2015 年度 CSIRT 構築および運用における実態調査

一般社団法人 JPCERT コーディネーションセンター

2016 年 6 月 29 日

1. はじめに

1.1. 調査の目的

近年のサイバー攻撃は、個別の組織や業界を標的とした攻撃、一個人の情報や金銭の搾取を目的とした攻撃、政治的な主張や技術力を誇示するための攻撃など、目的や対象、手法が多岐にわたり、事業の根幹を揺るがすような影響を及ぼすものもある。そのため、組織では、サイバー攻撃への備えが課題となっている。備えの一つとして、発生したセキュリティインシデントに組織が効果的に対処するための組織体制の要となる「Computer Security Incident Response Team (CSIRT)」の構築が注目されている。経済産業省が公開した「サイバーセキュリティ経営ガイドライン*1 」も CSIRT 整備の必要性に言及しており、今後 CSIRT を構築する組織の増加が見込まれる。

CSIRT の構築および運用については、母体となる組織文化や集められる要員の技術的背景などによって、さまざまな形態がある。そして、各組織の CSIRT の多くは、日本シーサート協議会 (以下、NCA) などの団体に加盟して他の CSIRT との交流を図ることにより、CSIRT の体制やその活動を他の CSIRT と比較している。その中で、多様な CSIRT の体制や活動などについて話し合うことで、グッド・プラクティスを模索している。本調査の目的は、そうした期待に応えて、国内の様々な組織における CSIRT 活動の実態を調査してまとめた資料として提供することにより、新たに CSIRT 構築しようとしている方々の参考としていただくだけではなく、既に CSIRT を運用している組織においても次の段階に向けた検討に役立てていただくことにある。

本調査では、NCA に加盟している CSIRT に対しアンケート調査やインタビューを実施した。アンケート調査では、組織体制やメンバー構成、ポリシーなど CSIRT の構築時に定義しておくべき項目を含めている。また、インタビューでは、CSIRT の運用改善の参考となるよう、各業界で際立った活動を行っている CSIRT を対象に、組織の取り組み状況や課題についてヒアリングした結果をまとめている。CSIRT の構築や活動の改善に関心をもっておられる方々の参考となることを願っている。

本調査におけるアンケートやインタビューにご協力くださった CSIRT の皆様には厚く感謝申し上げる。

1.2. 本報告書が想定している読者

本調査報告書が想定している読者は次のような方々である。

- CSIRT の構築を検討している担当者・責任者
- CSIRT を構築中の担当者・責任者
- CSIRT を運用中の担当者・責任者

*1 サイバーセキュリティ経営ガイドライン：
http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf

1.3. 調査方法の概要

1.3.1. アンケート調査

本調査で実施したアンケートの概要は次のとおりである。調査項目については表 1.3.1 を参照されたい。

実施日時	2015 年 12 月 8 日
実施対象	日本シーサート協議会 (NCA) 「第 11 回シーサートワーキンググループ会」参加組織
実施要綱	アンケート結果を分析して公開することにより CSIRT の周知啓発や、CSIRT コミュニティ活動の発展を図る等の調査の目的を説明した上で、上記の会合の参加組織に書面を配布して回答の記載を求め、会合の終了時に回収した。回答票への記名は自由。
調査票の概要	「CSIRT 構築・運用に関するアンケート」と題して、各組織におけるサービス提供範囲や運用状況などをたずねた。
回答組織数	66 組織

[表 1.3.1]　アンケート項目

アンケート項目
1.構築時の体制
1.1 構築を主導した部署
(a)　情報システム管理部門系 (b)　経営企画部門系 (c)　法務部門系 (d)　監査部門系 (e)　開発部門系 (f)　総務部門系 (g)　リスク対策部門系 (h)　セキュリティ対策部門系 (i)　品質保証部門系 (j)　その他自由記述　[　　]
1.2 構築に関わった部署　※複数回答可
(a)　情報システム管理部門系 (b)　経営企画部門系 (c)　法務部門系 (d)　監査部門系 (e)　開発部門系 (f)　総務部門系 (g)　リスク対策部門系 (h)　セキュリティ対策部門系 (i)　品質保証部門系 (j)　その他自由記述　[　　]
1.3 構築時に調整が必要だった部署　※複数回答可
(a)　情報システム管理部門系 (b)　経営企画部門系 (c)　法務部門系 (d)　監査部門系 (e)　開発部門系 (f)　総務部門系 (g)　リスク対策部門系 (h)　セキュリティ対策部門系 (i)　品質保証部門系 (j)　その他自由記述　[　　]
1.4 構築に携わった人数(外注含む)
(a)　5名未満

(b) 5名以上10名未満
(c) 10名以上20名未満
(d) 20名以上

1.5 構築開始時期

yyyy年mm月

1.6 構築完了時期(設立時期)

yyyy年mm月

2.CSIRTの体制

2.1 組織内のどの部署に配置されているか ※複数回答可

(a) 情報システム管理部門系
(b) 経営企画部門系
(c) 法務部門系
(d) 監査部門系
(e) 開発部門系
(f) 総務部門系
(g) リスク対策部門系
(h) セキュリティ対策部門系
(i) 品質保証部門系
(j) その他自由記述 [ ]

2.2 インシデント発生時のCSIRTに位置づけ ※複数回答可

(a) 現場で対応作業を実施または支援
(b) 技術的アドバイザー
(c) コーディネーター(調整役)
(d) その他自由記述 [ ]

2.3 CSIRTのサービス対象者 ※複数回答可

(a) 自組織内ユーザ
(b) グループ会社のユーザ
(c) 自社サービスを利用する顧客
(d) その他自由記述 [ ]

2.4 過去に外部からCSIRTに対して連絡、問い合わせはあったか ※複数回答可

(a) Webサービスの脆弱性に関するもの
(b) 製品の脆弱性に関するもの
(c) インシデントに関するもの
(d) その他自由記述 [ ]
(e) 問い合わせはなかった

2.4.1 CSIRTへの連絡、問い合わせはどこからあったか

(a) セキュリティベンダ

(b) IPA
(c) 一般ユーザ
(d) JPCERT/CC
(e) その他自由記述 [ ]

2.5 サイバー攻撃に関する情報共有の枠組みに参加しているか ※複数回答可

(a) IPA(J-CSIP)
(b) 金融 ISAC(各種ワーキンググループ)
(c) 警察庁(CCI)
(d) JPCERT(WAISE)
(e) その他自由記述 [ ]

2.6 情報共有に際して主に利用する表現方法は何か ※複数回答可

(a) テキスト
(b) Open IOC
(c) STIX/TAXII
(d) その他自由記述 [ ]

2.7 対象とする分野 ※複数回答可

[CSIRT が所属する組織のインシデント対応]
(a) 社向インフラ:社員が自社で利用するネットワークで発生したインシデントに対応
(b) 顧客向けサービスのシステム(ネットワーク接続サービス、Web アプリケーション、サービスなど):社外の利用者に対して提供しているサービスで発生したインシデントに対応

[CSIRT が所属しない組織のインシデント対応]
(c) 顧客納入済みシステム(SI 事業など)
(d) 顧客サイト(インシデントレスポンスサービス)

[上記以外]
(e) 自社製品(ハードウェア、ソフトウェア)の脆弱性対応
(f) その他自由記述 [ ]

2.8 インシデント発生時の CSIRT の権限

(a) 緊急度の高いインシデント発生時にシステムを停止する権限がある
(命令指示できる権限がある)
(b) 緊急度の高いインシデント発生時にシステムを停止する必要性について助言ができる
(c) 緊急度の高いインシデント発生時にシステムを停止する権限はない

2.9 具体的な提供サービス

【事後対応型サービス】… サービス毎に［内製/外注/提供していない］を選択
(a) アラートと警告
(b) インシデントハンドリング(オンサイト or アドバイス)

(c) 脆弱性ハンドリング(自社製品 or 利用製品・サービス)
(d) マルウエア解析
(e) フォレンジック
(f) ログ分析

【事前対応型サービス】… サービス毎に［内製/外注/提供していない］を選択
(g) パブリックモニタリング
(h) セキュリティ動向分析
(i) 侵入検知
(j) 技術動向監視
(k) 注意喚起・アナウンス
(l) セキュリティ関連情報の提供
(m) セキュリティ監査または審査
(n) セキュリティツール、アプリケーション、インフラ、およびサービスの運用
(o) セキュリティツールの開発(CSIRT が利用するものを含む)

【セキュリティ品質管理サービス】… サービス毎に［内製/外注/提供していない］を選択
(p) 新サービスまたはシステム等のリスク評価への関与
(q) 事業継続と障害復旧計画への関与
(r) 各種セキュリティに関わる相談対応
(s) 啓発・意識向上活動
(t) 教育／トレーニング
(u) 製品の評価または認定
(v) セキュリティポリシー策定への関与

【その他】… 上記以外のサービスがあれば自由記述で追記
(w) その他 [ ]

2.10 サービスレベルの定義はあるか

(a) ある
(b) ない
(c) その他自由記述 [ ]

2.11 報告を受けたインシデントについて分類を定義している

(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている
(b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている
(c) 明確に設定され、文書として存在しているが、正式に承認されていない
(d) だいたいの目安になるものは設定されているが、文書として存在していない
(e) 設定されておらず、発生の都度検討している

2.12 CSIRT のサービス対象者や権限、サービス、インシデントの定義等が文書化されている

(a) されている
(b) されていない
(c) その他自由記述 [ ]

2.13 セキュリティポリシーについて定義している

(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている
(b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている
(c) 明確に設定され、文書として存在しているが、正式に承認されていない
(d) だいたいの目安になるものは設定されているが、文書として存在していない
(e) 設定されておらず、発生の都度検討している

2.14 SOC による監視体制が運用・構築されているか

(a) 構築・運用している
(b) 構築運用していない

2.14.1 SOC の監視体制はどのようなものか

(a) 24 時間 365 日監視
(b) 平日日勤帯のみ
(c) その他自由記述 [ ]

2.14.2 SOC の運用体制はどのようなものか

(a) 自組織で運用している
(b) グループ会社に外注している
(c) 他社に外注している

2.14.2.1 SOC と CSIRT の関係はどのように位置づけられているか

(a) CSIRT が SOC 機能を有している
(b) SOC 内に CSIRT を構築している
(c) それぞれが独立した部署として存在しており、連携している

3.CSIRT メンバー

3.1 CSIRT メンバーの行動規範や指針が定められているか

(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている
(b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている
(c) 明確に設定され、文書として存在しているが、正式に承認されていない
(d) だいたいの目安になるものは設定されているが、文書として存在していない
(e) 設定されておらず、発生の都度検討している

3.2 設立当初のメンバー人数

○○人

3.2.1 正社員と外部委託のメンバーの割合

(a) すべて外部委託
(b) 正社員 2 割以下
(c) 正社員 2～4 割
(d) 正社員 4～7 割
(e) 正社員 8 割以上
(f) すべて正社員

3.3 現在のメンバーの人数

○○人

3.3.1 正社員と外部委託のメンバーの割合

(a) すべて外部委託
(b) 正社員 2 割以下
(c) 正社員 2～4 割
(d) 正社員 4～7 割
(e) 正社員 8 割以上
(f) すべて正社員

3.4 CSIRT メンバーに必要なスキルセットが定義されているか

(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている
(b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている
(c) 明確に設定され、文書として存在しているが、正式に承認されていない
(d) だいたいの目安になるものは設定されているが、文書として存在していない
(e) 設定されておらず、発生の都度検討している

3.5 CSIRT メンバー向けに組織内部で提供されているトレーニングを受講できる体制やルールが確立されているか

(a) CSIRT メンバーが参加するトレーニングについて、明確な基準が存在する
(b) CSIRT メンバーが参加するトレーニングについて、だいたいの目安になる基準は存在する
(c) CSIRT メンバーが参加するトレーニングについて、基準が確立しておらず、受講の都度検討している

3.6 CSIRT メンバー向けに外部の技術トレーニングを受講できる体制が確立されているか

(a) CSIRT メンバーが参加するトレーニングについて、明確な基準が存在する
(b) CSIRT メンバーが参加するトレーニングについて、だいたいの目安になる基準は存在する
(c) CSIRT メンバーが参加するトレーニングについて、基準が確立しておらず、受講の都度検討している

3.7 CSIRT メンバー向けに外部のコミュニケーショントレーニングを受講できる体制が確立されているか(プレゼンテーションやコミュニケーションスキルに関するトレーニング)

(a) CSIRT メンバーが参加するトレーニングについて、明確な基準が存在する
(b) CSIRT メンバーが参加するトレーニングについて、だいたいの目安になる基準は存在する

(c) CSIRT メンバーが参加するトレーニングについて、基準が確立しておらず、受講の都度検討している

3.8 メンバーのスキルを定量的に測定する仕組み(試験や資格など)があるか

(a) ある
(b) ない
(c) その他自由記述 [ ]

4.プロセスやルール

4.1 経営層(あるいは経営層を含む情報セキュリティ委員会等)へのエスカレーションルールは設定されているか

(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている
(b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている
(c) 明確に設定され、文書として存在しているが、正式に承認されていない
(d) だいたいの目安になるものは設定されているが、文書として存在していない
(e) 設定されておらず、発生の都度検討している

4.2 広報部門へのエスカレーションルールは設定されているか

(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている
(b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている
(c) 明確に設定され、文書として存在しているが、正式に承認されていない
(d) だいたいの目安になるものは設定されているが、文書として存在していない
(e) 設定されておらず、発生の都度検討している

4.3 法務部門へのエスカレーションルールは設定されているか

(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている
(b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている
(c) 明確に設定され、文書として存在しているが、正式に承認されていない
(d) だいたいの目安になるものは設定されているが、文書として存在していない
(e) 設定されておらず、発生の都度検討している

4.4 インシデントを防止、検知、解決するためのプロセスが定められているか

(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている
(b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている
(c) 明確に設定され、文書として存在しているが、正式に承認されていない
(d) だいたいの目安になるものは設定されているが、文書として存在していない
(e) 設定されておらず、発生の都度検討している

4.5 CSIRT の活動が内部評価や外部評価によって監査され、フィードバックを受ける体制が定められているか

(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている
(b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている
(c) 明確に設定され、文書として存在しているが、正式に承認されていない
(d) だいたいの目安になるものは設定されているが、文書として存在していない
(e) 設定されておらず、発生の都度検討している

4.6 緊急時に備えて、CSIRT メンバーや関連する担当者間の連絡網が整備されているか

(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている
(b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている
(c) 明確に設定され、文書として存在しているが、正式に承認されていない
(d) だいたいの目安になるものは設定されているが、文書として存在していない
(e) 設定されておらず、発生の都度検討している

4.7 CSIRT の目的やサービスについて説明した Web ページが自社のサイト内に存在するか

(a) 存在する
(b) 存在しない
(c) その他自由記述 [ ]

4.8 機微な内容を含むインシデントレポートや情報の取り扱い方法について定められているか

(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている
(b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている
(c) 明確に設定され、文書として存在しているが、正式に承認されていない
(d) だいたいの目安になるものは設定されているが、文書として存在していない
(e) 設定されておらず、発生の都度検討している

4.9 経営層(あるいは経営層を含む情報セキュリティ委員会等)に CSIRT 活動について定期的に報告を行う体制が定められているか

(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている
(b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている
(c) 明確に設定され、文書として存在しているが、正式に承認されていない
(d) だいたいの目安になるものは設定されているが、文書として存在していない
(e) 設定されておらず、発生の都度検討している

4.10 分類されたインシデントについて統計的な処理のうえ、サービス対象者等に開示するルール等が定められているか

(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている
(b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている
(c) 明確に設定され、文書として存在しているが、正式に承認されていない

(d) だいたいの目安になるものは設定されているが、文書として存在していない
(e) 設定されておらず、発生の都度検討している

4.11 CSIRT において定期的な打ち合わせを実施する体制が定められているか

(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている
(b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている
(c) 明確に設定され、文書として存在しているが、正式に承認されていない
(d) だいたいの目安になるものは設定されているが、文書として存在していない
(e) 設定されておらず、発生の都度検討している

5.ツールについて

5.1 IT 資産の管理を組織的に実施しているか

(a) 実施している
(b) 実施していない

5.2 インシデント対応を追跡するためトラッキングシステムやワークフローを導入している

(a) 実施している
(b) 実施していない

6.体制やルールの見直し

6.1 定期的にサービスの提供範囲の見直しを実施しているか

(a) 月に 1 回以上実施
(b) 四半期に 1 回
(c) 半年に 1 回
(d) 年に 1 回
(e) 年に 1 回未満
(f) 実施していない

6.2 定期的にセキュリティポリシー等の文書の見直しを実施しているか

(a) 月に 1 回以上実施
(b) 四半期に 1 回
(c) 半年に 1 回
(d) 年に 1 回
(e) 年に 1 回未満
(f) 実施していない

6.3 定期的に連絡体制図(メールアドレスや電話番号等)の見直しを実施しているか

(a) 月に 1 回以上実施
(b) 四半期に 1 回
(c) 半年に 1 回
(d) 年に 1 回
(e) 年に 1 回未満

- (f) 実施していない

7. レポート

- 7.1 定期的にレポートは発行しているか
  - (a) 月に 1 回以上実施
  - (b) 四半期に 1 回
  - (c) 半年に 1 回
  - (d) 年に 1 回
  - (e) 年に 1 回未満
  - (f) 実施していない
- 7.1.2 レポートの公開範囲
  - (a) 担当内
  - (b) 関連部署内
  - (c) 社内全体

1.3.2. インタビューの実施

NCA に加盟している 表 1.3.2 の CSIRT（9 チーム）を対象にインタビューを実施した。

[表 1.3.2] インタビュー対象組織

#	チーム名 （略称）	所属組織	インタビュー実施日
1	ASY-CSIRT	ANA システムズ株式会社	2016 年 1 月 18 日
2	DeNA CERT	株式会社ディー・エヌ・エー	2016 年 2 月 12 日
3	FJC-CERT	富士通株式会社	2015 年 12 月 14 日
4	Fuji Xerox CERT	富士ゼロックス株式会社	2015 年 12 月 24 日
5	I-SIRT	株式会社帝国ホテル	2016 年 1 月 20 日
6	MB-SIRT	森ビル株式会社	2015 年 12 月 25 日
7	NTT-CERT	日本電信電話株式会社	2016 年 2 月 10 日
8	T-SIRT	大成建設株式会社	2015 年 12 月 7 日
9	YMC-CSIRT	ヤマハ発動機株式会社	2016 年 2 月 3 日

※並びはチーム名のアルファベット順

各 CSIRT へのインタビュー項目は表 1.3.3 のとおりである。また、各 CSIRT の「組織形態」については JPCERT/CC が公開している「組織内における CSIRT の形態*2」に記載されている分類を参考に、各 CSIRT の組織形態として近いものを JPCERT/CC にて選択した。

[表 1.3.3] インタビュー項目

#	インタビュー項目	内容
1	組織概要	所属組織のサービス概要を中心に、設立の経緯や所属組織との関係
2	CSIRT の体制と保有する権限	CSIRT の要員が専任/兼任か、またその組織形態や CSIRT が所属する部門等。また、セキュリティインシデントが発生した際や脆弱性情報が流通した際の、システムを停止する等の権限の有無等
3	CSIRT 活動の成果	経営層に対する活動報告や社内外に向けた定期レポートの発行、CSIRT の活動における評価資料の有無等
4	CSIRT メンバーへの教育・研修	社内におけるインシデント対応演習等の実施状況や CSIRT 要員の技術者スキルの評価指標、CSIRT 要員の育成に関わる事項
5	CSIRT の体制やサービス、管理機能の見直し時期	CSIRT のサービスや提供範囲、セキュリティポリシー等の文書および連絡先一覧等の見直し等、最適化に関わる事項
6	まとめ	総括や CSIRT の特徴など

*2組織内における CSIRT の形態：
https://www.jpcert.or.jp/csirt_material/files/05_shape_of_csirt20151126.pdf

2. アンケート結果

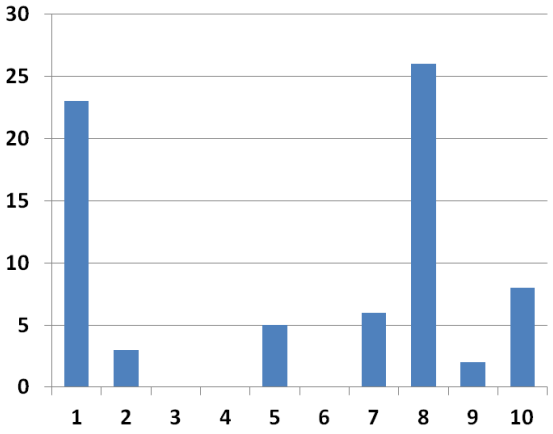
2.1. 構築時の体制

2.1.1. 構築を主導した部署

情報システム管理部門やセキュリティ対策部門が主導して構築された CSIRT が多い。

2.1.1. 構築を主導した部署

#	部署名	回答数
1	情報システム管理部門系	23
2	経営企画部門系	3
3	法務部門系	0
4	監査部門系	0
5	開発部門系	5
6	総務部門系	0
7	リスク対策部門系	6
8	セキュリティ対策部門系	26
9	品質保証部門系	2
10	その他自由記述	8



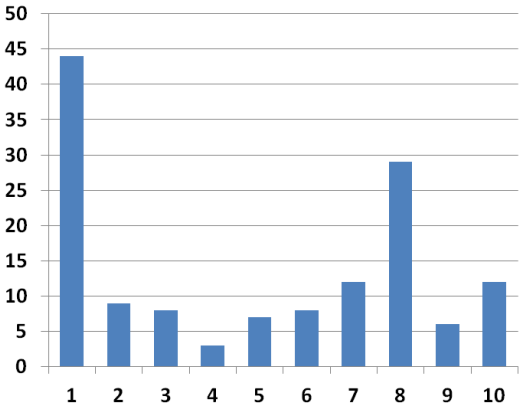
（複数回答あり　N = 66）

2.1.2. 構築に関わった部署

CSIRT 構築には、構築を主導した情報システム管理部門やセキュリティ対策部門に加えて、経営企画部や総務部門なども関わっている。

2.1.2. 構築に関わった部署

#	部署名	回答数
1	情報システム管理部門系	44
2	経営企画部門系	9
3	法務部門系	8
4	監査部門系	3
5	開発部門系	7
6	総務部門系	8
7	リスク対策部門系	12
8	セキュリティ対策部門系	29
9	品質保証部門系	6
10	その他自由記述	12



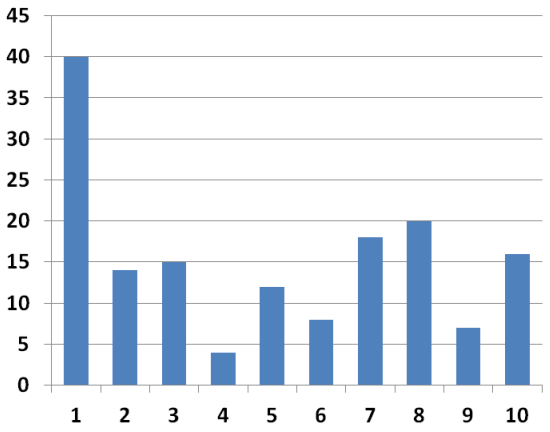
（複数回答あり　N = 66）

2.1.3. 構築時に調整が必要だった部署

CSIRT 構築に際して調整を必要とした部署としては、構築を主導した情報システム管理部門が最も多いが、他の様々な社内部門も含まれる。

2.1.3. 構築時に調整が必要だった部署

#	部署名	回答数
1	情報システム管理部門系	40
2	経営企画部門系	14
3	法務部門系	15
4	監査部門系	4
5	開発部門系	12
6	総務部門系	8
7	リスク対策部門系	18
8	セキュリティ対策部門系	20
9	品質保証部門系	7
10	その他自由記述	16



