

経営リスクと情報セキュリティ  
～ **CSIRT**：緊急対応体制が必要な理由 ～

一般社団法人 JPCERT コーディネーションセンター

2021年11月30日

## 変更履歴

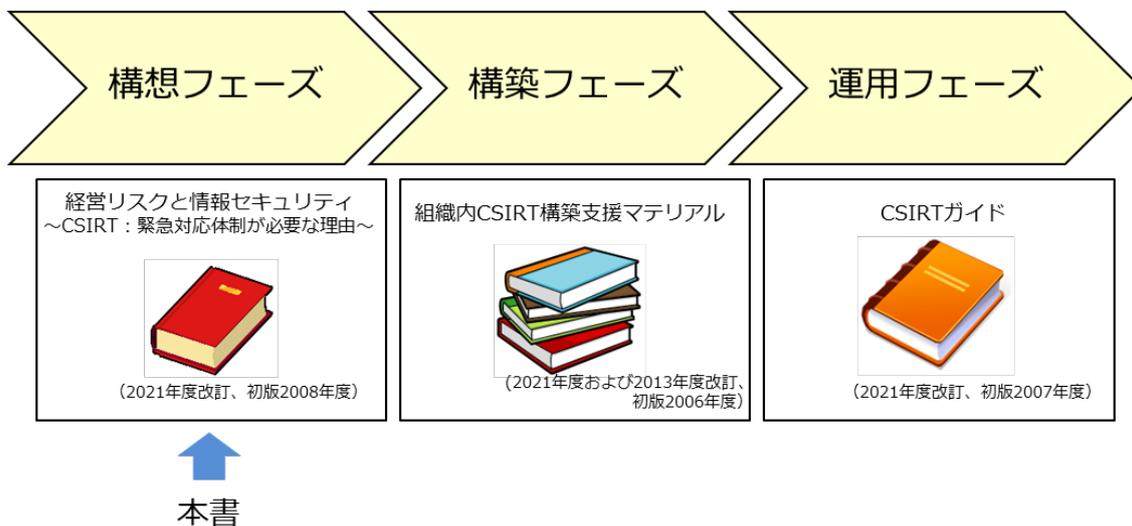
初版：2008年12月

改訂：2015年11月

改訂：2021年11月

## 本書の位置付け

一般社団法人 JPCERT コーディネーションセンター（以下「JPCERT/CC」）が提供する CSIRT 関連資料の構成は以下のとおりです。

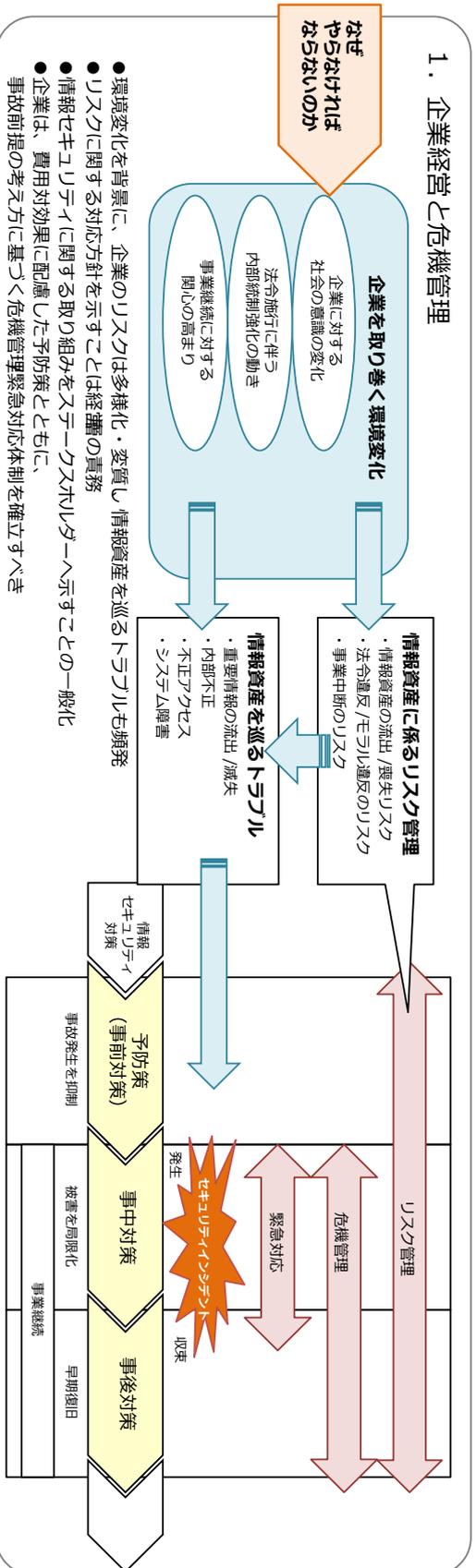


## 目次

|                                   |    |
|-----------------------------------|----|
| 1. 企業経営と危機管理 .....                | 1  |
| 1.1. 企業を取り巻く環境変化 .....            | 1  |
| 1.2. 情報資産を巡るトラブル .....            | 4  |
| 1.3. 情報資産に係るリスク管理 .....           | 9  |
| 1.4. 強化・実現すべき機能 — 危機管理／緊急対応 ..... | 13 |
| 2. 危機管理／緊急対応体制の実現に向けて .....       | 15 |
| 2.1. 危機管理／緊急対応体制の概念 .....         | 15 |
| 2.2. 危機管理／緊急対応体制の意義 .....         | 20 |
| 2.3. 組織内 CSIRT の事例 .....          | 26 |
