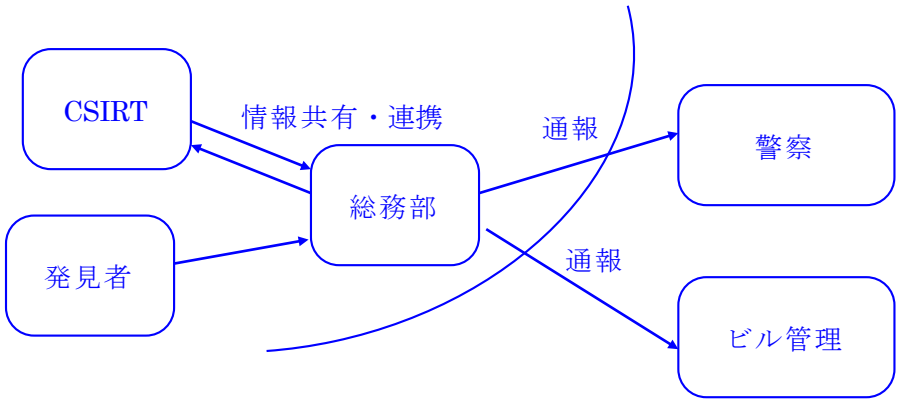
(例)

✧ ビル管理に対する通知等については、ビル管理規定に定められている。

✧ ビル管理規定において、インシデント対応に関する記述は、「不審者への対応」とそれにかかる「外部に対する連絡に関する規定」であった。

✧ ビル管理規定には、「総務部」が POC（連絡窓口）となっている。

✧ 既存の物理セキュリティ侵害に関する規定の概念図は以下のとおり。



17. 既存のインシデント対応計画

➢ *ポイント*

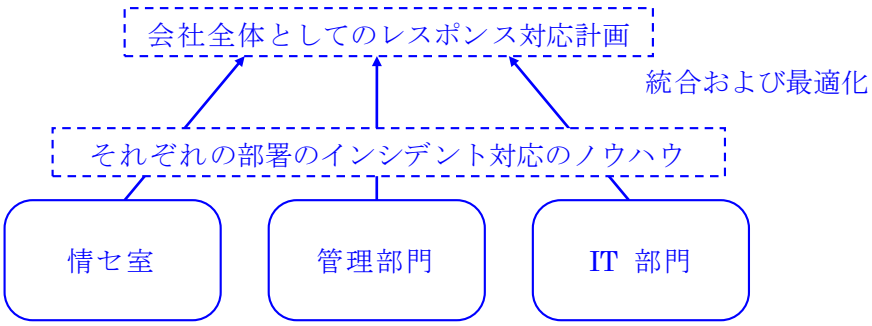
✧ *インシデント対応に関する既存の計画との整合性*

(例)

✧ 既存のインシデント対応に関する計画は存在していない。

✧ 各部署独自で経験的なインシデント対応に関するノウハウはあるが、文書化はされていない。

✧ 社内のインシデント対応を統合し、最適化することにより、会社全体としてのレスポンス対応計画を作成できる見込み。その概念図は以下の通り。

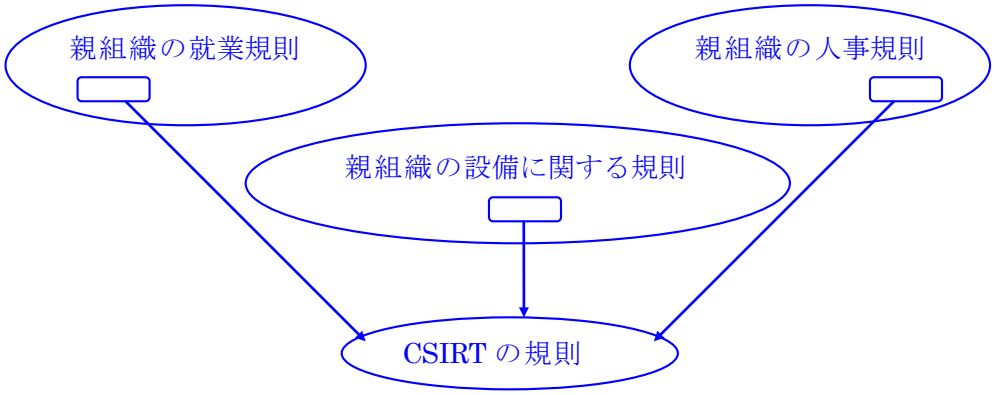


18. 親組織等の規則

- *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*

例）

- CSIRT に関する規則を策定する際、親組織に存在している各規則で使用している文言を適切に使用する。
- 特に、用語の定義に関して齟齬が出ないように、配慮する必要がある。
- 親組織との CSIRT の規則との相関関係の概念図は以下のとおり。



19. 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*

例）

- 既存のセキュリティポリシーは、予防策に関するものが多く、インシデントが発生した場合の記述が少ない。
- 既存のセキュリティプロシージャは、意思決定に関する記述が不足しており、その都度の判断が必要なところが散見される。
- インシデント対応の関する規定は、現在のセキュリティポリシーやプロシージャに基づいた、あるいは、その範囲内のものでなければならない。