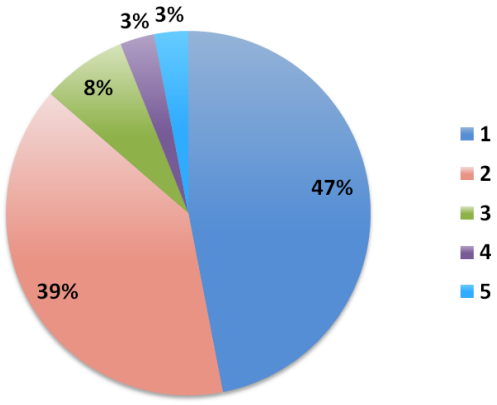
（複数回答あり　N = 61）

2.1.4. 構築に携わった人数（外注含む）

約半数の組織はメンバーが 5 名未満である。メンバーが 10 名未満の CSIRT が 8 割を超える。

2.1.4. 構築に携わった人数（外注含む）

#	人数	回答数
1	5 名未満	31
2	5 名以上 10 名未満	26
3	10 名以上 20 名未満	5
4	20 名以上	2
5	未回答	2

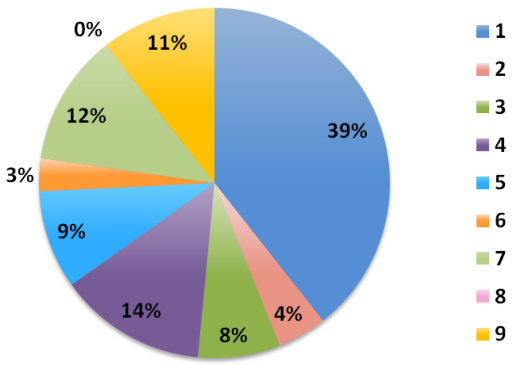


（複数回答なし N = 66）

2.1.5. 構築開始時期

2014 年以降に CSIRT 構築を開始した組織が約半数を占める。

2.1.5. 構築開始時期		
#	時期	回答数
1	2012 年以前	26
2	2013 年上半期	3
3	2013 年下半期	5
4	2014 年上半期	9
5	2014 年下半期	6
6	2014 年（月の記載なし）	2
7	2015 年上半期	8
8	2015 年下半期	0
9	未回答	7

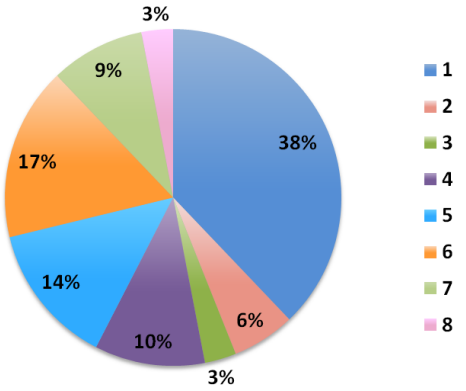


（複数回答なし N = 66）

2.1.6. 構築完了時期（設立時期）

2014 年以降に CSIRT 構築を完了した組織が半数以上を占める。構築にかかった期間については、アンケートの補足 1(P.105) に記載する。

2.1.5. 構築完了時期（設立時期）		
#	時期	回答数
1	2012 年以前	25
2	2013 年上半期	4
3	2013 年下半期	2
4	2014 年上半期	7
5	2014 年下半期	9
6	2015 年上半期	11
7	2015 年下半期	6
8	未回答	2



（複数回答なし N = 66）

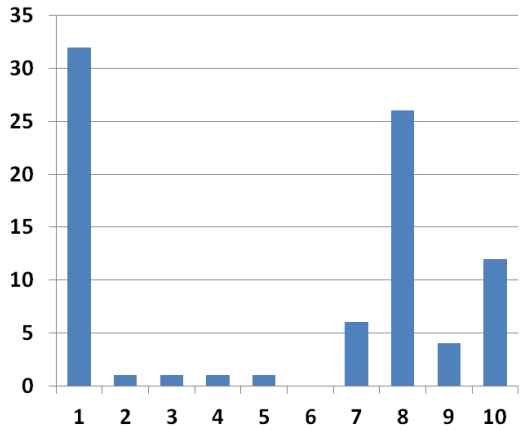
2.2. CSIRT の体制

2.2.1. 組織内のどの部署に配置されているか

CSIRT 構築を主導した情報システム管理部門やセキュリティ対策部門に CSIRT を設置している組織が多い。「その他」の回答の中には「調査研究部門系」を挙げた回答が 3 件あった。

2.2.1. 組織内のどの部署に配置されているか

#	部署	回答数
1	情報システム管理部門系	32
2	経営企画部門系	1
3	法務部門系	1
4	監査部門系	1
5	開発部門系	1
6	総務部門系	0
7	リスク対策部門系	6
8	セキュリティ対策部門系	26
9	品質保証部門系	4
10	その他自由記述	12



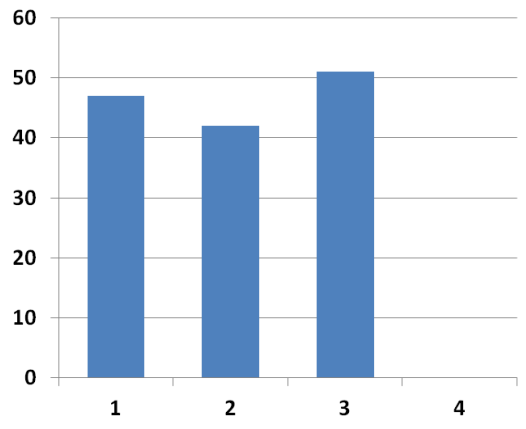
（複数回答あり N = 66）

2.2.2. インシデント発生時の CSIRT の位置づけ

インシデント発生時には、現場での対応から支援、調整役まで幅広い役割が CSIRT に求められている。

2.2.2. インシデント発生時の CSIRT の位置づけ

#	位置づけ	回答数
1	現場で対応作業を実施または支援	47
2	技術的アドバイザー	42
3	コーディネーター（調整役）	51
4	その他自由記述	0



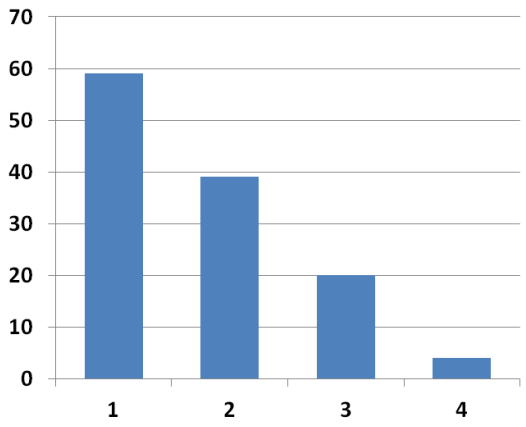
（複数回答あり N = 66）

2.2.3. CSIRT のサービス対象者

多くの CSIRT が、自組織内または自組織内グループ会社を CSIRT のサービス対象としている。また、自組織がサービスを提供している顧客を対象にしている組織も 3 割程度存在する。

2.2.3. CSIRT のサービス対象者

#	サービス対象者	回答数
1	自組織内ユーザ	59
2	グループ会社のユーザ	39
3	自社サービスを利用する顧客	20
4	その他自由記述	4



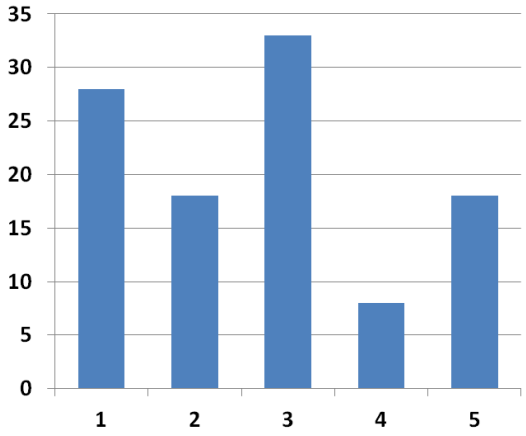
（複数回答あり　N = 66）

2.2.4. 過去に外部から CSIRT に対して連絡、問い合わせはあったか

多くの CSIRT が、外部からの連絡や問い合わせを経験している。

2.2.4. 過去に外部から CSIRT に対して連絡、問い合わせはあったか

#	連絡、問い合わせ内容	回答数
1	Web サービスの脆弱性に関するもの	28
2	製品の脆弱性に関するもの	18
3	インシデントに関するもの	33
4	その他自由記述	8
5	問い合わせはなかった	18



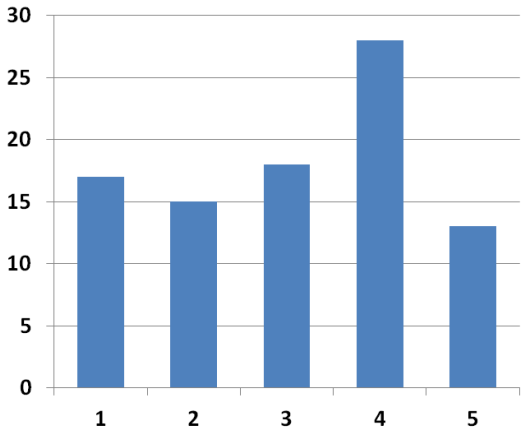
（複数回答あり　N = 66）

2.2.4.1. CSIRT への連絡、問い合わせはどこからあったか

複数の組織から連絡が行われているが、JPCERT/CC からの連絡や問い合わせが最も多い。

2.2.4.1. CSIRT への連絡、問い合わせはどこからあったか

#	組織名	回答数
1	セキュリティベンダ	17
2	IPA	15
3	一般ユーザ	18
4	JPCERT/CC	28
5	その他自由記述	13



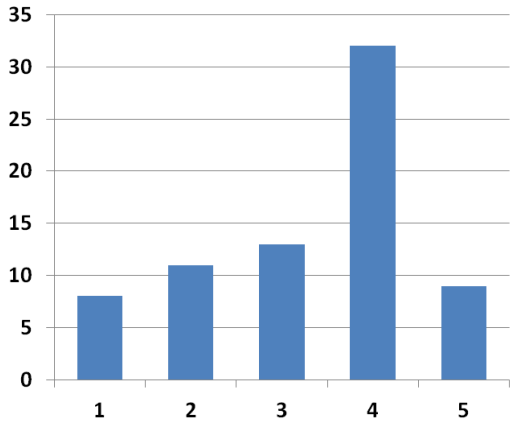
（複数回答あり　N = 48）

2.2.5. サイバー攻撃に関する情報共有の枠組みに参加しているか

サイバー攻撃に関連する情報共有の枠組み*3として JPCERT/CC が活用されている。「その他」の回答の中には「他の CSIRT」を挙げた回答が 5 件あった。

2.2.5. サイバー攻撃に関する情報共有の枠組みに参加しているか

#	情報共有の枠組み	回答数
1	IPA(J-CSIP)	8
2	金融 ISAC (各種ワーキンググループ)	11
3	警察庁(CCI)	13
4	JPCERT/CC(WAISE)	32
5	その他自由記述	9



（複数回答あり N = 44）

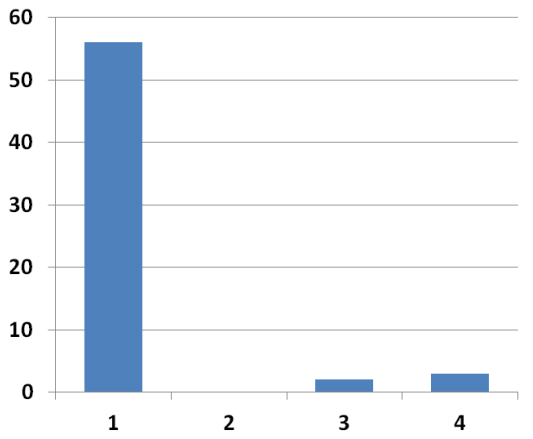
*3 J-CSIP：https://www.ipa.go.jp/security/J-CSIP/
金融 ISAC：http://www.f-isac.jp/working_group/
WAISE：https://www.jpcert.or.jp/wwinfo/

2.2.6. 情報共有に際して主に利用する表現方法は何か

情報共有に際して主に利用する表現方法*4は、テキストによる情報共有がほぼ全体を占める。

2.2.6. 情報共有に際して主に利用する表現方法は何か

#	表現方法	回答数
1	テキスト	56
2	Open IOC	0
3	STIX/TAXII	2
4	その他自由記述	3



（複数回答あり N = 56）

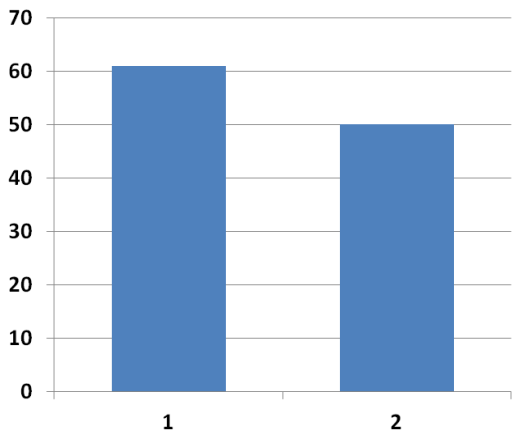
*4 Open IOC：http://www.openioc.org/
STIX：https://stixproject.github.io/about/
TAXII：https://taxiiproject.github.io/about/

2.2.7. 対象とする分野

CSIRT が提供するサービス対象の分野としては、ほぼすべての CSIRT が、自社で利用するネットワークで発生したインシデントや顧客向けサービスのシステムで発生したインシデントに対応していると回答していた。

2.2.7. 対象とする分野
[CSIRT が所属する組織のインシデント対応]

#	分野	回答数
1	社向インフラ:社員が自社で利用するネットワークで発生したインシデントに対応	61
2	顧客向けサービスのシステム(ネットワーク接続サービス、Web アプリケーション、サービスなど)社外の利用者に対して提供しているサービスで発生したインシデントに対応	50

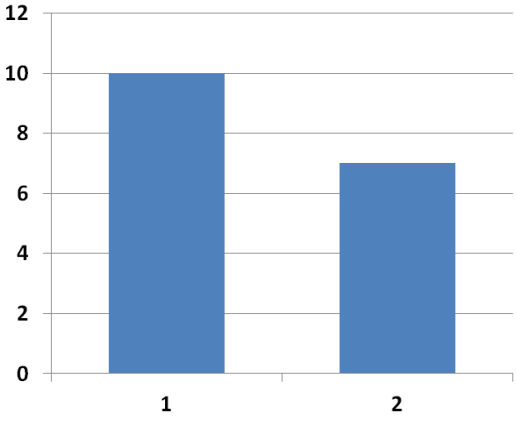


（複数回答あり N = 62）

顧客など組織外にインシデント対応サービスを実施している CSIRT は 2 割程度で少ない。

2.2.7. 対象とする分野
[CSIRT が所属しない組織のインシデント対応]

#	分野	回答数
1	顧客納入済みシステム (SI 事業など)	10
2	顧客サイト(インシデントレスポンスサービス)	7

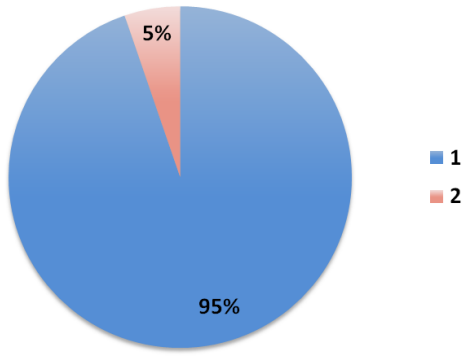


（複数回答あり N = 15）

インシデント対応に加えて、自社製品（ハードウェア、ソフトウェア）の脆弱性にも PSIRT[*5] として対応するサービスを有する CSIRT が一定数存在している。

2.2.7. 対象とする分野
［上記以外］

#	分野	回答数
1	自社製品(ハードウェア、ソフトウェア)の脆弱性対応	18
2	その他自由記述	1



（複数回答あり N = 19）

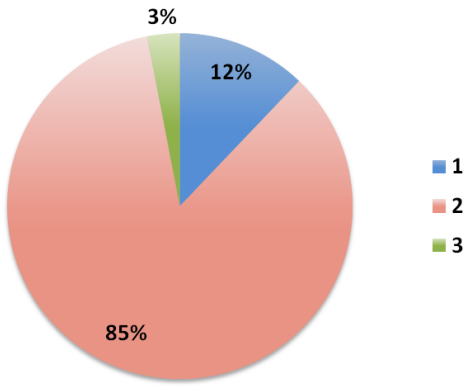
[*5] PSIRT：Product Security Incident Response Team の略称で、ソフトウエアやソフトウエア製品の脆弱性に関する情報の受付やその改修に向けた社内調整、公開を担当するチームを指す。

2.2.8. インシデント発生時の CSIRT の権限

緊急度の高いインシデントが発生した場合に、9 割程度の CSIRT は、関連するシステムの停止の要否について助言できる立場にある。システムの停止を命ずる権限を持っている CSIRT も 1 割程度ある。

2.2.8. インシデント発生時の CSIRT の権限

#	権限	回答数
1	緊急度の高いインシデント発生時にシステムを停止する権限がある	8
2	緊急度の高いインシデント発生時にシステムを停止する必要性について助言ができる	56
3	緊急度の高いインシデント発生時にシステムを停止する権限はない	2



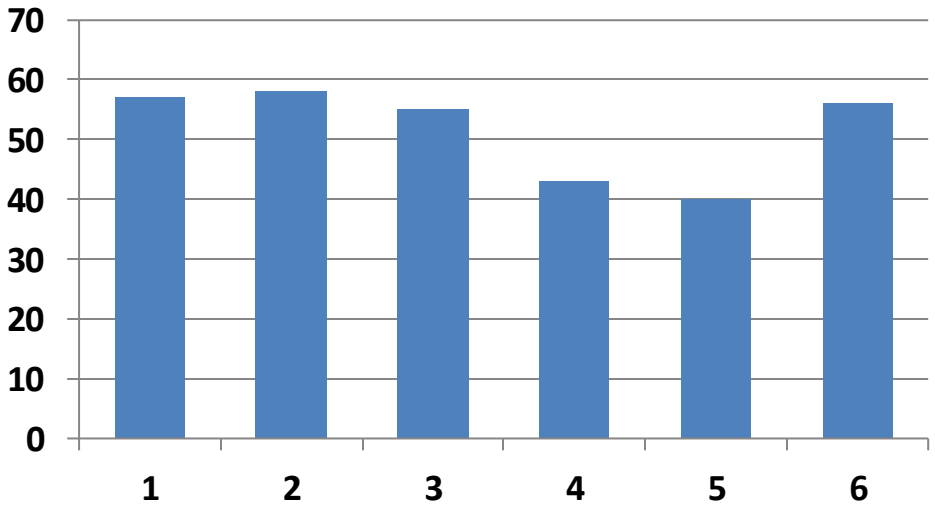
（複数回答なし N = 66）

2.2.9. 具体的な提供サービス

【事後対応型サービス】、【事前対応型サービス】及び【セキュリティ品質管理サービス】のそれぞれについて CSIRT が提供するサービスの内容をたずねた。【事後対応型サービス】として最も多くの CSIRT が提供しているのは「インシデントハンドリング」である。【事前対応型サービス】では、「注意喚起・アナウンス」を提供している CSIRT が多く、インシデントを未然に防止するために広く情報提供をする役割が重視されている。【セキュリティ品質管理サービス】では、「啓発・意識向上活動」、「教育/トレーニング」などのサービスを提供している CSIRT が多く、自組織内に対するセキュリティ意識向上に注力していることが分かる。

2.2.9. 具体的な提供サービス
【事後対応型サービス】

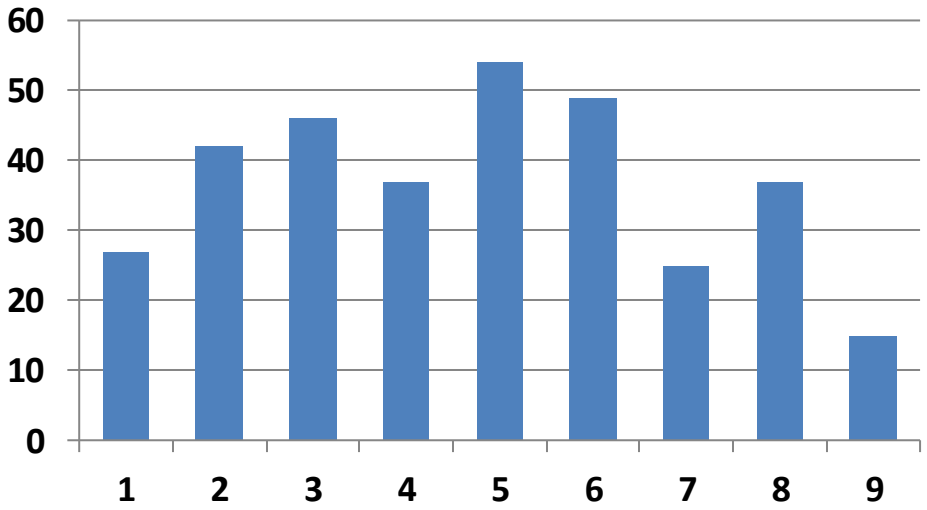
#	提供サービス	回答数
1	アラートと警告	57
2	インデントハンドリング(オンサイト or アドバイス)	58
3	脆弱性ハンドリング(自社製品 or 利用製品・サービス)	55
4	マルウエア解析	43
5	フォレンジック	40
6	ログ分析	56



（複数回答あり N = 66）

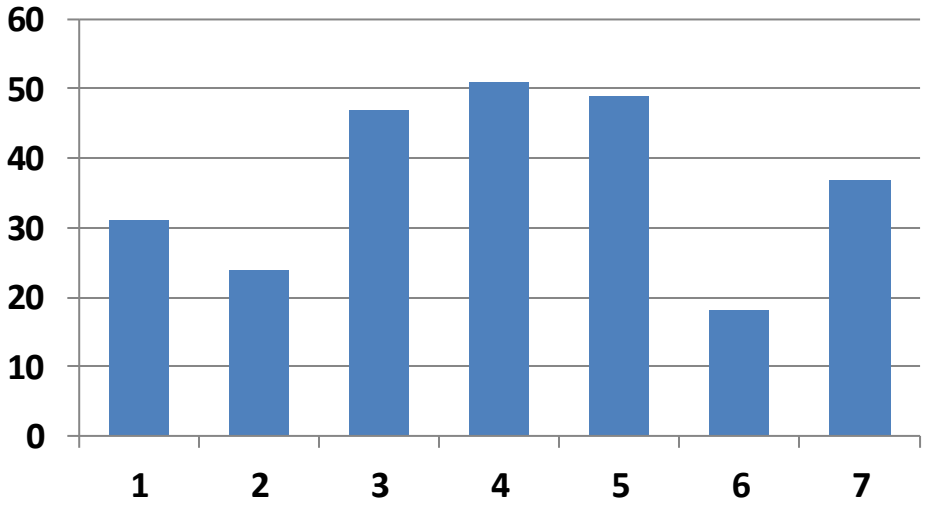
2.2.9. 具体的な提供サービス
【事前対応型サービス】

#	提供サービス	回答数
1	パブリックモニタリング	27
2	セキュリティ動向分析	42
3	侵入検知	46
4	技術動向監視	37
5	注意喚起・アナウンス	54
6	セキュリティ関連情報の提供	49
7	セキュリティ監査または審査	25
8	セキュリティツール、アプリケーション、インフラ、およびサービスの運用	37
9	セキュリティツールの開発(CSIRT が利用するものを含む)	15



（複数回答あり N = 66）

2.2.9. 具体的な提供サービス 【セキュリティ品質管理サービス】		
#	提供サービス	回答数
1	新サービスまたはシステム等のリスク評価への関与	31
2	事業継続と障害復旧計画への関与	24
3	各種セキュリティに関わる相談対応	47
4	啓発・意識向上活動	51
5	教育/トレーニング	49
6	製品の評価または認定	18
7	セキュリティポリシー策定への関与	37



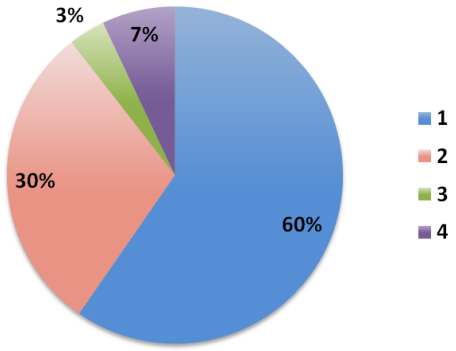
（複数回答あり N = 66）

CSIRT が提供するそれぞれのサービスについて、組織内部での実施（内製）か外部事業者への委託（外注）かの内訳は次のとおりである。

【事後対応型サービス】

2.2.9. 具体的な提供サービス
【事後対応型サービス】
(a) アラートと警告

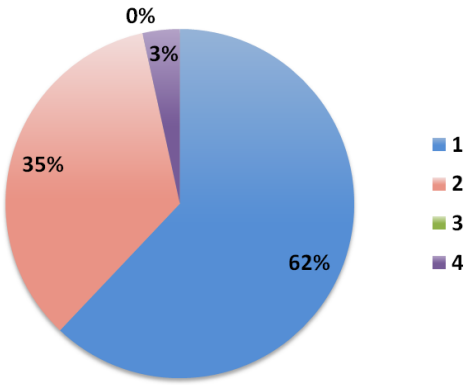
#	内製/外注	回答数
1	主に内製	34
2	内製と外注が半々	17
3	主に外注	2
4	未回答	4