| 2.4. 実現方法 .....                   | 30 |
| 3. 危機管理／緊急対応体制の活用に向けて .....       | 39 |
| 3.1. フィードバックによる組織強化 .....         | 39 |
| 3.2. アウトソーシングの活用とその限界 .....       | 41 |
| 3.3. 適切な維持・運営のために .....           | 42 |

# 経営リスクと情報セキュリティ ～ CSIRT : 緊急対応体制が必要な理由 ～

## 概要

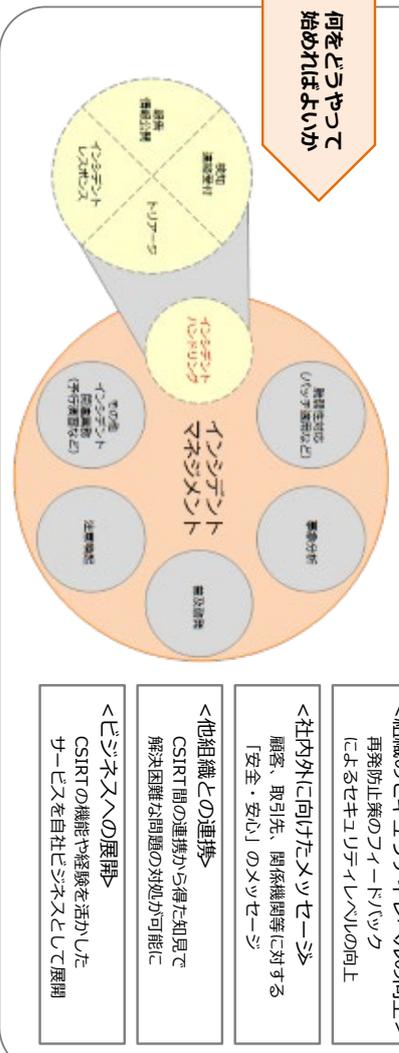


- 環境変化を背景に、企業のリスクは多様化・変質し、情報資産を巡るトラブルも頻発
- リスクに関する対応方針を示すことは経営層の責務
- 情報セキュリティに関する取り組みをステークホルダーへ示すことの一般化
- 企業は、費用対効果に配慮した予防策とともに、事故前提の考え方に基づく危機管理緊急対応体制を確立すべき

## 2. 危機管理/緊急対応体制の実現に向けて

- 緊急対応体制として、組織内CSIRT機能の整備が有効
- 国内外で組織内CSIRTの導入事例が増加
- 既存の体制との役割分担や整合が課題
- 経営層が先導して社内横断的な調整・連携を実現すべき

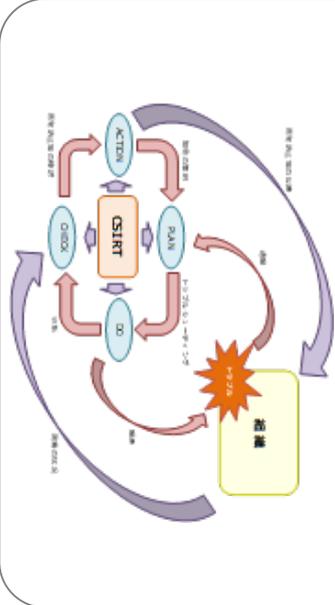
何をどうやって始めればよいか



## 3. 危機管理/緊急対応体制の活用に向けて

- インシデント対応から得た再発防止策を組織にフィードバック
- 要員不足時にはアウトソーシングの活用も視野に入れて検討
- 要員の育成と従業員への啓蒙が鍵
- 投入する資源のバランスに留意

どうやって維持・向上させるか



## 1. 企業経営と危機管理

### 1.1. 企業を取り巻く環境変化

#### (1) 企業に対する社会の意識の変化

近年、企業活動に対する株主や顧客、取引先、従業員、地域社会などの利害関係者の影響力が高まっている。グローバル化した市場への対応が求められることを背景に、それらの利害関係者は企業に対して、公正性と透明性の確保、法令順守、安全、環境保護、利用者の保護、社会的責任や説明責任を果たすことを高いレベルで求めるようになった。また、2006年の公益通報者保護法の施行によって内部告発のハードルが下がり、さらに昨今の SNS やブログ等の情報発信手段の多様化によって顧客を含む一般市民が企業に関する情報を発信することが容易となった結果、企業は以前にも増して社会からの厳しい視線に晒されることとなった。

このような環境下で企業活動に問題が発生したとき、コーポレートガバナンスが脆弱な企業では、問題の発覚の遅延、対応策の誤り、不誠実な対外説明などによってさらなる状況の悪化を招く。さらに、利害関係者が企業に対して訴訟を起こし、経営者の忠実義務違反や善管注意義務違反との判決が出れば、多額の賠償金が課せられるとともに、企業ブランドのイメージ失墜を招き、企業に対する市場からの厳しい評価に直結することになる。

#### (2) 企業の内部統制強化に対する要請

2005年の個人情報保護法の施行を契機として、個人情報の流出がマスコミで大きく取り上げられるようになった。その結果、企業における情報管理体制が法令順守の観点から重視されるようになった。また、同年には、企業の有する知的財産等の営業秘密が不正に持ち出され他社に利用されることを防ぐ目的で、不正競争防止法を一部改正し、営業秘密に係る刑事罰が強化された。これらの法令の施行や、当時日本を代表した複数の大手企業で、有価証券報告書虚偽記載、粉飾決算、企業買収に伴う証券取引法違反などの不祥事が次々と発覚したことを背景に、企業における内部統制の整備・運用を促す法制度が整備された。

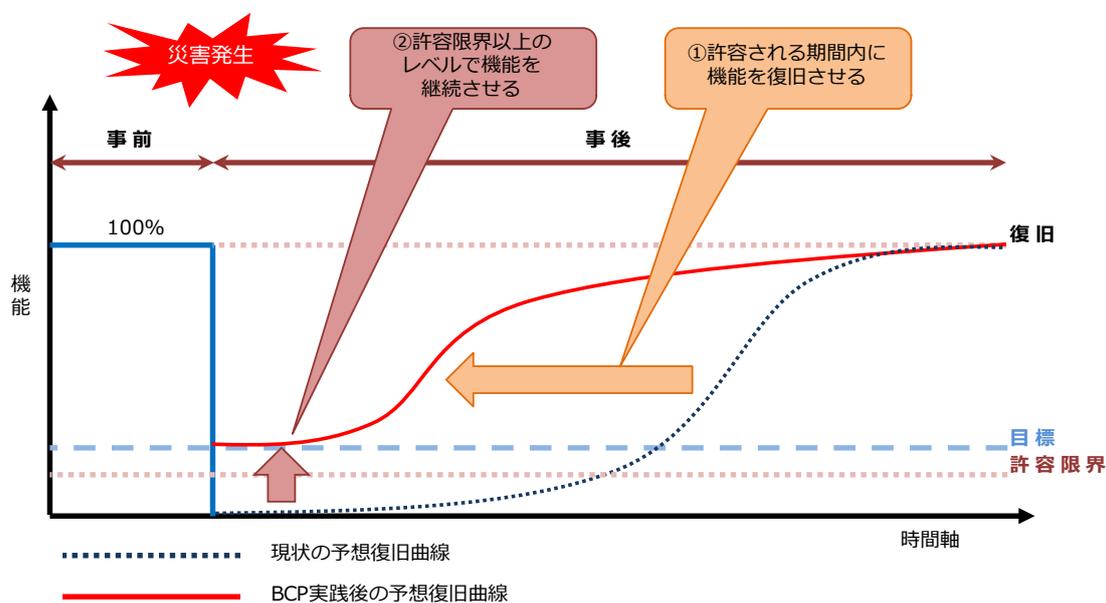
2006年5月に施行された改正会社法では、「損失の危険の管理に関する規程その他の体制」、すなわちリスク管理体制の整備が求められている。特に、業務のIT依存性や情報資産の価値が高い企業は、情報資産に係るリスクが大きく、そうしたリスクの監視や対応組織・手順等の整備など、リスク管理のしくみの確立が必須となる。実際には、ITの恩恵なしにビジネスを進めることができる事業は限られており、法令遵守の観点から見て、大半の企業が情報資産に係るリスク管理を含む内部統制強化を要請されている状況といえる。