（複数回答なし N = 57）

2.2.9. 具体的な提供サービス
【事後対応型サービス】
(b) インシデントハンドリング（オンサイト or アドバイス）

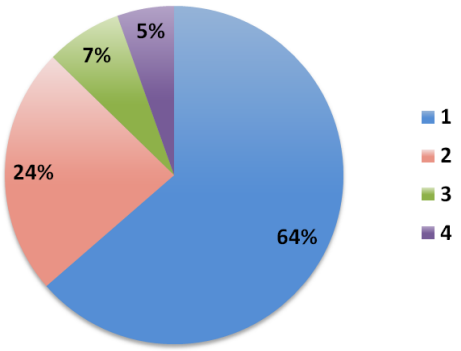
#	内製/外注	回答数
1	主に内製	36
2	内製と外注が半々	20
3	主に外注	0
4	未回答	2



（複数回答なし N = 58）

2.2.9. 具体的な提供サービス
【事後対応型サービス】
(c) 脆弱性ハンドリング（自社製品 or 利用製品・サービス）

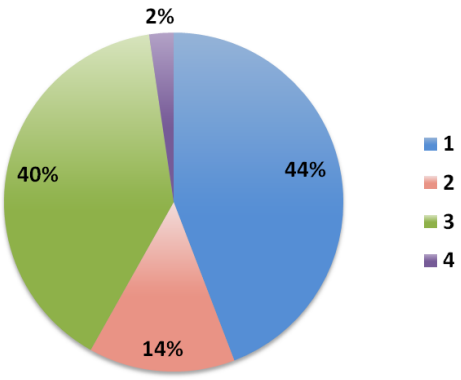
#	内製/外注	回答数
1	主に内製	35
2	内製と外注が半々	13
3	主に外注	4
4	未回答	3



（複数回答なし N = 55）

2.2.9. 具体的な提供サービス
【事後対応型サービス】
(d) マルウエア解析

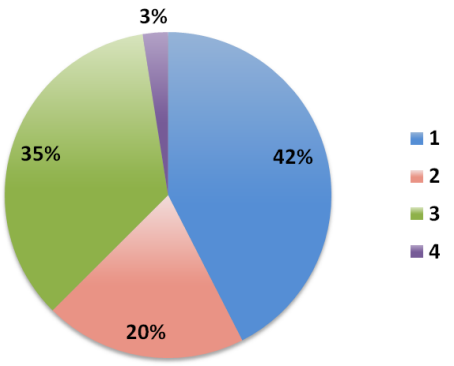
#	内製/外注	回答数
1	主に内製	19
2	内製と外注が半々	6
3	主に外注	17
4	未回答	1



（複数回答なし N = 43）

2.2.9. 具体的な提供サービス
【事後対応型サービス】
(e) フォレンジック

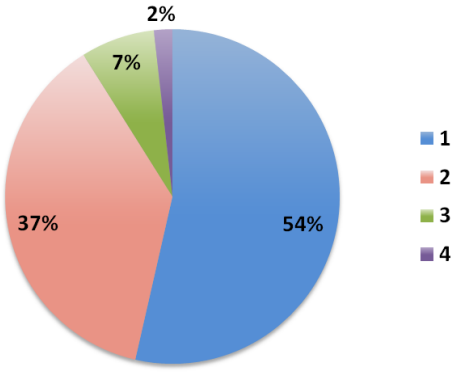
#	内製/外注	回答数
1	主に内製	17
2	内製と外注が半々	8
3	主に外注	14
4	未回答	1



（複数回答なし N = 40）

2.2.9. 具体的な提供サービス
【事後対応型サービス】
(f) ログ分析

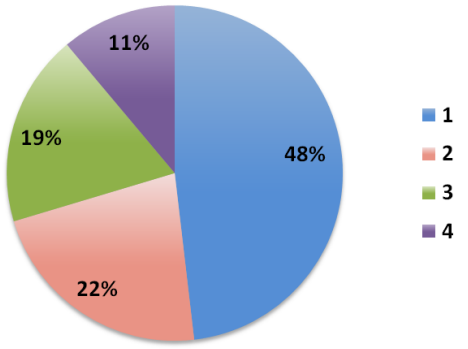
#	内製/外注	回答数
1	主に内製	30
2	内製と外注が半々	21
3	主に外注	4
4	未回答	1



（複数回答なし N = 56）

2.2.9. 具体的な提供サービス
【事前対応型サービス】
(g) パブリックモニタリング

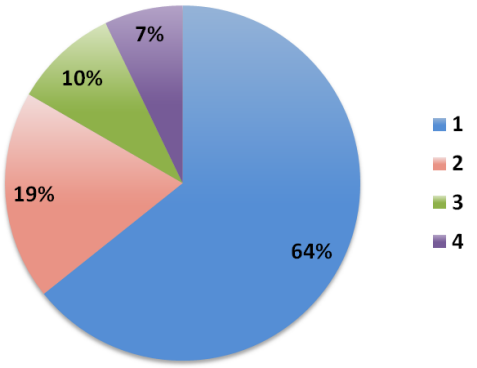
#	内製/外注	回答数
1	主に内製	13
2	内製と外注が半々	6
3	主に外注	5
4	未回答	3



（複数回答なし N = 27）

2.2.9. 具体的な提供サービス
【事前対応型サービス】
(h) セキュリティ動向分析

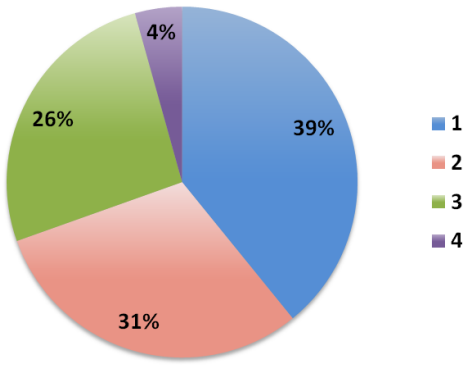
#	内製/外注	回答数
1	主に内製	27
2	内製と外注が半々	8
3	主に外注	4
4	未回答	3



（複数回答なし N = 42）

2.2.9. 具体的な提供サービス
【事前対応型サービス】
(i) 侵入検知

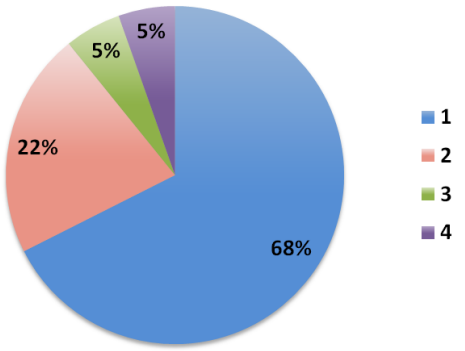
#	内製/外注	回答数
1	主に内製	18
2	内製と外注が半々	14
3	主に外注	12
4	未回答	2



（複数回答なし N = 46）

2.2.9. 具体的な提供サービス
【事前対応型サービス】
(j) 技術動向監視

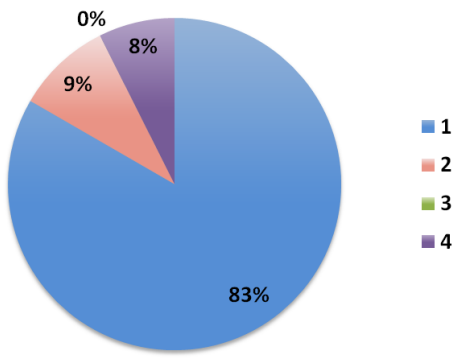
#	内製/外注	回答数
1	主に内製	25
2	内製と外注が半々	8
3	主に外注	2
4	未回答	2



（複数回答なし N = 37）

2.2.9. 具体的な提供サービス
【事前対応型サービス】
(k) 注意喚起・アナウンス

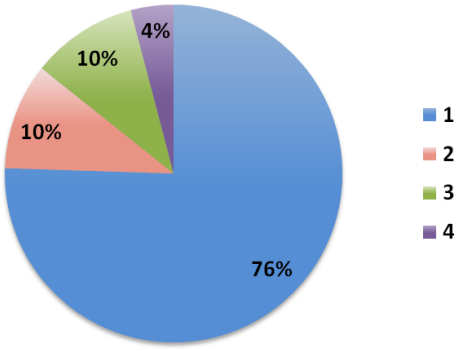
#	内製/外注	回答数
1	主に内製	45
2	内製と外注が半々	5
3	主に外注	0
4	未回答	4



（複数回答なし N = 54）

2.2.9. 具体的な提供サービス
【事前対応型サービス】
(l) セキュリティ関連情報の提供

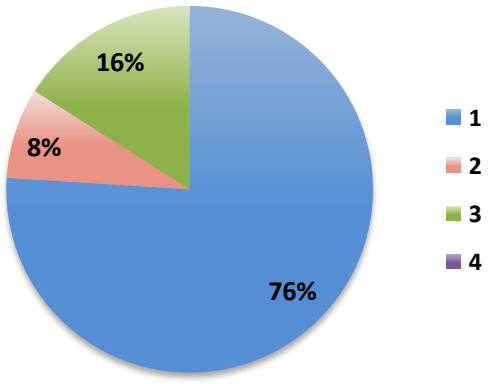
#	内製/外注	回答数
1	主に内製	37
2	内製と外注が半々	5
3	主に外注	5
4	未回答	2



（複数回答なし N = 49）

2.2.9. 具体的な提供サービス
【事前対応型サービス】
(m) セキュリティ監査または審査

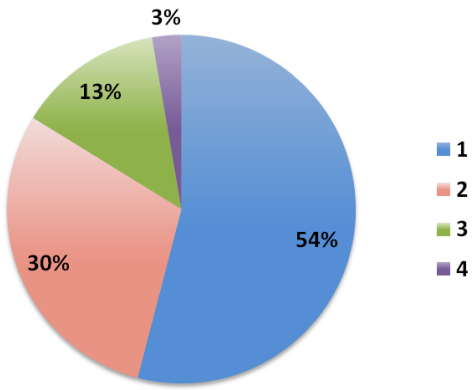
#	内製/外注	回答数
1	主に内製	19
2	内製と外注が半々	2
3	主に外注	4
4	未回答	0



（複数回答なし N = 25）

2.2.9. 具体的な提供サービス
【事前対応型サービス】
(n) セキュリティツール、アプリケーション、インフラ、およびサービスの運用

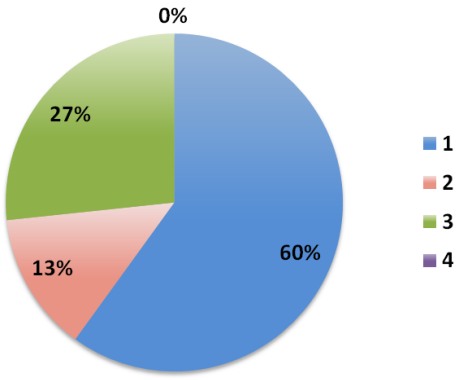
#	内製/外注	回答数
1	主に内製	20
2	内製と外注が半々	11
3	主に外注	5
4	未回答	1



（複数回答なし N = 37）

2.2.9. 具体的な提供サービス
【事前対応型サービス】
(o) セキュリティツールの開発（CSIRT が利用するものを含む）

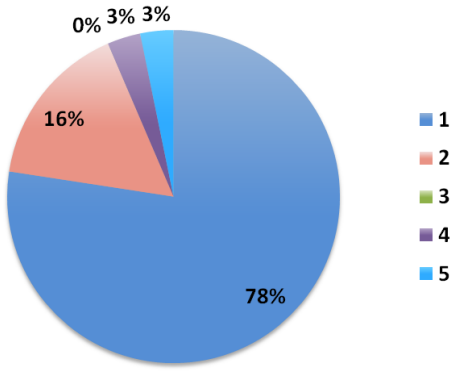
#	内製/外注	回答数
1	主に内製	9
2	内製と外注が半々	2
3	主に外注	4
4	未回答	0



（複数回答なし N = 15）

2.2.9. 具体的な提供サービス
【セキュリティ品質管理サービス】
(p) 新サービスまたはシステム等のリスク評価への関与

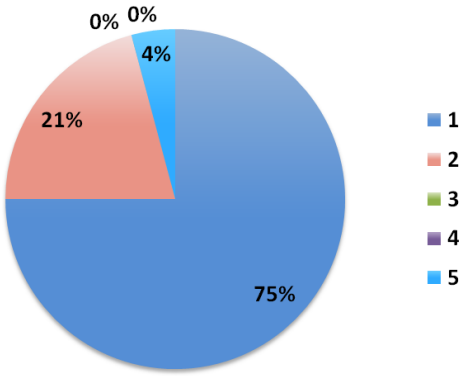
#	内製/外注	回答数
1	主に内製	24
2	内製と外注が半々	5
3	主に外注	0
4	別組織が対応	1
5	未回答	1



（複数回答なし N = 31）

2.2.9. 具体的な提供サービス
【セキュリティ品質管理サービス】
(q) 事業継続と障害復旧計画への関与

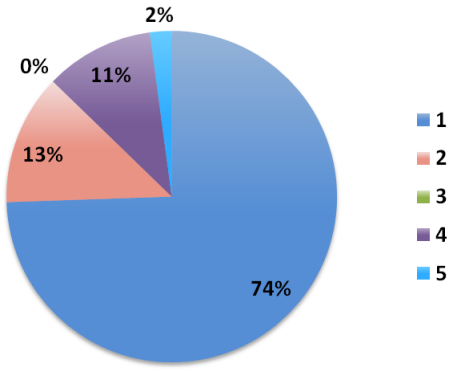
#	内製/外注	回答数
1	主に内製	18
2	内製と外注が半々	5
3	主に外注	0
4	別組織が対応	1
5	未回答	0



（複数回答なし N = 24）

2.2.9. 具体的な提供サービス
【セキュリティ品質管理サービス】
(r) 各種セキュリティに関わる相談対応

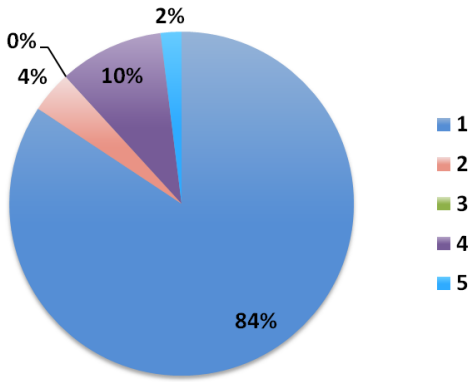
#	内製/外注	回答数
1	主に内製	35
2	内製と外注が半々	6
3	主に外注	0
4	別組織が対応	1
5	未回答	5



（複数回答なし N = 47）

2.2.9. 具体的な提供サービス
【セキュリティ品質管理サービス】
(s) 啓発・意識向上活動

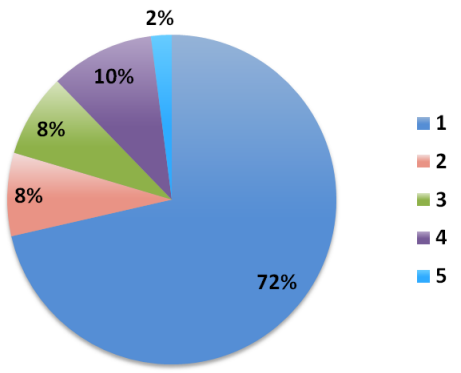
#	内製/外注	回答数
1	主に内製	43
2	内製と外注が半々	2
3	主に外注	0
4	別組織が対応	1
5	未回答	5



（複数回答なし N = 51）

2.2.9. 具体的な提供サービス
【セキュリティ品質管理サービス】
(t) 教育／トレーニング

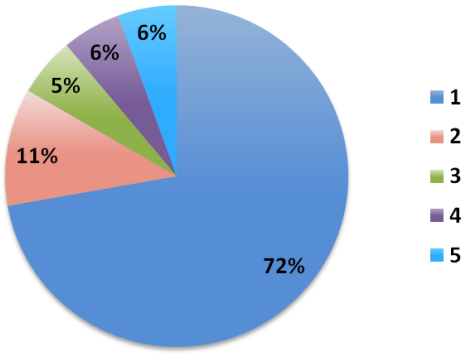
#	内製/外注	回答数
1	主に内製	35
2	内製と外注が半々	4
3	主に外注	4
4	別組織が対応	1
5	未回答	5



（複数回答なし N = 49）

2.2.9. 具体的な提供サービス
【セキュリティ品質管理サービス】
(u) 製品の評価または認定

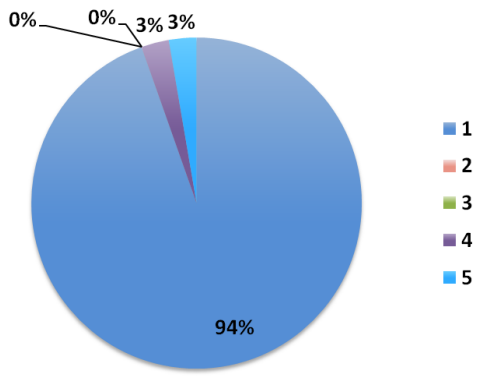
#	内製/外注	回答数
1	主に内製	13
2	内製と外注が半々	2
3	主に外注	1
4	別組織が対応	1
5	未回答	1



（複数回答なし N = 18）

2.2.9. 具体的な提供サービス
【セキュリティ品質管理サービス】
(v) セキュリティポリシー策定への関与

#	内製/外注	回答数
1	主に内製	35
2	内製と外注が半々	0
3	主に外注	0
4	別組織が対応	1
5	未回答	1



（複数回答なし N = 37）

【事後対応型サービス】、【事前対応型サービス】、【セキュリティ品質管理サービス】以外の提供サービスとして 1 組織が『脆弱性診断（主に内製)』を挙げた。

2.2.9. 具体的な提供サービス
【その他】

(w) その他

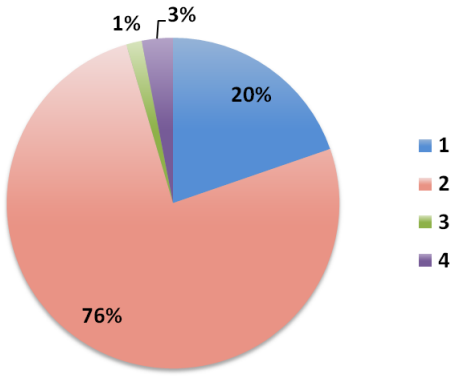
1	脆弱性診断(主に内製)	1

2.2.10. サービスレベルの定義はあるか

多くの CSIRT がサービスレベルを定義していない。

2.2.10. サービスレベルの定義はあるか

#	定義の有無	回答数
1	ある	13
2	ない	50
3	その他自由記述	1
4	未回答	2

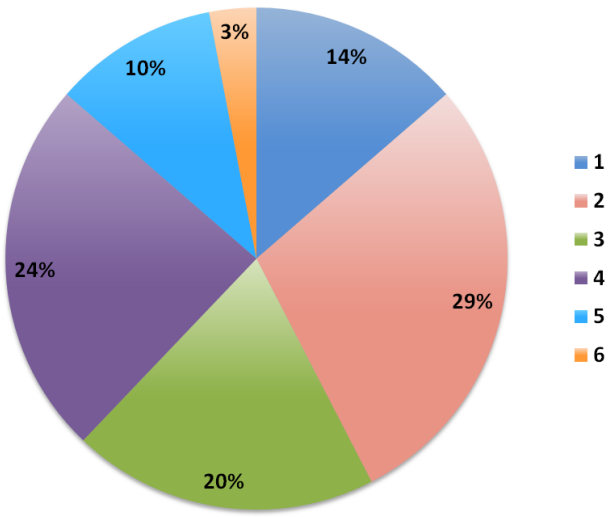


（複数回答なし N = 66）

2.2.11. 報告を受けたインシデントについて分類を定義している

文書化しないまでも、報告を受けたインシデントについての分類をあらかじめ定めている組織が多く、分類ごとにインシデント対応を実施している。

2.2.11. 報告を受けたインシデントについて分類を定義している		
#	定義や文書の有無	回答数
1	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	9
2	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	19
3	明確に設定され、文書として存在しているが、正式に承認されていない	13
4	だいたいの目安になるものは設定されているが、文書として存在していない	16
5	設定されておらず、発生の都度検討している	7
6	未回答	2



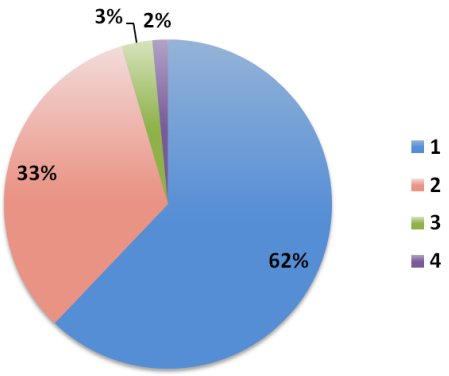
（複数回答なし N = 66）

2.2.12. CSIRT のサービス対象者や権限、サービス、インシデントの定義等が文書化されている

多くの CSIRT が役割やインシデントの定義等について文書化している。自由記述の 2 件についても「作成中」との回答であった。

2.2.12. CSIRT のサービス対象者や権限、サービス、インシデントの定義等が文書化されている

#	文書化の有無	回答数
1	されている	41
2	されていない	22
3	その他自由記述	2
4	未回答	1

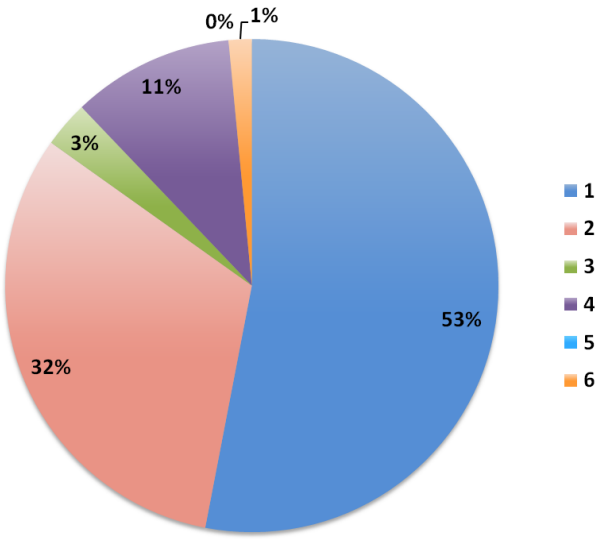


（複数回答なし N = 66）

2.2.13. セキュリティポリシーについて定義している

多くの組織がセキュリティポリシーを文書化している。ポリシーの統一・運用が実施されていることもわかる。

2.2.13. セキュリティポリシーについて定義している		
#	定義や文書の有無	回答数
1	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	35
2	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	21
3	明確に設定され、文書として存在しているが、正式に承認されていない	2
4	だいたいの目安になるものは設定されているが、文書として存在していない	7
5	設定されておらず、発生の都度検討している	0
6	未回答	1

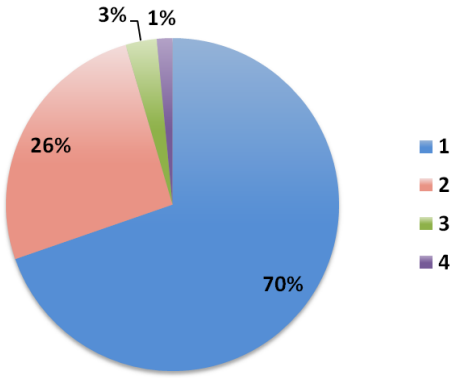


（複数回答なし N = 66）

2.2.14. SOC による監視体制が運用・構築されているか

多くの組織が、SOC による監視体制を運用・構築している。

2.2.14. SOC による監視体制が運用・構築されている		
#	SOC による監視体制の有無	回答数
1	構築・運用している	46
2	構築・運用していない	17
3	構築検討中	1
4	未回答	2

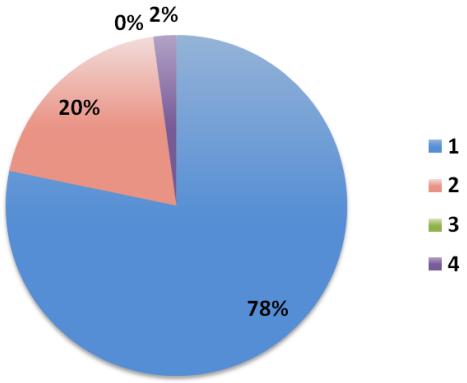


（複数回答なし N = 66）

2.2.14.1. SOC の監視体制はどのようなものか

設置されている場合には、ほとんどの SOC が 24 時間 365 日の体制で運用されている。

2.2.14.1. SOC の監視体制はどのようなものか		
#	監視体制	回答数
1	24 時間 365 日	36
2	平日日勤帯のみ	9
3	その他自由記述	0
4	他社は「24 時間 365 日」。グループ会社は「平日日勤帯のみ」	1



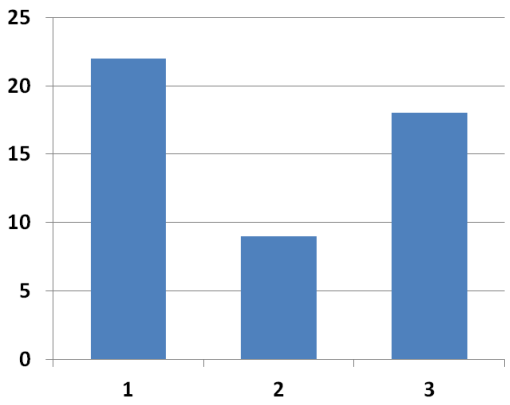
（複数回答なし N = 46）

2.2.14.2. SOC の運用体制はどのようなものか

SOC を運用している組織の半数弱が自組織で運用しており、それ以外はグループ会社もしくは他社に外注している。

2.2.14.2. SOC の監視体制はどのようなものか

#	監視体制	回答数
1	自組織で運用している	22
2	グループ会社に外注している	9
3	他社に外注している	18



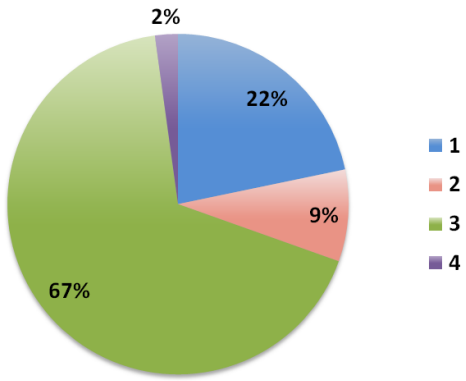
（複数回答あり N = 46）

2.2.14.3. SOC と CSIRT の関係はどのように位置づけられているか

SOC と CSIRT とを切り離して運用している組織が多い。

2.2.14.3. SOC の監視体制はどのようなものか

#	位置づけ	回答数
1	CSIRT が SOC 機能を有している	10
2	SOC 内に CSIRT を構築している	4
3	それぞれが独立した部署として存在しており、連携している	31
4	未回答	1



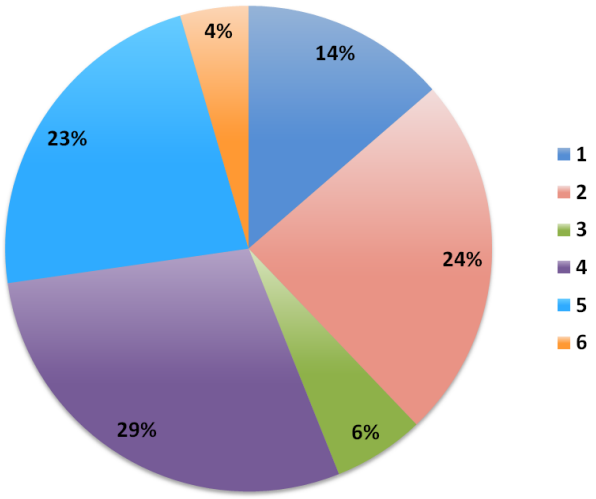
（複数回答なし N = 66）

2.3. CSIRT メンバー

2.3.1. CSIRT メンバーの行動規範や指針が定められているか

明確に文書化されていないまでも、多くの CSIRT が CSIRT メンバーの行動規範や指針を定められている。

2.3.1. CSIRT メンバーの行動規範や指針が定められているか		
#	定義や文書の有無	回答数
1	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	9
2	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	16
3	明確に設定され、文書として存在しているが、正式に承認されていない	4
4	だいたいの目安になるものは設定されているが、文書として存在していない	19
5	設定されておらず、発生の都度検討している	15
6	未回答	3



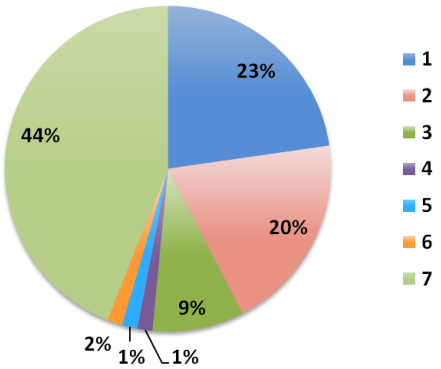
（複数回答なし N = 66）

2.3.2. 設立当初のメンバー数

設立時のメンバー数は、5 名未満の CSIRT が最も多く、未回答を除くと 10 名未満の CSIRT が半数以上を占めている。

2.3.2. 設立当初のメンバー数

#	人数	回答数
1	5 名未満	15
2	5 名以上 10 名未満	13
3	10 名以上 20 名未満	6
4	20 名以上	1
5	バーチャルなので流動性あり	1
6	不明	1
7	未回答	29



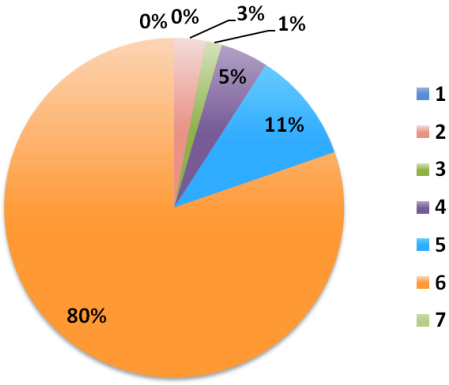
（複数回答なし N = 66）

2.3.2.1. 正社員と外部委託のメンバーの割合

正社員と外部委託メンバーの内訳は、設立時の CSIRT のメンバーをすべて正社員で構成している組織が多い。すべてを外部委託した組織はなかった。

2.3.2.1. 正社員と外部委託のメンバーの割合

#	割合	回答数
1	すべて外部委託	0
2	正社員 2 割以下	2
3	正社員 2 割～4 割	1
4	正社員 4 割～7 割	3
5	正社員 8 割以上	7
6	すべて正社員	53
7	未回答	0



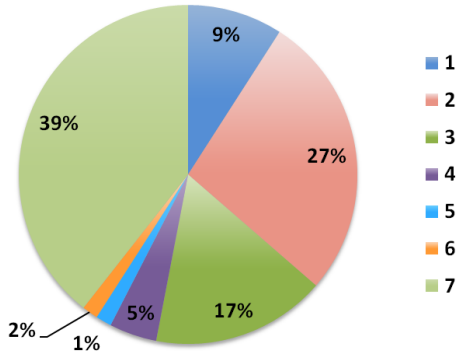
（複数回答なし N = 66）

2.3.3. 現在のメンバー数

現在のメンバー数は、5 名以上 10 名未満の CSIRT が最も多く、ほとんどの CSIRT が 20 名未満のメンバーで構成されている。

2.3.3. 現在のメンバー数

#	人数	回答数
1	5 名未満	6
2	5 名以上 10 名未満	18
3	10 名以上 20 名未満	11
4	20 名以上	3
5	5～20	1
6	バーチャルなので流動性あり	1
7	未回答	26



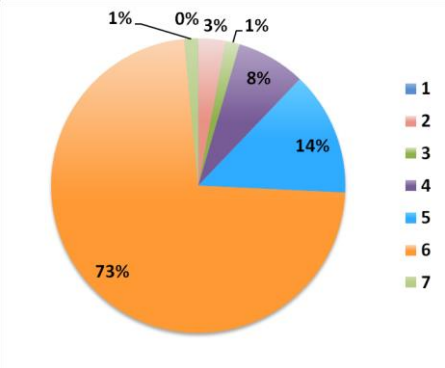
（複数回答なし N = 66）

2.3.3.1. 正社員と外部委託のメンバーの割合

現在の CSIRT のメンバーをすべて正社員で構成している組織が多い。
すべてを外部委託している組織はなかった。

2.3.3.1. 正社員と外部委託のメンバーの割合

#	割合	回答数
1	すべて外部委託	0
2	正社員 2 割以下	2
3	正社員 2 割～4 割	1
4	正社員 4 割～7 割	5
5	正社員 8 割以上	9
6	すべて正社員	48
7	未回答	1

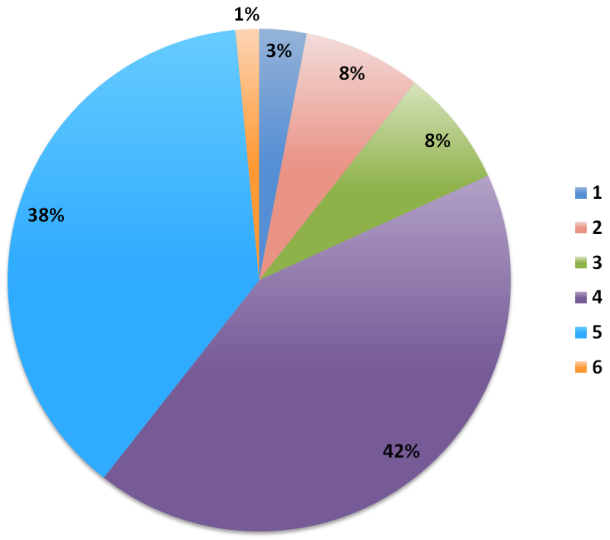


（複数回答なし N = 66）

2.3.4. CSIRT メンバーに必要なスキルセットが定義されているか

CSIRT メンバーに必要なスキルセットを設定している組織は少数で、スキル水準の目安を設けたり、その都度、判断したりしている組織が多い。

2.3.4. CSIRT メンバーに必要なスキルセットが定義されているか		
#	定義や文書の有無	回答数
1	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	2
2	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	5
3	明確に設定され、文書として存在しているが、正式に承認されていない	5
4	だいたいの目安になるものは設定されているが、文書として存在していない	28
5	設定されておらず、発生の都度検討している	25
6	未回答	1



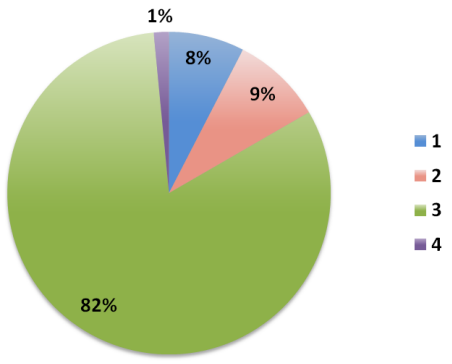
（複数回答なし N = 66）

2.3.5. CSIRT メンバー向けに組織内部で提供されているトレーニングを受講できる体制やルールが確立されているか

CSIRT のメンバーが参加する組織内トレーニングを明確に規定している組織は全体から見れば少なく、多くの組織がその都度、誰をどのトレーニングに参加させるべきかを判断している。

2.3.5. CSIRT メンバー向けに組織内部で提供されているトレーニングを受講できる体制やルールが確立されているか

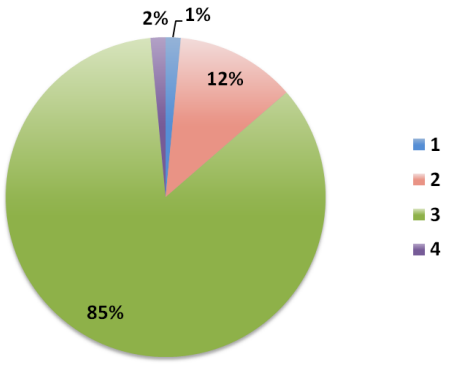
#	基準の有無	回答数
1	CSIRT メンバーが参加するトレーニングについて、明確な基準が存在する	5
2	CSIRT メンバーが参加するトレーニングについて、だいたいの目安になる基準は存在する	6
3	CSIRT メンバーが参加するトレーニングについて、基準が確立しておらず、受講の都度検討している	54
4	未回答	1



（複数回答なし N = 66）

2.3.6. CSIRT メンバー向けに外部の技術トレーニングを受講できる体制が確立されているか

CSIRT のメンバーが参加する組織外トレーニングを明確に規定している組織は少ない。その都度、組織外トレーニングの受講を判断している。

2.3.6. CSIRT メンバー向けに外部の技術トレーニングを受講できる体制が確立されているか			
#	基準の有無	回答数	
1	CSIRT メンバーが参加するトレーニングについて、明確な基準が存在する	1	
2	CSIRT メンバーが参加するトレーニングについて、だいたいの目安になる基準は存在する	8	
3	CSIRT メンバーが参加するトレーニングについて、基準が確立しておらず、受講の都度検討している	56	
4	未回答	1	

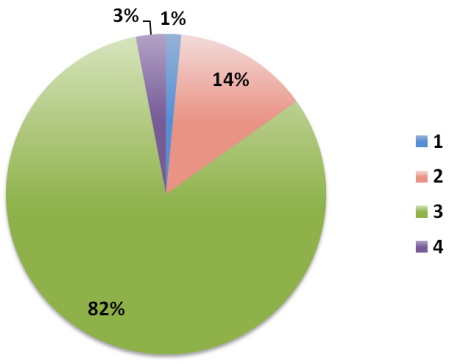
（複数回答なし N = 66）

2.3.7. CSIRT メンバー向けに外部のコミュニケーショントレーニングを受講できる体制が確立されているか（プレゼンテーションやコミュニケーションスキルに関するトレーニング）

明確な規定がある CSIRT は少ない。その都度の判断によっている。

2.3.7. CSIRT メンバー向けに外部のコミュニケーショントレーニングを受講できる体制が確立されているか（プレゼンテーションやコミュニケーションスキルに関するトレーニング）

#	基準の有無	回答数
1	CSIRT メンバーが参加するトレーニングについて、明確な基準が存在する	1
2	CSIRT メンバーが参加するトレーニングについて、だいたいの目安になる基準は存在する	9
3	CSIRT メンバーが参加するトレーニングについて、基準が確立しておらず、受講の都度検討している	54
4	未回答	2



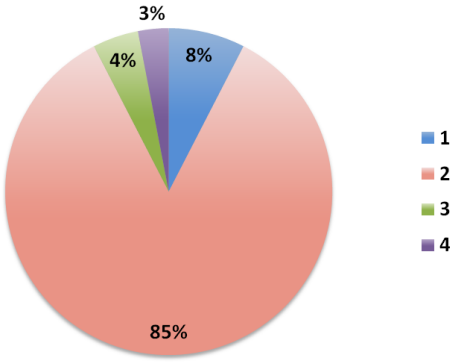
（複数回答なし N = 66）

2.3.8. メンバーのスキルを定量的に測定する仕組み（試験や資格など）があるか

CSIRT のメンバーのスキルを定量的に測定する仕組みを有している組織は少ない。なお自由記述の回答では「外部資格（CISM etc）」と回答した組織があった。

2.3.8. メンバーのスキルを定量的に測定する仕組み（試験や資格など）があるか

#	仕組みの有無	回答数
1	ある	5
2	ない	56
3	その他自由記述	3
4	未回答	2



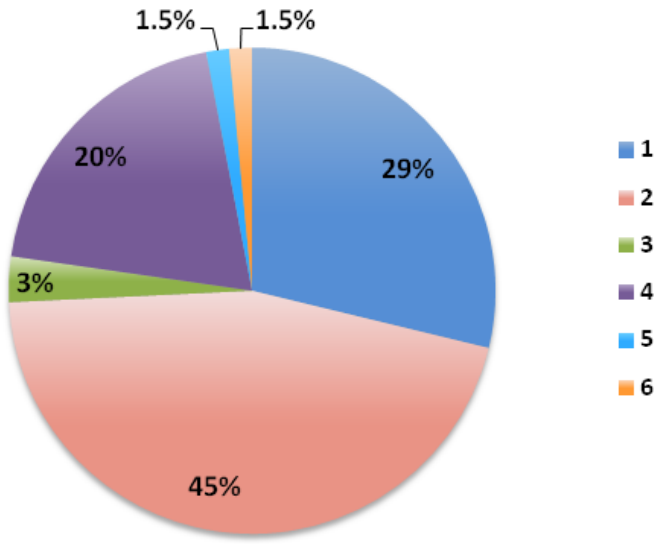
（複数回答なし N = 66）

2.4. プロセスやルール

2.4.1. 経営層（あるいは経営層を含む情報セキュリティ委員会等）へのエスカレーションルールは設定されているか

経営層へのエスカレーションルールが明確に設定され、それを文書化している組織が多い。

2.4.1. 経営層（あるいは経営層を含む情報セキュリティ委員会等）へのエスカレーションルールは設定されているか		
#	定義や文書の有無	回答数
1	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	19
2	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	30
3	明確に設定され、文書として存在しているが、正式に承認されていない	2
4	だいたいの目安になるものは設定されているが、文書として存在していない	13
5	設定されておらず、発生の都度検討している	1
6	未回答	1

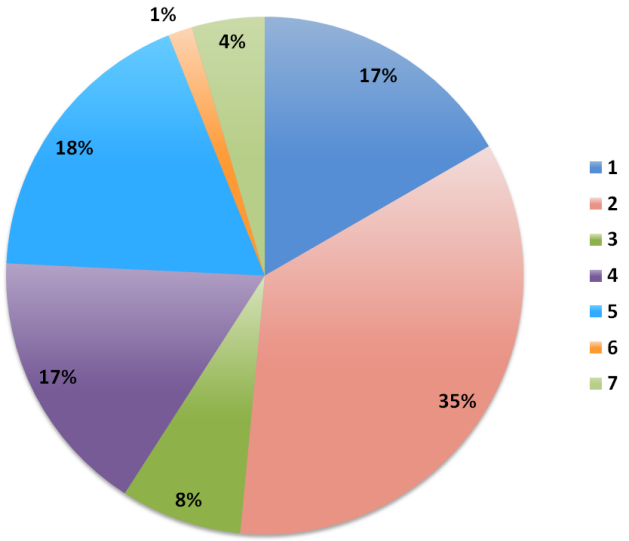


（複数回答なし N = 66）

2.4.2. 広報部門へのエスカレーションルールは設定されているか

広報部門へのエスカレーションルールが明確に設定され、それを文書化している組織が多い。

2.4.2. 広報部門へのエスカレーションルールは設定されているか		
#	定義や文書の有無	回答数
1	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	11
2	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	23
3	明確に設定され、文書として存在しているが、正式に承認されていない	5
4	だいたいの目安になるものは設定されているが、文書として存在していない	11
5	設定されておらず、発生の都度検討している	12
6	CSIRT メンバーであり常に共有している	1
7	未回答	3

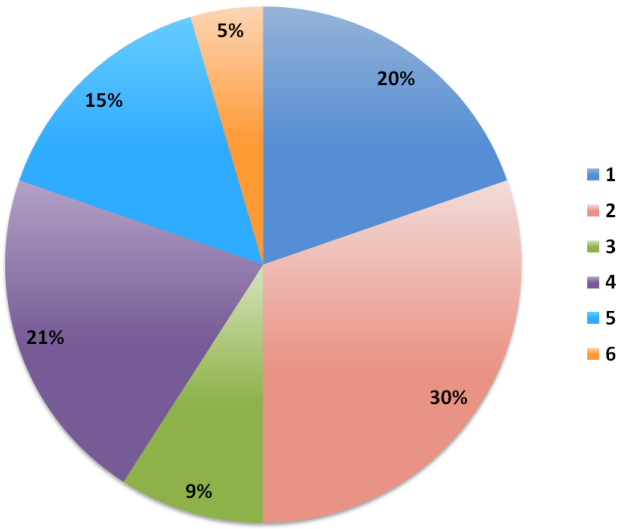


（複数回答なし N = 66）

2.4.3. 法務部門へのエスカレーションルールは設定されているか

法務部門へのエスカレーションルールが明確に設定され、それを文書化している組織が多い。

2.4.3. 法務部門へのエスカレーションルールは設定されているか		
#	定義や文書の有無	回答数
1	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	13
2	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	20
3	明確に設定され、文書として存在しているが、正式に承認されていない	6
4	だいたいの目安になるものは設定されているが、文書として存在していない	14
5	設定されておらず、発生の都度検討している	10
6	未回答	3

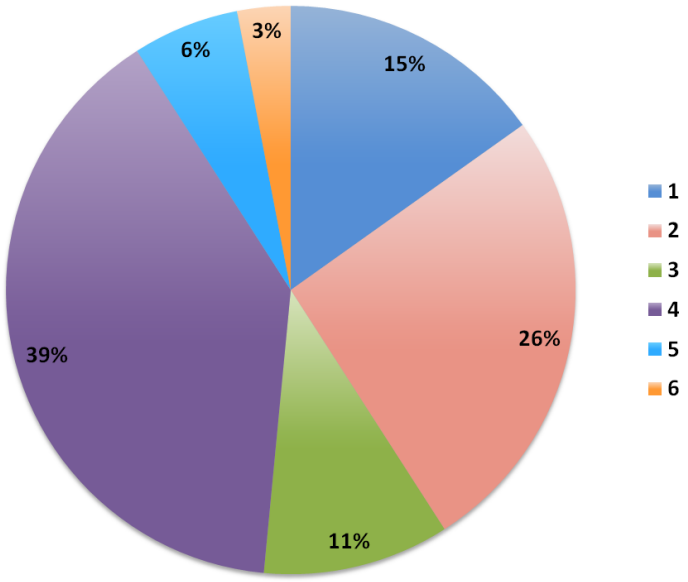


（複数回答なし N = 66）

2.4.4. インシデントを防止、検知、解決するためのプロセスが定められているか

インシデントを防止、検知、解決するためのプロセスについては、文書化されないまでも、インシデント発生から収束に到るまでの対応プロセスを定めている組織が多い。

2.4.4. インシデントを防止、検知、解決するためのプロセスが定められているか		
#	定義や文書の有無	回答数
1	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	10
2	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	17
3	明確に設定され、文書として存在しているが、正式に承認されていない	7
4	だいたいの目安になるものは設定されているが、文書として存在していない	26
5	設定されておらず、発生の都度検討している	4
6	未回答	2

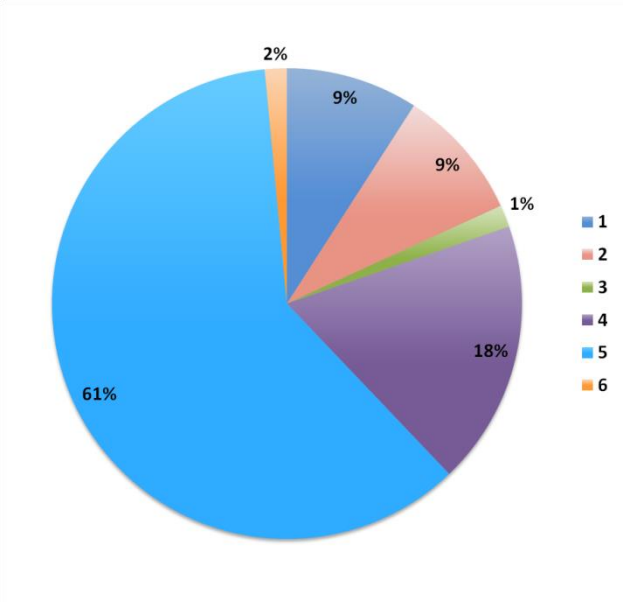


（複数回答なし N = 66）

2.4.5. CSIRT の活動が内部評価や外部評価によって監査され、フィードバックを受ける体制が定められているか

CSIRT の活動の内部評価や外部評価について、明確に定めている組織は少ない。

2.4.5. CSIRT の活動が内部評価や外部評価によって監査され、フィードバックを受ける体制が定められているか		
#	定義や文書の有無	回答数
1	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	6
2	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	6
3	明確に設定され、文書として存在しているが、正式に承認されていない	1
4	だいたいの目安になるものは設定されているが、文書として存在していない	12
5	設定されておらず、発生の都度検討している	40
6	未回答	1

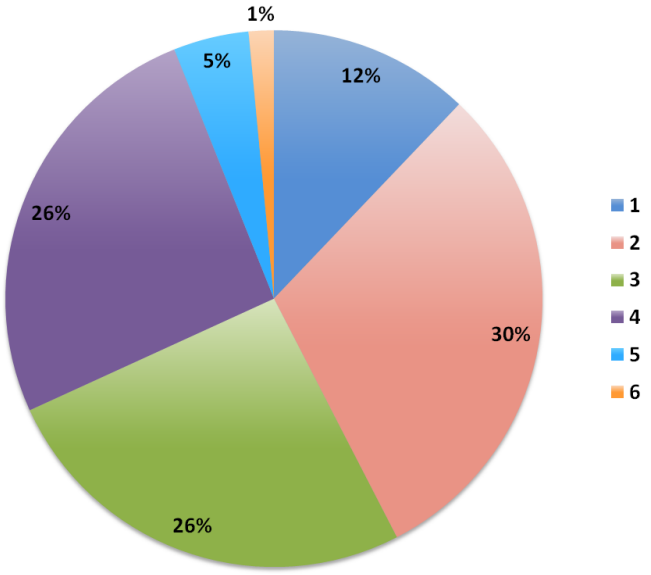


（複数回答なし N = 66）

2.4.6. 緊急時に備えて、CSIRT メンバーや関連する担当者間の連絡網が整備されているか

半数以上の CSIRT が、緊急時に備えて、CSIRT メンバーや関連する担当者間の連絡網を整備している。

2.4.6. 緊急時に備えて、CSIRT メンバーや関連する担当者間の連絡網が整備されているか		
#	定義や文書の有無	回答数
1	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	8
2	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	20
3	明確に設定され、文書として存在しているが、正式に承認されていない	17
4	だいたいの目安になるものは設定されているが、文書として存在していない	17
5	設定されておらず、発生の都度検討している	3
6	未回答	1



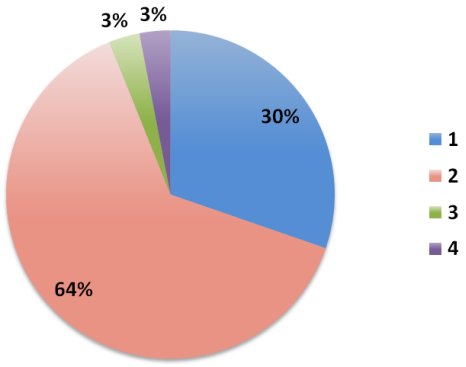
（複数回答なし N = 66）

2.4.7. CSIRT の目的やサービスについて説明した WEB ページが自社のサイト内に存在するか

CSIRT の目的やサービスについて説明した Web ページを自社のサイトに掲載している組織は 3 割程度である。

2.4.7. CSIRT の目的やサービスについて説明した Web ページが自社のサイト内に存在するか

#	存在の有無	回答数
1	存在する	20
2	存在しない	42
3	その他自由記述	2
4	未回答	2

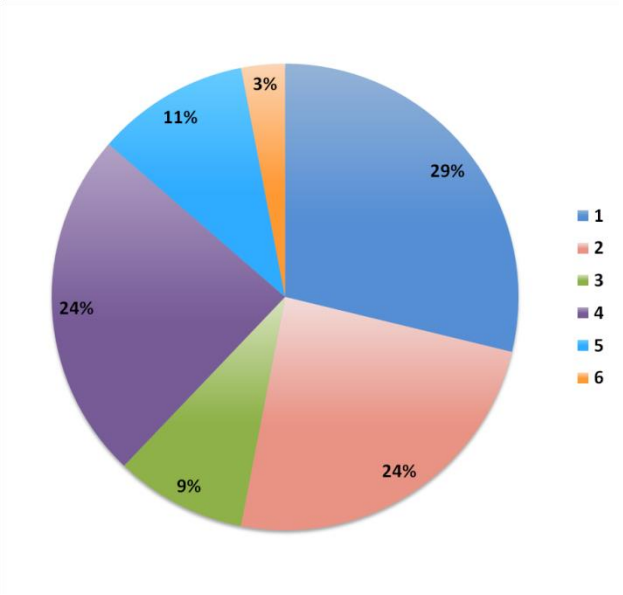


（複数回答なし N = 66）

2.4.8. 機微な内容を含むインシデントレポートや情報の取り扱い方法について定められているか

機微な内容を含むインシデントレポートや情報の取り扱い方法については、明確に定め、文書化している組織が半数を超えており、重要度が高い情報を適切に取り扱っている。

2.4.8. 機微な内容を含むインシデントレポートや情報の取り扱い方法について定められているか		
#	定義や文書の有無	回答数
1	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	19
2	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	16
3	明確に設定され、文書として存在しているが、正式に承認されていない	6
4	だいたいの目安になるものは設定されているが、文書として存在していない	16
5	設定されておらず、発生の都度検討している	7
6	未回答	2

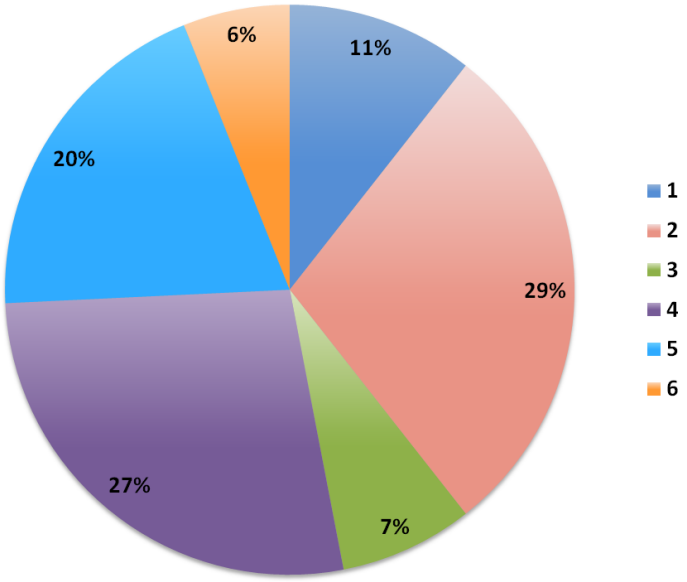


（複数回答なし N = 66）

2.4.9. 経営層（あるいは経営層を含む情報セキュリティ委員会等）に CSIRT 活動について定期的に報告を行う体制が定められているか

約半数の組織において、経営層を含む情報セキュリティ委員会等への定期的な活動報告が義務付けられている。

2.4.9. 経営層（あるいは経営層を含む情報セキュリティ委員会等）に CSIRT 活動について定期的に報告を行う体制が定められているか		
#	定義や文書の有無	回答数
1	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	7
2	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	19
3	明確に設定され、文書として存在しているが、正式に承認されていない	5
4	だいたいの目安になるものは設定されているが、文書として存在していない	18
5	設定されておらず、発生の都度検討している	13
6	未回答	4

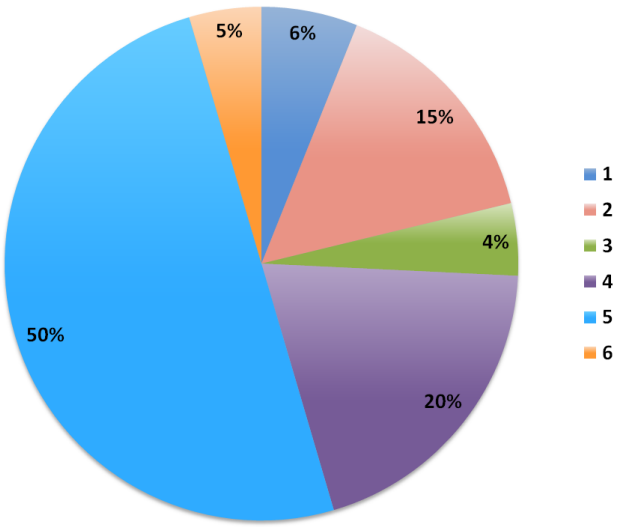


（複数回答なし N = 66）

2.4.10. 分類されたインシデントについて統計的な処理のうえ、サービス対象者等に開示するルール等が定められているか

発生したインシデントを分類し、統計情報としてサービス対象者等に開示するよう義務付けられたCSIRTは半数に満たない。半数の CSIRT は発生の都度、検討している。

2.4.10. 分類されたインシデントについて統計的な処理のうえ、サービス対象者等に開示するルール等が定められているか		
#	定義や文書の有無	回答数
1	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	4
2	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	10
3	明確に設定され、文書として存在しているが、正式に承認されていない	3
4	だいたいの目安になるものは設定されているが、文書として存在していない	13
5	設定されておらず、発生の都度検討している	33
6	未回答	3

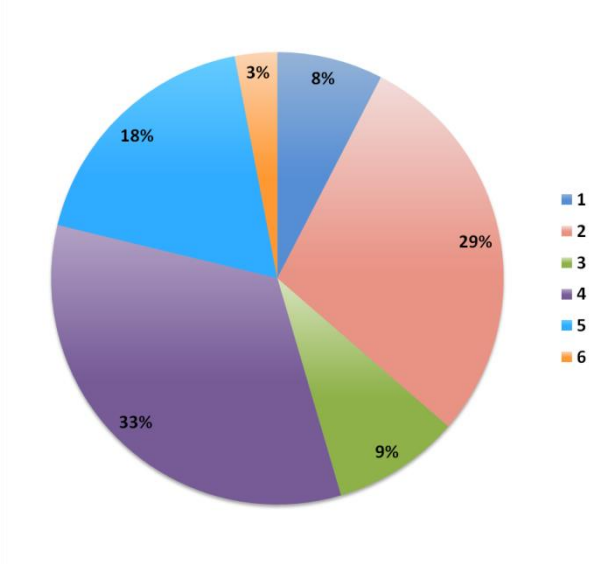


（複数回答なし N = 66）

2.4.11. CSIRT において定期的な打合せが定められているか

文書化しないまでも、CSIRT において定期的な打ち合わせを実施している組織が多く、CSIRT 内での情報共有がなされている。

2.4.11. CSIRT において定期的な打ち合わせを実施する体制が定められているか		
#	定義や文書の有無	回答数
1	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	5
2	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	19
3	明確に設定され、文書として存在しているが、正式に承認されていない	6
4	だいたいの目安になるものは設定されているが、文書として存在していない	22
5	設定されておらず、発生の都度検討している	12
6	未回答	2



（複数回答なし N = 66）

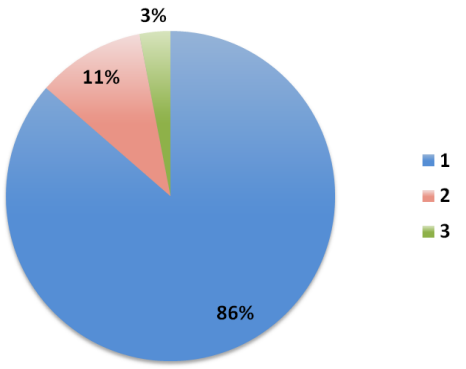
2.5. ツールについて

2.5.1. IT 資産の管理を組織的に実施しているか

情報や IT 資産の管理方法を組織として定め、それに従った管理を適切に行っている組織が 8 割以上を占めている。

2.5.1. IT 資産の管理を組織的に実施しているか

#	実施の有無	回答数
1	実施している	57
2	実施していない	7
3	未回答	2



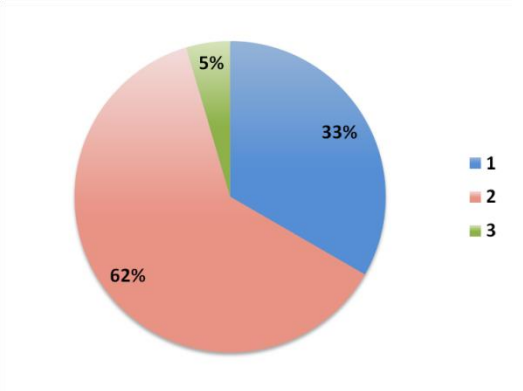
（複数回答なし N = 66）

2.5.2. インシデント対応を追跡するためトラッキングシステムやワークフローを導入している

インシデント対応を追跡するためトラッキングシステムやワークフローを導入している CSIRT は 3 割程度である。

2.5.2. インシデント対応を追跡するためトラッキングシステムやワークフローを導入している

#	導入の有無	回答数
1	導入している	22
2	導入していない	41
3	未回答	3



（複数回答なし N = 66）

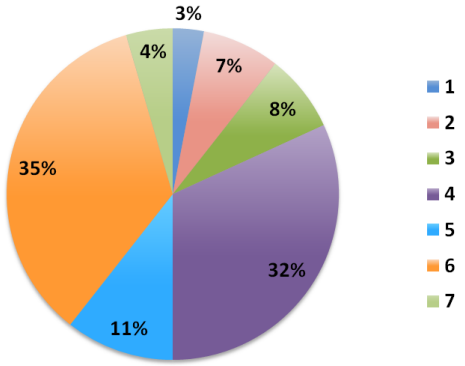
2.6. 体制やルールの見直し

2.6.1. 定期的にサービスの提供範囲の見直しを実施しているか

半数以上の CSIRT では、年に 1 回以上の頻度でサービスの提供範囲を見直している。

2.6.1. 定期的にサービスの提供範囲の見直しを実施しているか

#	周期	回答数
1	月に 1 回以上実施	2
2	四半期に 1 回	5
3	半年に 1 回	5
4	年に 1 回	21
5	年に 1 回未満	7
6	実施していない	23
7	未回答	3



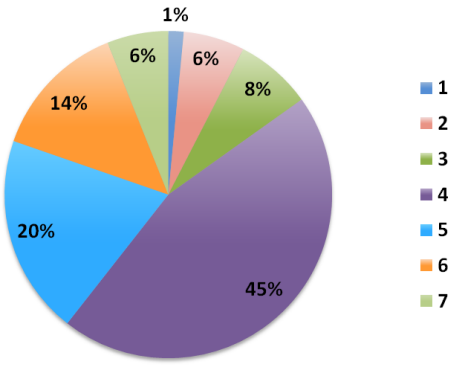
（複数回答なし N = 66）

2.6.2. 定期的にセキュリティポリシー等の文書の見直しを実施しているか

過半数の CSIRT が年に 1 回以上の頻度でセキュリティポリシーを見直している。

2.6.2. 定期的にセキュリティポリシー等の文書の見直しを実施しているか

#	周期	回答数
1	月に 1 回以上実施	1
2	四半期に 1 回	4
3	半年に 1 回	5
4	年に 1 回	30
5	年に 1 回未満	13
6	実施していない	9
7	未回答	4



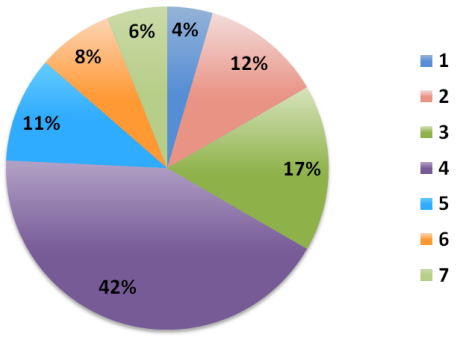
（複数回答なし N = 66）

2.6.3. 定期的に連絡体制図（メールアドレスや電話番号等）の見直しを実施しているか

7 割以上の CSIRT が年に 1 回以上の頻度で連絡体制図を見直している。

2.6.3. 定期的に連絡体制図（メールアドレスや電話番号等）の見直しを実施しているか

#	周期	回答数
1	月に 1 回以上実施	3
2	四半期に 1 回	8
3	半年に 1 回	11
4	年に 1 回	28
5	年に 1 回未満	7
6	実施していない	5
7	未回答	4



（複数回答なし N = 66）

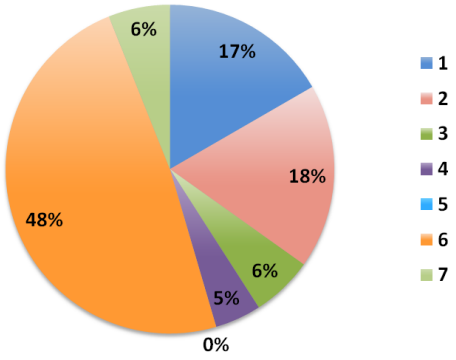
2.7. レポート

2.7.1. 定期的にレポートを発行しているか

半数程度の CSIRT が定期レポートを発行しており、月に 1 回以上の頻度で発行しているケースが最も多い。

2.7.1. 定期的にレポートを発行しているか

#	周期	回答数
1	月に 1 回以上実施	11
2	四半期に 1 回	12
3	半年に 1 回	4
4	年に 1 回	3
5	年に 1 回未満	0
6	実施していない	32
7	未回答	4



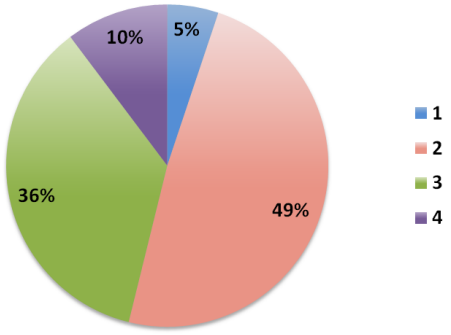
（複数回答なし N = 66）

2.7.1.1. レポートの公開範囲

半数程度の CSIRT がレポートを関連部署内に限って開示している。

2.7.1.1. レポートの公開範囲

#	公開範囲	回答数
1	担当内	2
2	関連部署内	19
3	社内全体	14
4	未回答	4



（複数回答なし N = 39）

3. NCA 参加 CSIRT へのインタビュー結果

3.1. ASY-CSIRT へのインタビュー

ASY-CSIRT		
組織名		ANA システムズ株式会社
事業分野		空運業
CSIRT 体制		
	組織形態	分散型 CSIRT
	人数規模	10 名程度
	所属	ANA ホールディングス
	活動予算	ANA ホールディングスで平常時の活動費を予算化。インシデント対応時の稼働費用は、システム障害時と同様に運用費として別途計上
主なサービス先		ANA ホールディングスの国内外のグループ企業

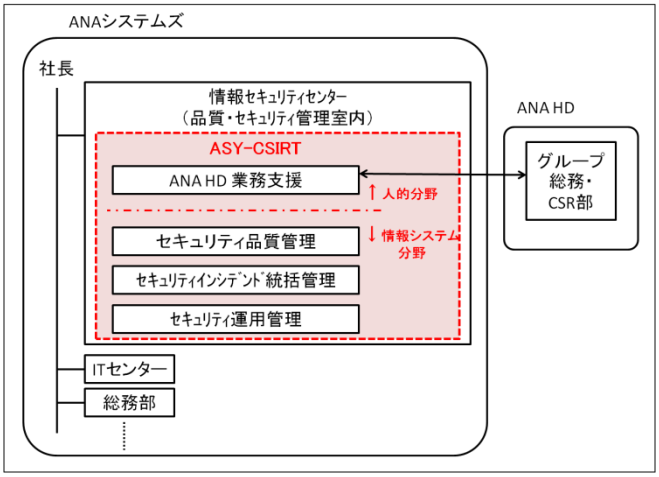
3.1.1. 組織概要

ANA Systems Co., LTD. Computer Security Incident Response Team (ASY-CSIRT) は、ANA システムズ株式会社によって運営されている CSIRT である。ANA グループ全体のセキュリティインシデントの早期復旧および影響範囲の極小化を目的として活動している。

[図 1] ASY-CSIRT 連絡窓口 阿部 恭一氏（中央）
伊藤 彰記氏（左）、村山 誠氏（右）

3.1.2. CSIRT の体制と保有する権限

ASY-CSIRT は、ANA システムズ株式会社のセキュリティ専門部署である品質・セキュリティ監理室に所属するメンバーで構成されており、ANA ホールディングス配下の仮想組織として、ANA グループセキュリティセンターの一部に配置されている。
ASY-CSIRT が発する指示は、「ANA ホールディングス」のセキュリティセンターからの指示として認識されている。



[図 2] ASY-CSIRT の体制図

ASY-CSIRT では、セキュリティに関する事案を一元化するため、情報システム分野とガバナンスを含め

た人的分野の 2 つの分野で活動している。

航空会社では、テロやハイジャック等に対して重点を置くリスク管理は慣例となっている。情報セキュリティも、事業リスクの一つとして捉えられており、ASY-CSIRT の活動も既存のリスク管理体制の中に位置づけられている。

ASY-CSIRT は、緊急時にシステムの停止を命ずる権限を持たないものの、システムの運用責任者に対して助言を行っている。また、新しいシステムを導入する際には、供用開始に先立って、システムがセキュリティガイドラインに適合しているかを ASY-CSIRT が確認する決まりになっている。

3.1.3. CSIRT 活動の成果

3.1.3.1. 経営層への活動報告

半期に一度経営層へ、年間の計画やその振り返りを報告している。また、重大なインシデントが発生した場合には臨時の報告を実施している。経営層に対してはなるべく専門用語を使わずに報告して、理解を得るよう努めており、例えば、経済産業省から「サイバーセキュリティ経営ガイドライン」が公表された 2 営業日後には ANA 社内における当該ガイドラインへの適合状況を経営層に報告する等、世間におけるセキュリティ動向についても迅速に把握分析して報告するよう努めている。

3.1.3.2. 定期レポートの発行

システムを運用している部門がシステム全体の運用状況をまとめたレポートを月に 1 度報告しており、その報告の中で、発生したセキュリティインシデントについて記載している。この報告はグループ社員および経営層に向けたものである。

3.1.3.3. CSIRT における定量的指標

事前に策定してある定義に沿った、「重大なインシデント」の発生を抑止することを、活動成果の最重要評価指標としている。また、各拠点に設置したセキュリティセンサ（トラフィックモニタやスパムフィルタ等）の結果から ANA グループ等の置かれている状況を確認し、それに対するセキュリティ対応件数や内容も指標の一つとしている。

3.1.4. CSIRT メンバーへの教育・研修

3.1.4.1. インシデント対応演習などの実施

CSIRT から ANA グループ全役職員に対して、セキュリティニュースやガイドラインなどの教育を 2 か月に 1 回実施している。ASY-CSIRT メンバーは、外部のインシデント対応演習に定期的に参加している。また、内部でのインシデント対応演習も毎週実施している。

3.1.4.2. 技術者スキルの定量的指標

情報セキュリティセンター全体で ASY-CSIRT メンバーとして必要な技術者スキルを設定している。スキルを「知識」、「企画」、「コミュニケーション」の 3 つのカテゴリに分け、それぞれのカテゴリで必要なスキルを定め、文書化している。例えば、「知識」では情報セキュリティスペシャリストや ISMS、「企画」についてはポリシーやガイドラインの策定能力、「コミュニケーション」については専門用語を使わずにインシデント対応状況を説明できる能力やプレゼンスキルが必要である旨等を定めている。

3.1.4.3. 人材育成

スキルについては 3.1.4.2 のように整備しているが、実践で培われたスキルが重要であると考えている。情報セキュリティセンターでは、実践に要求される業務を 3 つに分け、それぞれに人材育成パスを設定している。ドキュメント、教育、アセスメント、監査系の業務については、グループ内に顔が利くシニア層を対象とすることで、円滑な業務の推進を図っている。

担当業務	着任対象者	着任後に習得すべき知識やスキル
適合確認系	システム開発経験者	・セキュリティやマネジメントに関する知識 ・ポリシーやガイドラインの作成 ・適合確認業務　等
SOC、CSIRT、IRT (インシデント対応) 系	システム開発対応の経験に加え、障害対応経験者	・セキュリティやマネジメントに関する知識 ・ポリシーやガイドライン作成 ・インシデント対応業務
ドキュメント、教育、アセスメント、監査系	シニア層を含むスタッフやプレゼン経験者	・セキュリティやマネジメントに関する知識 ・教育資料の作成や従業員育成

3.1.5. CSIRT の体制やサービス、管理機能の見直し時期

3.1.5.1. サービス提供先や提供内容

情報セキュリティセンター設置時に立てた 3 年計画の中で、ASY-CSIRT のサービスの提供範囲を定義した。この定義は 3 年計画の満了時に見直す予定である。

3.1.5.2. セキュリティポリシー等の文書

ポリシーそのものを見直すことは少ない。システム構築のための各種ガイドラインに詳細な内容が記されており、これについては、年 2 回の見直しを実施している。

3.1.5.3. 連絡体制

インシデント発生時にも障害発生時と同じ連絡ルートを使うことになっている。この連絡ルートは定期的に見直しされる仕組みになっている。

3.1.5.4. インシデント管理

インシデント対応専用の管理ツールは用意せず、問合せ対応用の管理ツールを使用して管理している。

3.1.6. まとめ

航空会社としての長年の経験に基づくリスクマネジメントの仕組みが確立されており、情報セキュリティリスクも、その延長線上で捉えられている。ASY-CSIRT は、グループ全体の情報セキュリティ強化に貢献するだけでなく、新たに開発されるシステムのセキュリティ強化にも力を注ぎ、開発設計の段階からセキュリティの実装状況を確認する仕組み等を整備している。

3.2. DeNA CERT へのインタビュー

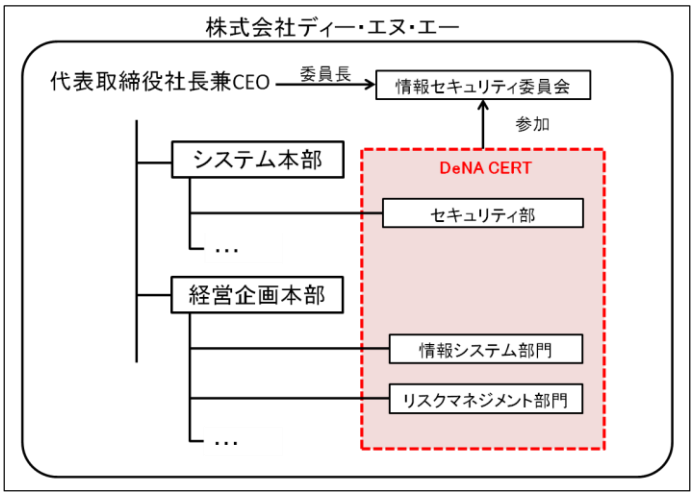
DeNA CERT		
組織名	株式会社 ディー・エヌ・エー	
事業分野	サービス業	
CSIRT 体制		
組織形態	統合型 CSIRT	
人数規模	10 名程度	
所属	システム本部　セキュリティ部	
活動予算	主に DeNA CERT を構成するセキュリティ部予算として確保	
主なサービス先	DeNA 本社および国内外グループ会社	

3.2.1. 組織概要

株式会社ディー・エヌ・エーは、ゲーム事業を主力としつつ、e コマース、キュレーションプラットフォーム、ヘルスケア事業など、DeNA は多岐にわたって幅広いサービスを提供している企業である。近年は、「インターネットによるリアル巨大産業の構造変革」を戦略の一つとして掲げ、様々な新規事業にも積極的に取り組んでいる。

[図 1] DeNA CERT メンバー 渡辺 文恵 氏

DeNA CERT は、株式会社 ディー・エヌ・エー傘下のグループ各社が展開するサービスや各社の社内システムなどをセキュアに保つこと、グループ企業内で発生するインシデントに迅速に対処することを目的として設立された。



[図 2] DeNA CERT 体制図

3.2.2. CSIRT の体制と保有する権限

DeNA CERT は、システム本部セキュリティ部を中心に、情報システム部門やコーポレート部門（リスクマネジメント部門）などの関連部門からの兼務者を加えて構成されている。

セキュリティ部は、ポリシーの策定やその運用のモニタリングなどを行うセキュリティ推進グループと、脆

弱性診断やチート対策、ネットワーク監視などを行うセキュリティ技術グループからなる。DeNA CERT のコアメンバーは、セキュリティ推進グループに所属し、ほぼ専任で DeNA CERT の業務に当たっている。

DeNA グループでは、社長が委員長を務める「情報セキュリティ委員会」がセキュリティ全般に関する最高意思決定機関であり、DeNA CERT そのものに権限は存在しない。情報セキュリティ委員会は、セキュリティポリシーを定め、その中で、インシデントの発生に気付いた社員は DeNA CERT に対して報告すること、DeNA CERT は当該社員に助言を行うこと、および当該社員は勝手な判断によりインシデントに対応しないことを義務付けている。

3.2.3. CSIRT 活動の成果

3.2.3.1. 経営層への活動報告

DeNA CERT は、毎月 1 回開催されている情報セキュリティ委員会に、重要なインシデントやモニタリング結果、新しい施策などについて報告している。また、セキュリティ部は、システム本部長に対して、月次で軽微なインシデントも含めた報告を行っている。

3.2.3.2. 社内外に向けた発行文書

社内向けにセキュリティ関連の情報を発信する Web サイトがあり、DeNA CERT 活動報告や社内インシデントの発生状況などの統計データを月次で更新して掲載している。また、同サイトに、DeNA CERT のメンバーが、月に数件の頻度でセキュリティ関連コラムを掲載している。
この Web サイトの運営はセキュリティ推進グループが行い、記事作成はセキュリティ推進・セキュリティ技術両グループで行っている。また、パートナー向けサイトのコラムにセキュリティに関する記事を投稿することもある。

3.2.3.3. CSIRT における活動評価の指標

DeNA CERT の活動を評価する指標は現在のところは特に定めていない。しかし、e ラーニングによる社員向けのセキュリティ教育の受講率や修了試験の合格率の目標を立てている。DeNA では e ラーニングによるコンプライアンス研修が毎月行われており、その修了試験でも全 10 問のうち 3 問をセキュリティ関連としている。特に、セキュリティに関するテーマや個人情報保護に関するテーマを取り上げている。また、過去にキュリティ相談をした従業員からアンケートを取り、相談対応や対策、ルールの見直しなどに活用している。

3.2.4. CSIRT メンバーへの教育・研修

3.2.4.1. インシデント対応演習などの実施

セキュリティ部及び DeNA CERT や従業員を対象とした演習を年に数回実施したいと考えている。昨年は、全従業員向けに標的型メール攻撃訓練を、DeNA CERT メンバー向けにサイバーディフェンスの名和氏をファシリテータに迎えサイバー演習を実施した。

3.2.4.2. 技術者スキルの定量的指標

DeNA CERT としてメンバーの技術スキルを評価する定量的な指標は定めていない。なお、社外のセミナーの受講や公的資格の受験についても、希望があれば内容を検討して個別に判断している。DeNA CERT だけに限らず、会社全体として社員個人の意志を尊重する組織文化である。

3.2.4.3. 人材育成

現在、育成計画等を定めてはいない。社内向けのセキュリティ関連コラムの執筆は、スキルアップの機会と考え、メンバーが持ち回りで担当している。

3.2.5. CSIRT の体制やサービス、管理機能の見直し時期

3.2.5.1. サービス提供先や提供内容

現在の体制は 2014 年度に構築された。約 2 年が経過したため、現在 CSIRT 機能の充実や拡充に向けた計画を立てている。具体的には、人材育成や、他社 CSIRT との連携や勉強会の実施を検討している。

3.2.5.2. セキュリティポリシー等の文書

セキュリティポリシーは年に 1 度見直すように規定されている。その他のマニュアル等の文書は、半年に 1 度、実際の運用とギャップがないか確認を行っている。

3.2.5.3. 連絡体制

DeNA 全社で 3 ヶ月に 1 回行われる自主監査の一環として、確認と見直しが行われている。

3.2.5.4. インシデント管理

全社で使用している案件管理システム（他社製）を利用してインシデントを管理しており、特別なツールは使っていない。

3.2.6. まとめ

社長以下、社員一人ひとりに到るまでリテラシーが高く、CSIRT の活動でも「指示命令に従わせる」場面がない。これは、「社訓」ともいうべき「DeNA Quality*6」により、物事についてしっかり考え抜く姿勢が社員に浸透し、会社全体が自律的にセキュリティを高める方向に動いているためである。
また、社員の平均年齢が 30 歳強と若いこともあるが、DeNA CERT のメンバーも若い。DeNA CERT の技術を支えているセキュリティ技術部でも、新卒者を積極的に受け入れ、セキュリティ知識やスキルを身に着けている。社内の状況や希望に併せて開発などの事業部門に異動となるケースもあり、社内のセキュリティ人材の確保・育成にも積極的に取り組んでいる。

*6 TOP>企業情報>コーポレートアイデンティティ：DeNA Quality http://dena.com/jp/company/policy/

3.3. FJC-CERT へのインタビュー

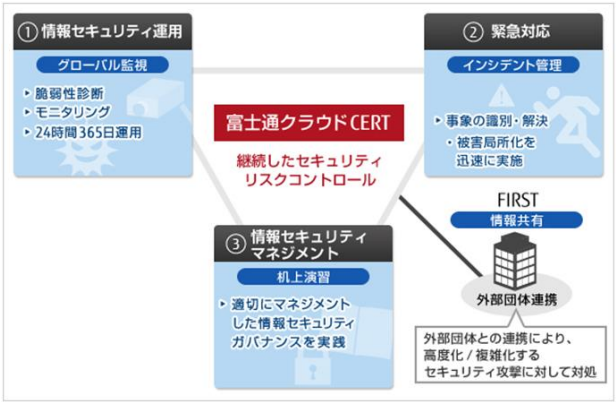
FJC-CERT		
組織名	富士通株式会社	FUJITSU
事業分野	情報通信業	
CSIRT 体制		
組織形態	集中型 CSIRT	
人数規模	40 名程度	
所属	セキュリティマネジメントサービス事業本部	
活動予算	社外向けサービスを提供している各事業本部が FJC-CERT の活動費用を負担	
主なサービス先	主に富士通クラウドサービスの利用者（コーポレートや製品の脆弱性は FJC-CERT の提供範囲外であり、別チームが担当）	

3.3.1. 組織概要

富士通株式会社は、大手電機メーカーの一つとして、通信システムや情報処理システム、通信デバイス等を製造販売している。加えてクラウドサービスの提供も手掛けている。富士通クラウド CERT（FJC-CERT）は、後者に対応するために設置された CSIRT である。

[図 1] FJC-CERT 代表　山下 眞一郎 氏（右）
連絡窓口　佳山 こうせつ 氏（左）

富士通がパブリック型クラウドサービスを開始しグローバル（世界 6 ヶ国）に展開するにあたって、クラウドにおけるセキュリティ上の脅威（サイバーテロや不正利用、情報漏えいなど）に対して迅速に対応することを目的として FJC-CERT が設立された。なお、FJC-CERT はサービス提供先の部署（受益部署）が負担する費用で運用されていることも特徴となっている。



[図 2] FJC-CERT の活動概念図

3.3.2. CSIRT の体制と保有する権限

FJC-CERT は、セキュリティマネジメントサービス事業本部サイバーディフェンスセンターのメンバー（40 名程度）から構成される。
FJC-CERT 自体はサービスの緊急時のシステム停止

などを命ずる権限はなく、サービスオーナーに、技術的な助言や協力を行う立場にある。

脆弱性／サイバー脅威情報の収集やサービスに対する不正アクセスのモニタリングが主な活動である。製品のセキュリティを担当する部署や、社内環境を防御する部署と協調して、サービスにおけるセキュリティマネジメントも実施している。インシデント発生時には、事象を分析し適切に対応することで、被害を最小限に抑える役割を担っている。

3.3.3. CSIRT 活動の成果

3.3.3.1. 経営層への活動報告

経営層も参加するセキュリティ委員会（半年に 1 度程度）で活動状況を報告している。また、受益部署向けに、インシデント対応件数や不正アクセスのモニタリング状況をまとめた月報を発行している。

3.3.3.2. 社内外に向けた発行文書

「重大セキュリティ事故ゼロ」を目標として掲げて活動しており、日々の活動状況について、全社員向けに社内サイト上で活動に関する報告を公開している。

3.3.3.3. CSIRT における活動評価の指標

運営費は受益部署が負担しているため、受益部署に対して年度初めに明示した活動目標を CSIRT の活動の指標としている。

3.3.4. CSIRT メンバーへの教育・研修

3.3.4.1. インシデント対応演習などの実施

重大なインシデントが発生した際に迅速に対応するために、関連部署や各サービスのオーナーを集めた机上のインシデント対応演習を定期的に実施している。

3.3.4.2. 技術者スキルの定量的指標

FJC-CERT の技術者のみならず、富士通グループ全体に「セキュリティマイスター認定制度」を設けている。社内におけるセキュリティ人材の技術や活動実績を可視化することで、セキュリティ技術スキルの向上へのモチベーションを高めている。

「セキュリティマイスター認定制度」では、システム開発やサービス運用の実務者が対象の「フィールド領域」、高度なセキュリティ特化技術を有する「エキスパート領域」に加え、いわゆるホワイトハットハッカーに相当する「ハイマスター領域」の 3 領域に分類されており、それぞれを細分化した 15 分野

の人材像モデルを定義している*7。また、「セキュリティマイスター認定制度」は人事評価や奨励金支給などの制度とは関係なく、サイバーセキュリティに関する技能を持った人材を発掘・育成し、顧客の安心安全な ICT 運用を支えることを目的に設けられている。

3.3.4.3. 人材育成

セキュリティマイスター認定制度の教育プログラムを利用して、人材育成を実施している。教育プログラムには、「共通教育」と「専門教育」のコースがあり、例えばエキスパート領域における共通教育コースでは、富士通社内に構築されたサイバーレンジ（仮想演習場）を使用した、実践力の養成を重視するプログラムを提供している。さらに、セキュリティに関する実践的な知識や技術を問う「富士通サイバーセキュリティコンテスト」を、富士通グループ全社から出場者を募って年 2 回開催している。セキュリティに素養のある人材を可視化・発掘する取組みの一つであり、将来のセキュリティマイスターを発掘・育成する環境を作ることで、技術やモチベーションの向上を図っている。

3.3.5. CSIRT の体制やサービス、管理機能の見直し時期

3.3.5.1. サービス提供先や提供内容

サービス内容や提供範囲の見直しは、必要に応じて実施している。特に脆弱性ハンドリングサービスを提供していることから、設計段階でのセキュリティ検討を含め、セキュリティコンサルティングサービスも提供している。

3.3.5.2. セキュリティポリシー等の文書

セキュリティポリシーの見直しは、必要に応じて対応することになっているが、直近で見直しは発生していない。ただし、サービス内容の見直しと合わせて、手順やガイドラインの見直しは、都度、実施している。

3.3.5.3. 連絡体制

適宜、見直しを実施している。机上訓練の実施（四半期に 1 回程度）しており、連絡体制を見直すきっかけを得ることも多い。

3.3.5.4. インシデント管理

FJC-CERT では、受益部署向けに成果を数値化して情報を発信するため、オープンソースのチケット管理システムを導入している。

*7 FUJITSU Security Initiative セキュリティマイスター認定制度 : 富士通
http://jp.fujitsu.com/solutions/safety/security-initiative/security-meister/

3.3.6. まとめ

繰返しになるが、次の 3 点が FJC-CERT の特長である。

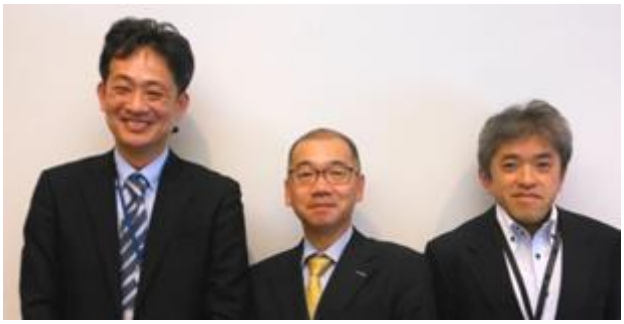
1. FJC-CERT は、社外にサービスを提供している事業本部に対して、その提供サービスについてのセキュリティを担う組織として定義されている
2. 「予防対策」（サービス設計時の脆弱性の作り込み防止など）を実施した上で、「対症療法」（水際防御）で当座の攻撃を防ぎつつ、「原因療法」（脆弱性診断）により継続的にリスクをコントロールしている
3. 社内関連部署と継続的に連携するために、人材育成や社内セキュリティコンテストの開催を通じて、社内に仲間を増やす活動を実施している

3.4. Fuji Xerox CERT へのインタビュー

Fuji Xerox CERT	
組織名	富士ゼロックス株式会社
事業分野	製造業
CSIRT 体制	
組織形態	分散型 CSIRT
人数規模	約 20 名
所属	総務部
活動予算	総務部の活動費として予算化
主なサービス先	富士ゼロックス及び同社の国内外グループ企業

3.4.1. 組織概要

富士ゼロックス株式会社は、複合機などの製造販売、および総合文書管理ソリューションのコンサルティングなどを提供する、大手電子機器メーカーである。国内のみならず、国外にも幅広くサービスを展開している。

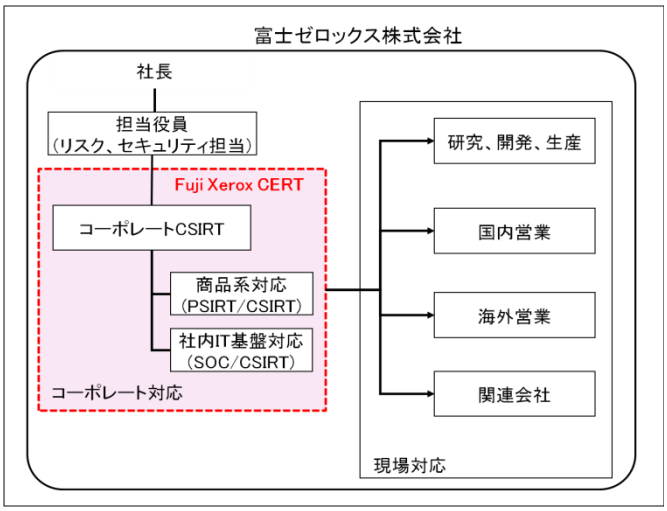


[図 1] Fuji Xerox CERT 代表 神林 彰 氏（中央）
連絡窓口　増田 佳弘 氏（右）
漆嶌 賢二 氏（左）

セキュリティに関する脅威にグローバルに対応するため、2010 年より CSIRT 活動を開始し、2014 年に Fuji Xerox CERT として NCA に正式加盟した。Fuji Xerox CERT は、富士ゼロックス及び同社の国内外グループ企業を対象として、サイバー攻撃等の脅威に対して、予防・検知・迅速な事後対応を組織横断的に行っている。

3.4.2. CSIRT の体制と保有する権限

Fuji Xerox CERT は、社内インフラで発生したインシデントに対応する情報システム部門と情報子会社のメンバー、及び製品やサービスに関わるインシデント（脆弱性対応＝PSIRT 機能を含む）に対応する品質保証部門と開発部門のメンバーからなる仮想組織である。



[図 2] Fuji Xerox CERT の体制図

リスクマネジメントを担当する総務部情報セキュリティセンターが事務局をしている。
総務部情報セキュリティセンターは、開発や営業、法務など、様々な部門の出身者から構成されており、中にはフォレンジクスを行うメンバーもいる。また、社内インフラの運用を行っている情報子会社は SOC 機能を担っている（一部は専門業者に外注している）。米国ゼロックス社とは、CSIRT 同士ではなく、各部門で連携している。

Fuji Xerox CERT 自体に、サービス停止などを指示または命令する権限はないが、必要があれば、Fuji Xerox CERT を構成するリスクマネジメント部門、情報システム部門、品質保証部門などが指示や命令を出す。また、情報セキュリティやシステムを担当する役員ら（いわゆる CISO に相当）から指示命令が下されることもある。

Fuji Xerox CERT は、基本的に、技術的なアドバイザーや社内関連部門や外部 CSIRT とのコーディネーター、リスクマネジメントを担う役割として位置づけられている。例えば、社内インフラで発生したインシデントは、CERT に状況がエスカレーションされ、リスクの程度を判断すると共に、主管である情報システム部門と情報子会社が対処する。また、製品の脆弱性やサービスに関連したインシデントについては各製品やサービスの主管部門が対応し、サービス停止などの判断はその部門の担当役員が行う。

今まではセキュリティ関連の情報を CERT のメンバーが所属する部署の名前で発信していたが、今後は、国内外のグループ会社に広く認知してもらうため「Fuji Xerox CERT」の名前で情報を発信していきたいと考えている。

3.4.3. CSIRT 活動の成果

3.4.3.1. 経営層への活動報告

年に 2 回、情報セキュリティ対策の実施状況などを経営層に説明している。インシデントについては軽微なものを含め、週次でリスクマネジメント担当役員に報告している。これらとは別に、関連する経営層に対して月 1 回の報告を実施している。いずれの報告も経営層からの指示により行われている。

3.4.3.2. 定期レポートの発行

経営層向けの活動報告の中から社外に公表してもそれほどリスクが高くない内容を整理するなどし、年に 1 回程度、「情報セキュリティ報告書」としてレポートを公開している。

3.4.3.3. CSIRT における定量的指標

定量的な指標とは異なるが、手順等の文書化や訓練の実施など、CSIRT としての年度計画を立てていて、その進捗を月 1 回の会合で確認している。

3.4.4. CSIRT メンバーへの教育・研修

3.4.4.1. インシデント対応演習などの実施

1 年に 1 回以上の演習を行う方針で、次のような演習ないし訓練を実施している。

- 社員向け標的型攻撃対応訓練
- CSIRT メンバー及び現場部門メンバーによる合同の机上演習

3.4.4.2. 技術者スキルの定量的指標

CSIRT のメンバーに対しては特に設けていない。全社的（特に情報子会社）には公的資格の取得を推奨している。

3.4.4.3. 人材育成

CSIRT のメンバーの人材育成は特別に実施してはいない。新入社員に対して IT パスポートレベルのスキルが身につく研修を組んでいる。現在は、2、3 年次のステップアップ要件として、情報セキュリティマネジメント試験の合格を考えている。

3.4.5. CSIRT の体制やサービス、管理機能の見直し時期

3.4.5.1. サービス提供先や提供内容

年度ごとにサービス提供範囲を見直すスキームが整備されており、それに従って見直しを実施している。

3.4.5.2. セキュリティポリシー等の文書

年度ごとにセキュリティポリシー等の文書が実際の運用とギャップがないかを見直している。

3.4.5.3. 連絡体制

関係者による会合を月に 1 回開催しており、そこで見直しや確認が行われている。

3.4.5.4. インシデント管理ツール

CSIRT としてサイバーセキュリティだけを個別に管理しているインシデント管理ツールはまだない（現在検討中）が、情報セキュリティ・インシデント全般については自社開発の製品を使って総務部情報セキュリティセンターが管理している。また、インシデントの報告や対応には自社開発の「事故報告管理システム」や「脆弱性情報自動配信システム」を使っている。

3.4.6. まとめ

製造事業者として長年培ってきた経験と組織文化があり、品質保証に関しては、常に安全を重視した対応を行ってきた。経営層の情報セキュリティに対する関心も高く、新入社員に対しても、安全に対する意識を根付かせるような活動を行っている。

3.5. I-SIRT へのインタビュー

I-SIRT	
組織名	株式会社帝国ホテル
事業分野	サービス業
CSIRT 体制	
組織形態	分散型 CSIRT
人数規模	事務局 5 名
所属	情報システム部
活動予算	情報システム部の活動費として予算化
主なサービス先	帝国ホテル及び帝国ホテルグループ全体

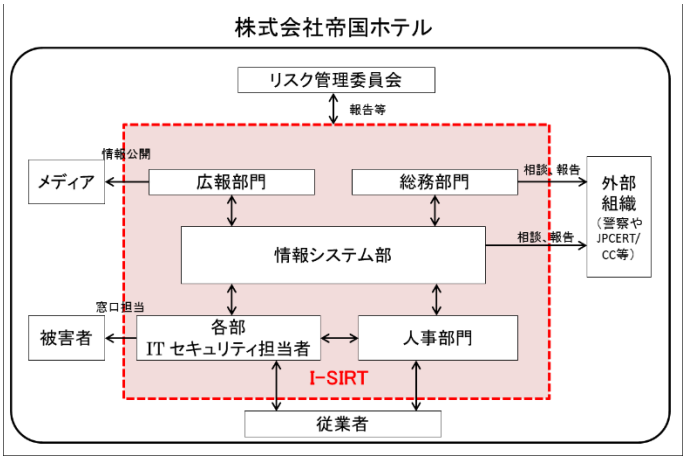
帝国ホテル

3.5.1. 組織概要

[図 1] I-SIRT 代表　今井　徹 氏（左から 2 番目）
連絡窓口　白坂 孝一 氏（左から 1 番目）
ほか I-SIRT のみなさん

Imperialhotel-Security Incident Response Team（I-SIRT）は、帝国ホテル及び帝国ホテルグループの CSIRT であり、ホテル業界で初めて NCA に加盟した CSIRT である。I-SIRT では、グループ内の IT に関わるセキュリティインシデントの防止、および発生時のハンドリングや起こりうるリスクの極小化を目的とした活動を行っている。

3.5.2. CSIRT の体制と保有する権限



[図 2] I-SIRT の体制図

I-SIRT は、組織横断的なメンバーで構成された既存のリスク管理機能に、新たにセキュリティの役割を持たせた仮想組織である。事務局は情報システム部が担っており、I-SIRT の連絡窓口として各部署に「IT セキュリティ担当者」を配置している。

帝国ホテルでは I-SIRT 設立以前から、テロや食品衛生など様々なリスクに対してリスク管理委員会を設け、対策や活動を行っていた。IT セキュリティに関しては、情報システム部が単独で対応していたが、I-SIRT を設立し全社的に取り組む方針が確立した。

インシデントが発生した場合、I-SIRT 事務局は発生部署や情報システム部の担当者に指示や助言を行うとともに、I-SIRT メンバーである関連各部と連携し、全社機関であるリスク管理委員会に適時報告する。技術的に高度な対応が必要な場合は、外部の専門組織とも連携する。

3.5.3. CSIRT 活動の成果

3.5.3.1. 経営層への活動報告

経営層も出席するリスク管理委員会への活動報告を半年ごとに実施している。これによりサイバー攻撃も重大な事業リスクの一つであることが経営層にも浸透してきている。

3.5.3.2. 定期レポートの発行

リスク管理委員会への活動報告の他に、従業者の知識の向上を目的として、各部の IT セキュリティ担当者向けに「IT セキュリティ通信」というレポートを月次で発行している。本レポートでは、標的型攻撃メール等サイバー攻撃の脅威や、セキュリティポリシーを守る重要性などを紹介している。

3.5.3.3. CSIRT における定量的指標

現状、I-SIRT 活動の定量的な評価指標はない。

3.5.4. CSIRT メンバーへの教育・研修

3.5.4.1. インシデント対応演習などの実施

社内向けの標的型攻撃メール訓練では、メールを開いてしまった際に自部門の IT セキュリティ担当者に報告する等、エスカレーションフローを意識するように指導している。IT セキュリティ担当者から報告を受け I-SIRT のメンバーが対象の現場に向かうといった本番を意識した訓練を実施した。訓練実施後、I-SIRT 事務局に不審メールの報告が増加したなど、従業者のセキュリティに対する意識の向上を実感している。

3.5.4.2. 技術者スキルの定量的指標

現状では、技術者のスキルを定量的に評価する指標は存在していない。本業が「サービスを提供する」ことである為、技術者スキルの定量的評価に重きを置いた活動はしていない。

3.5.4.3. 人材育成

人材育成の一環として、一般的な IT 系の資格取得に対する援助や支援制度は存在するものの、明確な I-SIRT としての人材の定義に関する取り決めは現在のところない。I-SIRT 事務局には IT に関する業務経験

が少ない営業部門出身のメンバーもいるため、育成は中期計画を立て業務を通じて実施しているが、セキュリティに精通した人材の確保も課題と考えている。

3.5.5. CSIRT の体制やサービス、管理機能の見直し時期

3.5.5.1. サービス提供先や提供内容

年度ごとの予算確保のタイミングで人的、技術的、物理的にセキュリティ対応策を見直しているほか、状況の変化に応じた見直しも適宜実施している。

3.5.5.2. セキュリティポリシー等の文書

I-SIRT 設立以前にも、情報システムに関する規程があったが、I-SIRT 設立後にセキュリティの項目を追加した。また、従業者へ規程の周知を図るため、内容を分かりやすく解説した「情報システム安全管理ハンドブック」を作成・配布した。

3.5.5.3. 連絡体制

I-SIRT 事務局は各部の IT セキュリティ担当者を通じて情報伝達を行っている。連絡体制図は、人事異動のタイミングで見直している。

3.5.5.4. インシデント管理

インシデント管理ツールなどは特に使用せず、Excel で管理している。また、OneNote を使用し、インシデントの対応状況を共有している。

3.5.6. まとめ

ホテル業として培ってきたリスク管理の経験から、特に「宿泊客の個人情報」が攻撃者の標的になるリスクが高く、守るべき対象であると認識している。セキュリティの対策は必須と考えているが、ホテルとして、利便性の向上も重視して活動している。IT 知識に精通した人材の確保は課題であるものの、NCA のワーキンググループや同業他社との連携を通して情報収集能力を高め、人的、技術的、物理的なセキュリティ対策が出来るよう強化している。

3.6. MB-SIRT へのインタビュー

MB-SIRT		
組織名	森ビル株式会社	
事業分野	不動産業	
CSIRT 体制		
組織形態	分散型 CSIRT	
人数規模	5 名程度	
所属	情報システム部	
活動予算	情報システム部の活動予算として予算化	
主なサービス先	森ビル及びその関連会社	

3.6.1. 組織概要

森ビル株式会社は、都市再開発事業や不動産の賃貸・管理のみならず、文化や芸術などを含めた都市づくりを国内外で展開する大手不動産企業である。

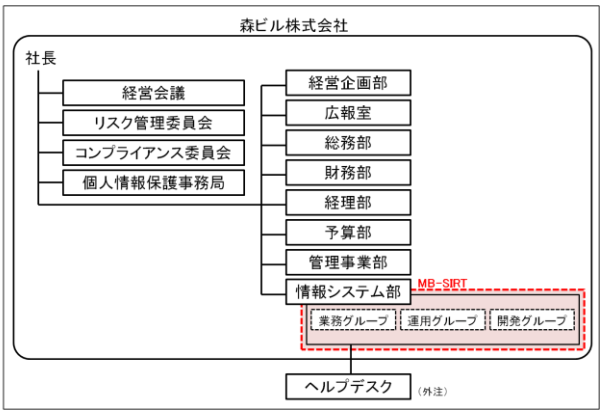
2014 年 3 月に自組織で運営する Web サイトが改ざんされたことをきっかけに、森ビル株式会社セキュリティインシデントレスポンスチーム（MB-SIRT）が構築された。MB-SIRT では、自組織及びグループ会社を対象にセキュリティインシデント発生時の対応に加えて、インシデントを未然に防ぐための社員への啓発活動やセキュリティルールの整備などの活動を行っている。

[図 1] MB-SIRT 連絡窓口 佐藤 芳紀 氏

3.6.2. CSIRT の体制と保有する権限

MB-SIRT は、情報システム部門で情報セキュリティを担当するメンバーから構成される。

森ビルでは、MB-SIRT 設立以前より情報システム部が中心となってインシデント対応を実施していた。情報システム部の主管役員が CISO の役割を担っている。MB-SIRT は、情報システム部を中心に構築されたフレームワークに則って活動している。意思決定は情報システム部及び関係する部署にて行われ、MB-SIRT のみ



[図 2] MB-SIRT の体制図

で判断して活動するわけではない。

なお、情報システム部は、森ビル社内の情報システムについて運用管理だけでなく企画開発の機能も備えている。全てではないが関連会社を含めた森ビル企業グループの IT に関連する業務を、一部予算を含めて集中的に担っている（ただし、森ビルが管理するビルの管理システムは別の部門が所管しているが、今後は更なる連携が必要になると考えている）。

セキュリティインシデント発生時には、MB-SIRT は技術対応およびその支援を行う。必要に応じて、リスク管理委員会や個人情報保護事務局、広報室などと連携する。また、技術的に高度な対応が必要になった場合は、外部の専門業者に委託している。

3.6.3. CSIRT 活動の成果

3.6.3.1. 経営層への活動報告

リスク管理委員会を通じて技術対応や支援についての概要を活動報告として不定期に行っている。また、入手した情報の対応の重要度によっては、情報システム部より、対応状況の報告を行うこともある。

3.6.3.2. 社内外に向けた発行文書

規程やセキュリティ情報等は、情報システム部から発信している。今のところ MB-SIRT から発信している公開文書はない。

3.6.3.3. CSIRT における活動評価の指標

現時点で、CSIRT の活動を定量的に評価する指標は策定されていない。経営層には活動報告にて技術対応や支援内容を共有している。経営層は、情報セキュリティを不動産業における物理セキュリティの延長線上に存在する必要不可欠なものと捉えているため、セキュリティに対する関心は高い。

3.6.4. CSIRT メンバーへの教育・研修

3.6.4.1. インシデント対応演習などの実施

全社員を対象とする標的型メール訓練を実施している。ただし、CSIRT を対象としたインシデント対応演習は実施していないが、今後実施を検討している。

3.6.4.2. 技術者スキルの定量的指標

技術者の IT スキルを定量的に評価する指標は現在のところ存在しない。

3.6.4.3. 人材育成

MB-SIRT では、メンバーに対して、資格の取得や外部セミナーなどの受講を積極的に支援している。しかし、取得すべき資格や受講すべきセミナーなどについて具体的な決まりはなく、参加の是非については都度判断している。

3.6.5. CSIRT の体制やサービス、管理機能の見直し時期

3.6.5.1. サービス提供先や提供内容

情報システム部の予算計画のタイミングで見直している。

3.6.5.2. セキュリティポリシー等の文書

森ビルでは、全社規程の見直しを、年に一度実施するように通達があり、これに合わせてセキュリティ関連の規程を見直している。また、これとは別に、情報システム部では、システム入替えのタイミングでも随時、見直している。

3.6.5.3. 連絡体制

人事異動のタイミングで適宜見直している。隔週で開催されるリスク管理委員会でも見直される。

3.6.5.4. インシデント管理

MB-SIRT としては、情報システム部における記録としてインシデントを管理しているものの、現時点ではツールを用いた管理はしていない。一般社員からの問合せ等を受け付ける外部委託のヘルプデスクでは、自社開発したデータベースシステムを用いてインシデント管理が行われている。

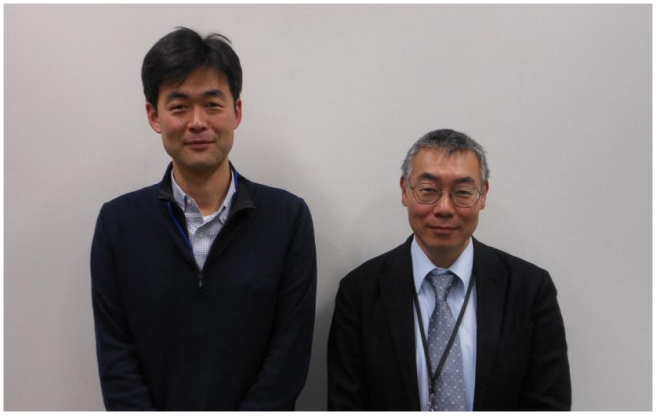
3.6.6. まとめ

情報システム部が、IT システムに関する企画から開発・運用までの全ライフサイクルを任されていて、技術者のモチベーションが高い。そのため、MB-SIRT メンバーも運用中の IT システムの構造を熟知しており、インシデント発生時も円滑な対応が可能になっている。

3.7. NTT-CERT へのインタビュー

NTT-CERT		
組織名	日本電信電話株式会社	
事業分野	情報・通信業	
CSIRT 体制		
組織形態	調整役 CSIRT	
人数規模	60 名程度	
所属	セキュアプラットフォーム研究所	
活動予算	セキュアプラットフォーム研究所の研究費として確保	
主なサービス先	NTT グループ会社	

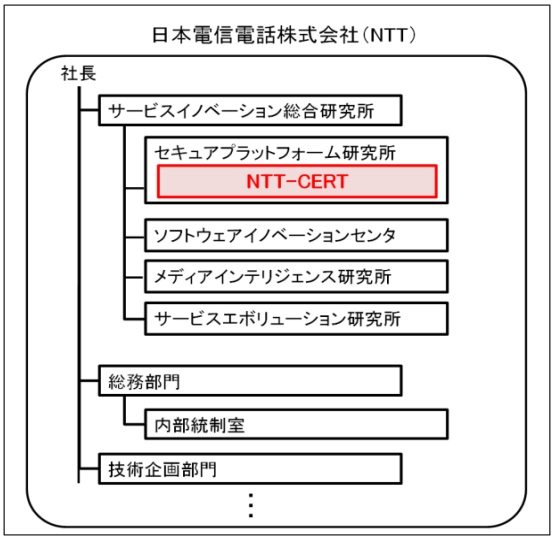
3.7.1. 組織概要



[図 1] NTT-CERT 連絡窓口　関戸　直生 氏（左）
小村　誠一 氏※（右）
※現在 NTT アドバンステクノロジ株式会社に所属

NTT-CERT は、日本電信電話株式会社（NTT）のサービスイノベーション総合研究所内にあるセキュアプラットフォーム研究所に所属している CSIRT である。セキュアプラットフォーム研究所は、暗号技術やサイバーセキュリティ、セキュリティアーキテクチャなどのセキュリティに関する研究開発をしており、セキュリティリスクマネジメントプロジェクトにて、CSIRT としてのオペレーションを実施している。NTT-CERT は、NTT グループ全体に対してセキュリティ関連情報の提供、調査、分析、啓発活動等をサービスとして提供している。また、NCA の設立発起人の 1 チームである。

3.7.2. CSIRT の体制と保有する権限



[図 2] NTT-CERT の体制図

NTT-CERT は、NTT グループに関連するセキュリティインシデント情報の受付、対応支援、再発防止策の検討、トレーニングプログラム等の提供およびセキュリティ関連情報の提供などを行っている。また、NTT グループのリスクマネジメント体制に組み込まれており、NTT グループの災害対策チームとしても活動している。調整役 CSIRT として、60 名程度（外部委託組織等からの支援者含む）のメンバーにより構成されている。
NTT-CERT では、グループ各社に対する指示権限や統

制権を保有せず、技術的な情報の提供とグループ内組織によるセキュリティ関連活動の調整及び対応等の活動を行っている。NTT-CERT から提供された情報をどう活用するかは、グループ各社の判断に委ねられている。グループ各社への命令権限は、NTT（持株会社）の総務部門に置かれた内部統制室が有している。

3.7.3. CSIRT 活動の成果

3.7.3.1. 経営層への活動報告

月に一度、研究所の幹部に対して、セキュリティアラート発信やインシデントハンドリング等の件数や傾向を報告している。これらの情報をもとに四半期レポートも策定し発行している。

3.7.3.2. 定期レポートの発行

セキュリティに関するアナリストレポートと脆弱性レポートを、NTT-CERT のグループ向けホームページを通じて適宜配信している。また、年 1 回、セキュリティの動向やセキュリティ製品の検証結果等をまとめたアニュアルレポートを社外にも公開している。

3.7.3.3. CSIRT における定量的指標

年 1 回、JNSA （Japan Network Security Association）がまとめた報告書に基づいて、NTT グループ内で発生したインシデントの想定被害額を算定し、研究所の幹部に報告している。このデータは、CSIRT 活動の効果について数値で説明できるため、セキュリティ施策の効果を客観的に比較できると考えている。

3.7.4. CSIRT メンバーへの教育・研修

3.7.4.1. インシデント対応演習などの実施

年 1 回、NTT グループ 10 社を集めて、100 人規模のインシデント対応演習を実施している。

3.7.4.2. 技術者スキルの定量的指標

一部の技術分野では保有している資格をもとに、初級レベルや中級レベルといったスキル認定をしている。セキュリティに関する推奨資格は、NTT-CERT で助言することもある。

3.7.4.3. 人材育成

2020 年までに NTT グループ内のセキュリティ人材を 10,000 人育成する計画があり、それに向けて各人が目指すべき将来像の定義づけを試行的に進めている。また、TRANSITS にも参加し、有資格者を保有している。

3.7.5. CSIRT の体制やサービス、管理機能の最適化

3.7.5.1. サービス提供先や提供内容

年 1 回、予算確保のタイミングで、サービス提供範囲について見直しを実施している。NTT-CERT 内にインシデント対応等のノウハウも蓄積されてきたため、昨年、サービス提供範囲を拡大した。今後は国外のグループ会社へも情報提供等のサービスを提供できないか検討している。

3.7.5.2. セキュリティポリシー等の文書

NTT グループ会社のセキュリティポリシーは NTT の内部統制室が作成しており、ポリシー作成時に NTT-CERT は助言や技術的支援を行っている。NTT-CERT 自身のセキュリティポリシーについては年 1 回の予算確保の際に内容の見直しを行っている。

3.7.5.3. 連絡体制

NTT の技術企画部門が連絡体制表を管理している。グループ各社と 24 時間 365 日連絡がとれる体制が整備されており、人事異動のタイミング等で適宜更新されている。

3.7.5.4. インシデント管理

インシデントハンドリングには、連絡窓口が管理している案件管理簿を使用している。また、独自ツールのシステム開発も行っている。

3.7.6. まとめ

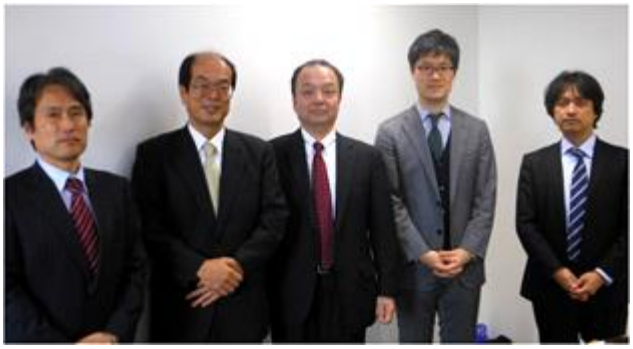
NTT-CERT は「研究所が運営している CSIRT」組織である。対象は NTT グループ会社であるが、NTT-CERT は各部門に対する権限を一切持っていない。そのため、各部門が気軽に相談できる雰囲気が醸成され、円滑にコミュニケーションがとれている。
CSIRT はコミュニケーション能力が大事という考えのもと、インシデント対応演習や情報連絡会、ワークショップなどを通じて、顔が見えるグループ会社を超えたネットワーク作りにも力を入れている。

3.8. T-SIRT へのインタビュー

T-SIRT		
組織名	大成建設株式会社	大成建設 TAISEI For a Lively World
業界団体	建設業	
CSIRT 体制		
組織形態	分散型 CSIRT	
人数規模	8 名	
所属	社長室　情報企画部	
活動予算	情報企画部の活動費として予算化	
主なサービス先	大成建設及びそのグループ/関連会社	

3.8.1. 組織概要

大成建設は、日本を代表する大手総合建設会社に数えられる企業であり、Taisei-SIRT（略称：T-SIRT） は、その組織内 CSIRT である。T-SIRT は建設業界で初めて NCA に加盟した CSIRT でもある。

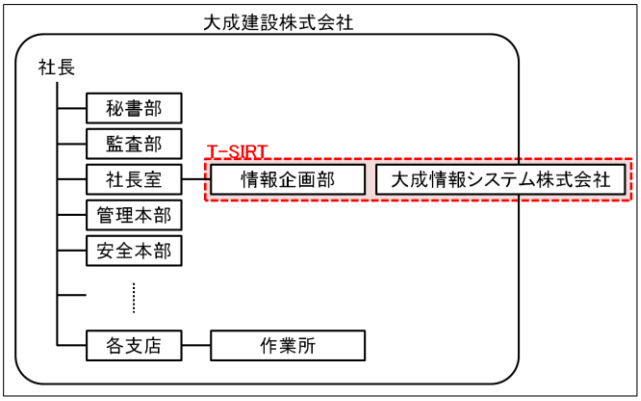


[図 1] T-SIRT 代表　柄 登志彦 氏（中央）
連絡窓口　北村 達也 氏（左から 2 番目）
ほか T-SIRT のみなさん

従来は、情報企画部にて、組織内のインシデント対応や情報収集を行っていたが、近年のサイバー攻撃の急増を踏まえ、必要な機能を CSIRT として独立させるとともに、緊急時の対応体制を拡充強化した。

3.8.2. CSIRT の体制と保有する権限

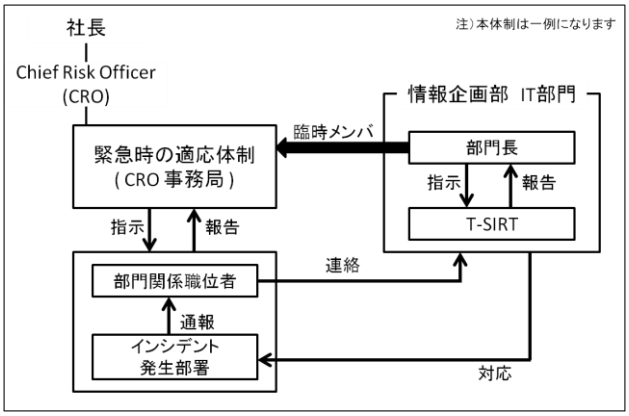
T-SIRT は、社長室直下の情報企画部と情報系グループ会社である大成情報システム（TAIS）のメンバーから構成される分散型 CSIRT である。情報企画部 IT 部門の部門長が、T-SIRT を所掌しており、メンバーは、各グループの役職者（チームリーダー）から構成される。分散型 CSIRT で課題になりがちな、権限や対応範囲の曖昧さを解消するため、ドキュメント類の整備に注力している。



[図 2] T-SIRT の体制図

大成建設では、既存のリスクマネジメントの体制が存在しており、T-SIRT の活動を含めて、既存のワークフ

ローの中で展開されている。T-SIRT は、業務手順や機器の取扱ルールなどの整備を担うほか、社内やグループ関連会社に対して、セキュリティに関する助言や協力を行っている。
重大なインシデントが発生した際には、緊急時の対応体制（CRO*8事務局）のメンバーとして情報企画部長を招集する。T-SIRT は、その対応体制の一翼として、技術支援と連絡対応窓口の役割を担う。



[図 3] 重大インシデント発生時の対応体制

3.8.3. CSIRT 活動の成果

3.8.3.1. 経営層の活動報告

活動報告は、週次と年次で行っている。週次報告では、社長室長に情報が共有される。年次報告では、PC の紛失などのセキュリティ事故やその被害内容、新たな情報セキュリティ施策、社員教育などを報告書にまとめ、社長室長および総務部長へ報告している。総務部長は、大成建設においてリスクマネジメント体制を統括している。

3.8.3.2. 社内外に向けた発行文書

経営層向けの年次報告書と、全社員に向けた注意喚起を発行している。全社員向けの注意喚起では、脆弱性情報などの技術的な内容を避けて、社員の誰もが気をつけるべき事故事例などを紹介している。

3.8.3.3. CSIRT における活動評価の指標

現時点で、T-SIRT の活動を評価する定量的な指標は設定していないが、定期的な活動報告や日常的な情報セキュリティ活動を行っていることもあり、経営層からは一定の評価が得られている。一方で、全社員に向けた教育や啓発の機会にて注意を呼びかけるなどの活動の結果、PC の紛失や業務に関係のないホームページ閲覧などのセキュリティ事故の件数が減少してきており、T-SIRT の成果の一つと考えている。

3.8.4. CSIRT メンバーへの教育・研修

3.8.4.1. インシデント対応演習などの実施

T-SIRT メンバーは、最低年に一度は、セキュリティベンダによるハンズオンを受けている。そのほか、JPCERT/CC による演習や NCA が主催する TRANSITS Workshop*9などにも積極的に参加している。

*8 CRO : Chief Risk Officer の略称で、最高リスク管理責任者のことを指す。
*9 TRANSITS Workshop : CSIRT の設立の促進、既存の CSIRT の対応能力向上を目的としたトレーニングを行うワークショップ

3.8.4.2. 技術者スキルの定量的指標

T-SIRT としてメンバーの技術スキルを評価する定量的な指標は定めていない。なお、TAIS には、公的な資格の取得を評価し奨励する制度がある。

3.8.4.3. 人材育成

外部研修を受けることで T-SIRT メンバーのスキルアップを図っている。また、キャリアパスなどの整備も進めている。

3.8.5. CSIRT の体制やサービス、管理機能の見直し時期

3.8.5.1. サービス提供先や提供内容

T-SIRT では、年度ごとに提供サービス範囲を最適化し、改善計画を検討した上で、必要な投資については情報企画部の予算として計上している。

3.8.5.2. セキュリティポリシー等の文書

セキュリティポリシーなどの文書の整備は、情報企画部の担当室が行っている。T-SIRT は、セキュリティポリシーの改訂提案やセキュリティポリシーに則ったインシデント対応マニュアル等個別のプロシージャ（手順書）の整備を行っている。

3.8.5.3. 連絡体制

大成建設では、緊急時の連絡網や電話帳が常に最新の状態に維持されており、この連絡網の中で T-SIRT からのインシデント連絡体制も管理されており、連絡先が不明になる事態は起こりにくいと考える。また、広報室や総務部、社内交換室にも、外部からのエスカレーションルールを周知している。

3.8.5.4. インシデント管理

TAIS は障害対応などを管理するデータベースをもっているが、T-SIRT では特別な管理ツールは導入していない。専用の管理ツールの必要性は強く認識している。現状では、例えば脆弱性対応には表計算ソフトを用いて管理している。

3.8.6. まとめ

大成建設では、IT を業務効率化のために活用しており、また、事業継続（BCP、BCM、BIA）を意識した経営的視点でプロアクティブなセキュリティ対策を目指していることから、外部組織との IT や情報セキュリティに関する情報交換は比較的行いやすいと考えている。そのため、NCA など外部との情報交換の場に積極的に参加している。また、外部組織の活動状況に触れることで、知識の吸収だけでなく、抱えている悩みに関する意見交換が可能になり、CSIRT メンバーのモチベーション維持、向上にも繋がっている。

3.9. YMC-CSIRT へのインタビュー

YMC-CSIRT		
組織名	ヤマハ発動機株式会社	YAMAHA Revs Your Heart
事業分野	製造業	
CSIRT 体制		
組織形態	分散型 CSIRT	
人数規模	8 名	
所属	情報システム部	
活動予算	情報システム部の活動費として予算化	
主なサービス先	ヤマハ発動機株式会社及び同社の国内外のグループ企業	

3.9.1. 組織概要

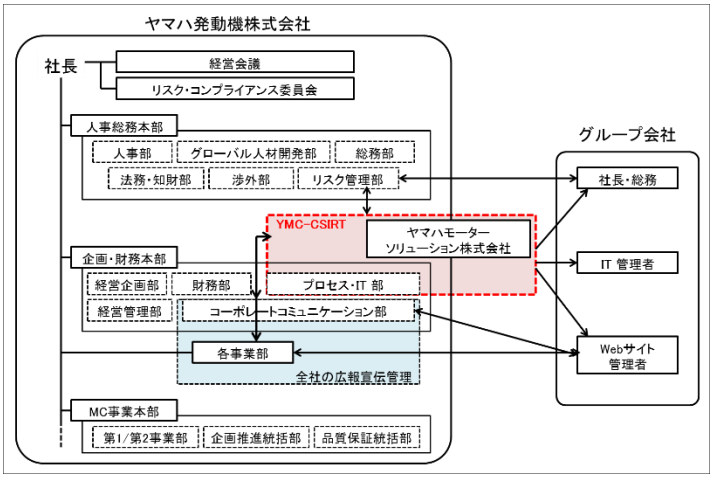
ヤマハ発動機は、自動二輪車をはじめ、ボートや船外機などのマリン製品、スノーモービルをはじめとするレジャービーグルなど、様々な製品を日本のみならず世界に向けて製造販売している大手製造会社である。

Yamaha Motor Corporation Computer Security Incident Response Team（YMC-CSIRT）は、ヤマハ発動機の国内・国外のグループ会社を対象に、Web サイトやシステムにおけるインシデント対応の他、情報収集や警戒情報の発信を行っている。

[図 1] YMC-CSIRT　連絡窓口 原子 拓 氏（右から 1 番目）
ほか YMC-CSIRT のみなさん

3.9.2. CSIRT の体制と保有する権限

YMC-CSIRT は 2013 年 11 月に設立された。メンバーは、企業・財務本部に属するプロセス・IT 部のインフラ運用担当者や、その技術者である。1 名は YMC-CSIRT の専任であるが、それ以外のメンバーはプロセス・IT 部の他の業務を兼務している。



[図 2] YMC-CSIRT の体制図

ヤマハ発動機では、2007 年頃より、リスク管理部を設置して内部統制やリスク管理を実施しており、YMC-CSIRT はリスク管理部とも密接な関係にある。
インシデントなどが発生した際の対応方針を決定する裁量権限については、リスク管理部の所掌業務とされているが、IT リスクに関する権限に関しては YMC-CSIRT が対応している。注意喚起などの対策情報なども YMC-CSIRT から発信される。

3.9.3. CSIRT 活動の成果

3.9.3.1. 経営層への活動報告

リスク管理部からインシデント発生件数などを経営層に報告している。リスク管理部には、100 社を超えるグループ会社の製品に関係するインシデント情報が、YMC-CSIRT を受付窓口として、報告される仕組みとなっている。

3.9.3.2. 社内外に向けた発行文書

特に、社内外に向けて定期的に発行している文書はない。

3.9.3.3. CSIRT における活動評価の指標

YMC-CSIRT の活動を評価する指標として、インシデント発生件数の上限などの目標を設定している。
目標を達成できるかどうかは、毎年大きく変化する攻撃のトレンドの影響を受けるので、活動評価と、予算要求と直結させることは考えていない。

3.9.4. CSIRT メンバーへの教育・研修

3.9.4.1. インシデント対応演習などの実施

YMC-CSIRT では、2015 年にインシデント発生時の対応フローを作成した。現在は、そのフローに沿って実施・確認を行っている段階である。現段階ではインシデント対応演習などは実施していない。

3.9.4.2. 技術者スキルの定量的指標

YMC-CSIRT には、メンバーの技術者スキルを評価したり、資格の取得を推奨したりする制度はまだない。

3.9.4.3. 人材育成

YMC-CSIRT では、明確なスキルマップやキャリアパスなどの教育スキームや研修制度などを用意していない。しかし、人材育成は今後三年間で取り組む課題の 1 つとなっている。OS などを含む基礎的な IT 関

連知識を持ったセキュリティに詳しい専門家や、社内調整ができる人材を育成していきたいと考えている。

3.9.5. CSIRT の体制やサービス、管理機能の見直し時期

3.9.5.1. サービス提供先や提供内容

YMC-CSIRT のサービス提供先や内容は、プロセス・IT 部内で継続的に見直しを検討している。YMC-CSIRT 設立当初は、組織の Web サイトのみが対応範囲であったが、現在は企業内の情報システムなどにも積極的に対応しており、対象範囲は拡大している。今後は、CSIRT のサービス範囲の拡大や、PSIRT 機能の追加などについても検討を進める予定である。

3.9.5.2. セキュリティポリシー等の文書

セキュリティポリシー等の文書の見直しは、リスク管理部が担当している。しかし、情報セキュリティガイドラインについては、事案発生時における YMC-CSIRT の対応に整合した内容にするため、YMC-CSIRT が作成している。

3.9.5.3. 連絡体制

最新の連絡体制を共有する仕組みが全社的に整備されている。

3.9.5.4. インシデント管理ツール

インシデント管理ツールを導入し、対応状況を随時共有できるようになっている。インシデントに関するコミュニケーション手段として、メールだけでなく、掲示板システムを導入している。また、自席にいない場合でも容易に情報共有できる、チャットなどを用いた仕組みも整備している。

3.9.6. まとめ

各事業所からインシデントとして報告される前の早い段階で相談を持ちかけられるなど、組織の協調性や連携意識の高さから YMC-CSIRT は円滑に活動できている。地方都市に本社機能を置いていると、都会との情報格差が生じやすいため、NCA などを通じて、他組織の事例やベストプラクティスを積極的に収集するなど、情報セキュリティに関するリテラシーの向上に努めている。セキュリティの領域は、他組織と競い合うのではなく、ベストプラクティスを共有するなど相互に協力し、マイナス要素をプラスに変えて行く姿勢で取り組んでいる。

4. 構築時に定めておくべき事項

既存 CSIRT へのアンケートとインタビュー結果から、組織内 CSIRT の構築を検討している組織が構築時に定めておくべき事項として次の 6 つが抽出された。

1. CSIRT が提供するサービス範囲
2. CSIRT が持つ権限
3. CSIRT を配置する部署や構成メンバー
4. 連絡窓口（Point of Contact：PoC）
5. 社内に対して CSIRT の活動効果が伝わるような報告体制
6. 定期的な CSIRT 活動の見直し

これらのポイントを順に紹介する。

4.1. CSIRT が提供するサービス範囲

組織によって、事業内容や規模、部門構成、想定しているリスクが異なる。そのため、CSIRT を構築するにあたっては、まず次の項目について検討する必要がある。

- CSIRT が提供すべきサービスやサービスレベル、サービス対象、リスクの許容度
- CSIRT の責任範囲や CSIRT に割り当てるべきリソース、SLA *10など
- 組織の方針を文書化したセキュリティポリシーと、経営層によるその承認

実際にアンケート 2.2.12 の結果でも、6 割ほどの組織でサービスに関する定義が文書化されていた。また、アンケート 2.2.13 の結果では、セキュリティポリシーに関して 8 割を超える組織で文書化され、経営層に承認されていた。

NCA が提供している CSIRT スタータキット*11 では、CSIRT の提供サービスを、「事後対応型サービス」、「事前対応型サービス」、「セキュリティ品質管理サービス」の 3 つに大別している。まずは組織の置かれている状況を考慮し、提供するサービスをいずれかに絞り込むのか、すべてを対象とするのか決める必要がある。

3 つに分類したサービスのうち、多くの CSIRT が提供サービスとして選択していた内容はアンケートによれば次のとおりである。

*10 SLA : Service Level Agreement の略称で、サービスを提供者とその利用者の間で結ばれるサービスのレベル（定義、範囲、内容、達成目標等）に関する合意サービス水準、サービス品質保証
*11 CSIRT スタータキット : http://www.nca.gr.jp/imgs/CSIRTstarterkit.pdf

・事後対応型サービス
- インシデント発生時に迅速に対応するための「インシデントハンドリング」や「アラート」など

・事前対応型サービス
- 平常時に、攻撃活動などがないか監視する「侵入検知」など

・セキュリティ品質管理サービス
- 自組織のセキュリティへの意識を高める「啓発活動」や「注意喚起」など
- インシデント対応等のスキル向上を目的とした「トレーニング」など

これらのサービスが多くの CSIRT で提供されていることから、CSIRT は自組織を守り、起こりうる被害を低減する役割を担っていることがわかる。また、これらのサービスは、既存組織が有するリスク管理体制等で、類似した仕組みがある程度整備されている場合も多く、比較的サービスの導入が容易であると考えられる。まずは、これらを CSIRT のサービスとして活動を開始し、適宜そのサービス提供範囲を自組織に適したものに見直すことが重要であると言える。

4.2. CSIRT が持つ権限

セキュリティインシデントの対応では、組織として迅速かつ的確な意思決定が求められる。そのために、あらかじめ意思決定に責任を持つ部署もしくは人物を決めておくべきである。CSIRT はそのような部署もしくは人物を支援する立場にある。意思決定の判断材料となる情報を調査し、提供するために、どのような権限が必要なのかを明確にすべきである。

例えば、インシデント発生時、リスク回避のためシステムを停止せざるを得ない状況に陥った場合、アンケート 2.2.8 の結果からは、

・CSIRT にシステム停止の権限が付与されている：12%
・CSIRT にシステム停止の権限はなく、助言が行える：85%
・CSIRT にシステム停止の権限はなく、助言も行っていない：3%

との回答が得られた。インタビューの結果からも見て取れるように、必ずしも CSIRT にシステム停止のような強力な権限がなくても CSIRT として機能すると言える。

また、アンケート 2.2.12 から分かるように、約 6 割の組織で CSIRT の権限やインシデントの定義等が文書化されている。CSIRT は他部署と連携して調査を行う場合も多く、どこまで調査を行い、どこまで決定する権限があるかを組織内規定として文書化することにより、インシデント発生時に CSIRT は定義したサービスを円滑かつ適切に提供できる。

4.3. CSIRT を配置する部署や構成メンバー

CSIRT を構成するメンバーが組織内のシステムやセキュリティ知識について精通している場合、インシデント発生時に迅速かつ適切に対応できる。そのため、インシデント発生時に調査等が行いやすい部署に CSIRT を配置し、そのようなメンバーを所属させることで、CSIRT の活動を円滑に進めることができる。

アンケート 2.1.1（構築を主導した部署）、2.2.1（設置された部署）の回答から、多くの組織で情報システム管理部門やセキュリティ対策部門が、CSIRT の構築を主導したり、CSIRT の設置部署として選定されたりする傾向にあることがわかった。これは、通常業務として、システムや機器のメンテナンスや、セキュリティ対応を実施している部署を CSIRT の配置場所としたためと考えられる。しかしながら、必ずしも CSIRT を配置する部署は、こういった部署である必要はないと考えている。定義したサービスを提供するために、各部署と連携しやすい部署に設置すればよいだろう。

また、アンケート 3.1 から、8 割の CSIRT で全ての所属メンバーが正社員であるとの回答が得られたが、必ずしも全員が正社員である必要はない。秘密保持についての取り決めを交わした上で、CSIRT 活動を円滑に進めることができるのであれば、CSIRT を構成するメンバーとして外部委託組織等からの人的支援を受けることに問題はないと考えている。

4.4. 連絡窓口（Point of Contact：PoC）

組織が提供しているサービスに脆弱性があった、または外部ネットワークに向けて不正な通信が発生していた場合、外部組織からセキュリティに関する報告を受けることがある。そうした報告や依頼を正確に受け取り、迅速に対応するための連絡窓口（Point of Contact：PoC）を CSIRT に設置して外部に公表するとともに、報告内容を適切な部署へエスカレーションする体制が求められる。

例えば、アンケート 2.4.1 の結果では、

- 経営層へのエスカレーションルールが明確に文書化されている組織：77%
- 経営層へのエスカレーションルールが文書として明確にされておらず、
  大体の基準が設定されている組織：20%
- 設定されておらず、発生の都度検討している：1.5%
- 未回答：1.5%

との回答が得られ、ほとんどの組織で経営層へのエスカレーションルールが定められ、連絡窓口も整備されていることがわかった。

また、アンケート 2.2.5 の結果では、インタビューを行った組織の多くが、NCA をはじめとした情報共有の枠組みに参加していた。また、知識の獲得や知見の共有等も CSIRT メンバーのモチベーション維持に

役立っているとの声もあった。
PoC には脆弱性情報を含めた脅威情報や、インシデント関連情報等の受付業務だけではなく、他組織と情報共有する役割も求められている。

そのため、PoC には円滑にコミュニケーションが図れる人物が適切であろう。幅広い情報収集だけでなく、攻撃手法やその対策に関して、より詳細な情報を入手できる可能性があるためである。PoC として活動を進めていき、組織内外を問わず信頼を得ていくことで、さらに情報収集のアンテナを広げることができるだろう。

4.5. 社内に対して CSIRT の活動効果が伝わる報告体制

CSIRT の活動を組織内に報告、紹介することは、組織メンバーの意識の向上に貢献したり、CSIRT に対する信頼を得たりすることに繋がると考えられる。それにより、インシデントの前兆の段階で報告が上がるなどの協力により、CSIRT 活動を円滑に進めることが可能となる。

アンケート 2.7.1 の結果から、約半数の組織で、定期的なレポートを発行していることがわかった。その多くが、関連部署や社内全体向けにレポートを発行していた。

また、アンケート 2.4.9 の結果から、約半数の組織で経営層を含む情報セキュリティ委員会等への定期的な活動報告の体制が定められていたほか、インタビューでは、業界に関連した事案や、法整備の影響について資料を適宜まとめ、経営層へ報告している組織もあった。

CSIRT の活動は組織によってはコストセンタとしか見られない一面もあり、CSIRT の活動が適切に評価されず、継続したサービスの提供や人材育成等、さらなる改善のための予算確保が難しい場合がある。こうした状況下であっても、削減効果や活動成果を経営層や社内外に報告することで、CSIRT 活動の有用性について理解を得やすくなる。これを実現するためには、

- 事前に想定されるインシデントに対するリスク評価を実施する
- インシデントの発生から収束までの期間をどの程度短縮できたかを想定する
- リスク評価をもとに、対応コストをどの程度低減できたかを評価する

上記などを行うことによって、CSIRT の活動は組織にとって有益であり、有効な投資であると伝えることが重要である。活動は可能な限り定量的に評価することで、経営層や社内外への CSIRT の有用性をより効率的に伝えられると考えられる。本調査の中では JNSA が定めた評価指標[*12]に基づいてインシデントハンドリングできなかった場合の想定被害額を算定し、報告しているという組織も見られた。

[*12] JNSA (Japan Network Security Association) より公開されている「情報セキュリティインシデントに関する調査報告書」http://www.jnsa.org/result/incident/

4.6. 定期的な CSIRT 活動の見直し

サイバー攻撃の動向や技術の発展、自組織の事業展開の変化などによって、定義した CSIRT のサービス内容や権限では、適切に対応できなくなる場合がある。これを防ぐため、定期的にサービスや CSIRT の活動体制を見直すことが重要である。

アンケート 2.6.1、2.6.2、2.6.3 の結果から、多くの CSIRT で少なくとも年に一回、活動体制の見直しを実施していることが分かる。インタビューの結果からは、その見直しの対象は、サービスや体制、権限など、多岐にわたっていることがわかった。設立して間もない CSIRT では、現状は機能やサービスについて不足はないが今後見直す予定はある、との声があった。
また、組織では定期的な人事異動があるのが通例であり、それは CSIRT でも変わらない。構成メンバーの変更により、今まで提供できていた CSIRT のサービスレベルを保てなくなる可能性があるかもしれない。そのため、メンバーのスキルセットを定義し、求められたサービスレベルを維持するために適切なメンバーを配置することが重要である。スキルレベルを定量的に測ることで、メンバーのトレーニングの必要性や、トレーニングを行う環境の整備、そのための予算確保について経営層に訴えることが可能となる。

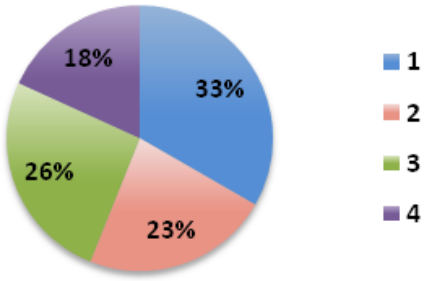
アンケート 3.4 の結果からは、スキルセットが定義されている組織は少数であった。また、インタビューでは、セキュリティ知識だけでなく、プレゼンテーション能力や自組織の事業内容について等、幅広いスキルが CSIRT メンバーに求められているため、教育や研修等の仕組みを設けることを検討しているとの声が多く聞かれた。CSIRT を支えるメンバーを育成するといった観点でも、スキルの定量評価は、大きな課題ととらえている組織が多いと考えられる。

補足 1. CSIRT 構築にかかった期間

アンケート 2.1.5、2.1.6 の結果から構築を開始してから設立するまでの期間を算出した。CSIRT の構築にかかった期間については、半数以上のチームが 1 年以内に設立していることがわかる。

補足 1. CSIRT 構築にかかった期間

#	時期	回答数
1	6 ヶ月未満	22
2	6 ヶ月以上 1 年未満	15
3	1 年以上	17
4	未回答	12



（複数回答なし N = 66）

6 ヶ月未満で CSIRT を構築した 22 組織に限定すると、約 7 割に当たる 15 の組織で、比較的最近である 2014 年以降に構築されていたことがわかった。これは、セキュリティに対する関心の高まりが経営層にも広がっていて、調整が円滑に進んだためではないかと考えられる。また、NCA の活動として、ある程度 CSIRT に関する知見が蓄積され、それが共有されたためではないだろうか。サイバー攻撃に関する早期の対策が求められていることもあるが、しっかりと組織内の定義を策定し、文書化に要する時間についても考慮して、構築していただきたい。

補足 2. CSIRT が配置されている部署と提供サービスの関連

CSIRT が配置されている部署と提供するサービスについて相関分析を行った。多くのサービスにおいて、そのサービスを提供するために内製している、または、外部委託している割合に大きな差異は見られなかった。しかし、CSIRT が配置されている部署を以下の 2 つに分類した場合に、一部のサービスの内製と外部委託の割合に差異が見られた。ただし、情報システム管理部門系とセキュリティ対策部門系にまたがった CSIRT については記載していない。

・情報システム管理部門系に所属しているが、セキュリティ対策部門系には所属していない
　平均メンバー数：11.6 人
　CSIRT の提供するサービスの内製 / 外部委託における割合の特徴：
　- マルウエア解析サービスを提供している組織の多くでは、何らかの業務を外部委託している
　- フォレンジックサービスにおいて内製と外部委託の割合は同程度である

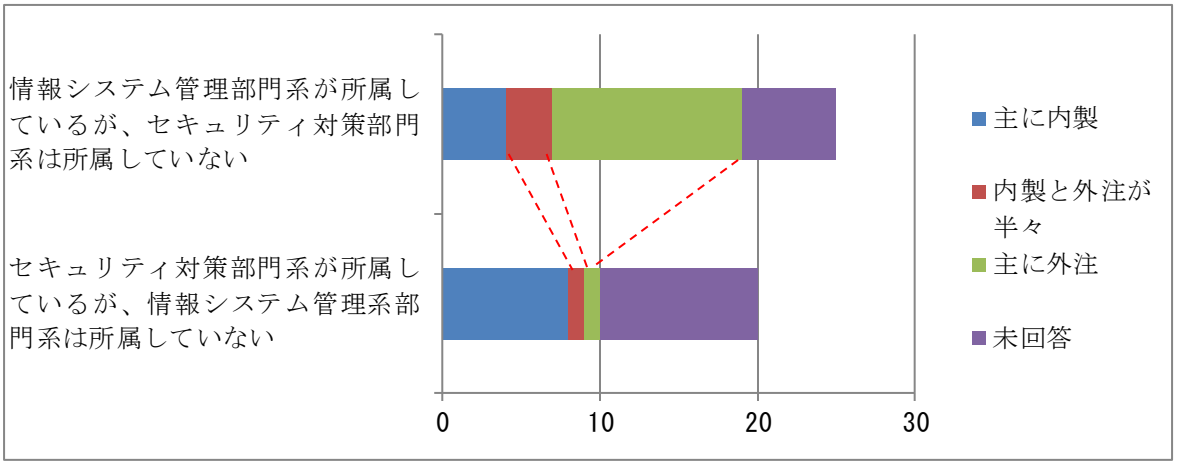
・セキュリティ対策部門系に所属しているが、情報システム管理部門系には所属していない
　平均メンバー数：13.0 人
　CSIRT の提供するサービスの内製 / 外部委託における割合の特徴：
　- マルウエア解析サービスを提供している組織の多くは、内製している
　- フォレンジックサービスにおいて外部委託の割合が低い

結果より、一部ではあるが、CSIRT が配置されている部署と提供しているサービスに特徴が見られることがわかる。これは特定のサービスを提供するために設置する部署が選定された可能性がある。

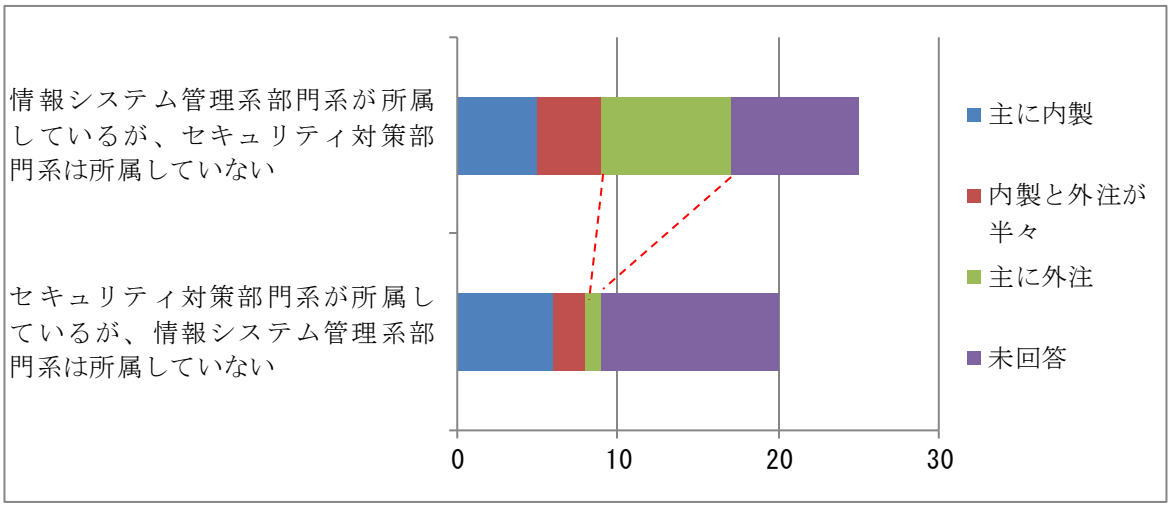
自組織で定義された CSIRT が提供するサービスを実現するために、内製・外部委託にこだわらず必要な方法を選択することが有効である。

補足 2.1. CSIRT が配置されている部署と提供サービスの関連（マルウエア解析）

内製/外注	情報システム管理部門系が所属しているが、セキュリティ対策部門系は所属していない	セキュリティ対策部門系が所属しているが、情報システム管理部門系は所属していない
主に内製	4	8
内製と外注が半々	3	1
主に外注	12	1
未回答	6	10



補足 2.2. CSIRT が配置されている部署と提供サービスの関連（フォレンジック）		
内製/外注	情報システム管理部門系が所属しているが、セキュリティ対策部門系は所属していない	セキュリティ対策部門系が所属しているが、情報システム管理部門系は所属していない
主に内製	5	6
内製と外注が半々	4	2
主に外注	8	1
未回答	8	11



5. 最後に

前章で述べたように、組織内 CSIRT の構築時に定めておかなければならない 6 つの項目が、本調査で明らかになった。しかし、これらの項目は、組織内 CSIRT の運用のために最低限必要な条件だが、これらを満たしていれば組織から求められている活動ができるとは限らない。組織内 CSIRT が効果的に機能するためには、組織内の他の部門や組織外の CSIRT 等との情報共有や連携がきわめて重要である。本章では、このことについて、本調査におけるインタビュー等で得られた知見を交えて述べる。

インタビュー先の CSIRT の一部では、情報の共有や対応に関して、社内の関係部門の協力や理解が得られない等で苦労したが、関係部門を巻き込んだ演習の訓練などの実績を積み重ね、それを組織内に広く展開することで、強固な信頼関係を構築するに至ったとの経験談を聞くことができた。

また、他の組織の CSIRT と信頼関係を構築する重要性を訴える声もあった。NCA やその他のコミュニティ活動に参加し、自組織のインシデント対応の事例を共有し、他の組織と積極的に CSIRT 活動に関する意見の交換や知見の共有を行うことで、自組織への対応を見直すきっかけになったためである。さらに、自ら進んで自組織で取り組んだ改善事例等を他組織と共有することによって、信頼関係の醸成につながり、さらなる情報交換を促進できると考えている。CSIRT 同士の連携により、国内全体の CSIRT の活動がさらに活性化され、結果として自組織の CSIRT の成長に繋がるであろう。

初めて CSIRT を立ち上げようとしている組織には、前章で述べた 6 つの事項を定めることは荷が重いかも知れない。だが、6 つの事項を最初から完璧に定義できていた組織は少ない。立ち上げの段階では、これらの定義に部分的な不備があってもよいので、他の組織の CSIRT の事例を参考にしつつ、まずはスモールスタートでも CSIRT を立ち上げることをお勧めしたい。そして、演習や訓練等を含めた日々の運用や他の組織の CSIRT との情報交換、時には実際のインシデント対応を通じて、CSIRT として必要な技術的な知見や経験値を蓄積し、組織に必要とされ、信頼される CSIRT へと発展することを望む。本報告書がそのための参考となるよう願っている。