また、2007年9月に施行された金融商品取引法では、上場企業に自らの財務情報に係る内部統制の状況について評価・報告させる内部統制報告を求めている。

### (3) 事業継続に対する関心の高まり

近年、わが国では大規模地震等の自然災害を中心に、欧米ではテロの脅威を念頭において、事業継続に対する関心が高まりつつある。例えば半導体業界では、2001年9月11日の米国同時多発テロが契機となって、事業継続管理（BCM：Business Continuity Management）/事業継続計画（BCP：Business Continuity Plan）重視の姿勢にシフトしていった結果、2002年以降、米国のICメーカーによる取引先へのBCM/BCPに関する確認要請が強まり、その影響は業界全体へと広がった。

事業継続を巡る国際標準化の動きについては、2006年11月に英国規格協会（BSI：British Standards Institution）がBCMのガイドラインとなる「BS25999-1：事業継続管理-第1部 実践規範」<sup>1</sup>を発行、国際標準化機構（ISO：International Organization for Standardization）に提案するとともに、翌年11月にはBCMS（事業継続マネジメントシステム）に関する認証基準となる「BS25999-2：事業継続管理-第2部 仕様」を発行した。これらはそれぞれISO22301およびISO22313へ引き継がれ国際規格化されている。



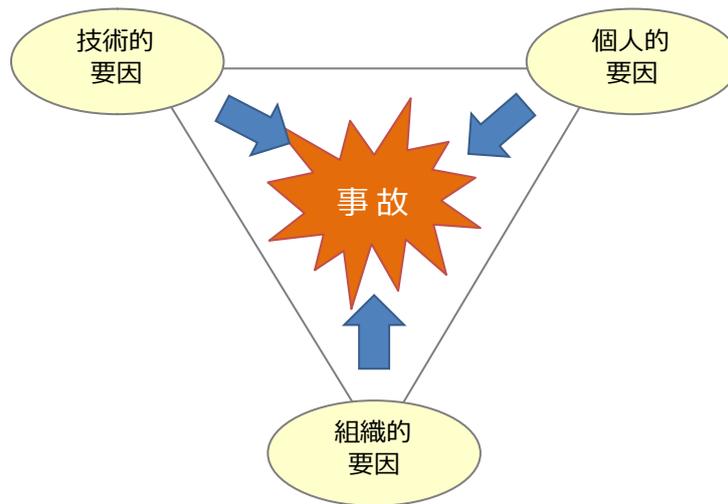
#### 1-1 BCP の概念]

(出典：内閣府「平成24年版防災白書」, 2012/06/19)

学術研究のアプローチでは、「高信頼性組織（HRO: High Reliability Organization）」に関する研究が注目を集めている。研究によると、「重大な事故には組織のあり方が大きく関わっている」とされ、技術的要因や人的要因だけに問題の根拠があるのではないことが指摘され

<sup>1</sup> BS25999-1によると、BCPとは「組織が予め定めた許容可能なレベルで、その重要な活動を実施し続けることを可能とするため、何らかのインシデント発生時に備え、開発され、まとめられ、維持されている文書化された一連の手順及び情報の集合体」であり、BCMとは「組織への潜在的脅威や、そうした脅威が現実となった場合に引き起こされる可能性のある事業運営上の影響を特定する包括的なマネジメントプロセス」とされる。

ている<sup>2</sup>。



[図 1-2 事故分析における3つのパースペクティヴ]

(出典：JPCERT/CC「ICT業界にみる高信頼性組織（HRO）の現状と課題」<sup>2</sup>, 2006/06/20)

<sup>2</sup> <http://www.jpCERT.or.jp/research/>

## 1.2. 情報資産を巡るトラブル

1.1.に示した環境変化の中で、これまで情報資産<sup>3</sup>を巡るトラブル（「情報セキュリティインシデント<sup>4</sup>」という。）が数多く発生してきている。情報セキュリティインシデントは、決して「対岸の火事」ではなく、さまざまな企業で起こっている現実の問題として捉えるべきである。以下に、類型化したパターンを示す。

### (1) 重要情報の流出・滅失

個人情報や顧客から預かった営業秘密等の重要情報について、脅迫や売買目的で不正に持ち出されたケース、業務目的で持ち出したメディアが紛失・盗難に遭ったケース、情報システムや利用する外部クラウドサービスの設定不備により流出したケース、従業員による誤操作・誤送信により流出したケースなどが報告されており、それらの事例には枚挙に暇がない。そうした情報紛失の事態は、社会的信用を失うだけでなく、被害者による集団訴訟により情報流出元企業の損害賠償責任が認定されるなど、金銭的損失にもつながっている。

### (2) 内部不正

従業員や退職者、関係者、委託社員などが故意またはミスなどによって、業務上知り得た情報や権限を利用して組織の情報資産に対して行う侵害行為を指す。情報管理体制の不備（例：担当者が異動してもそのIDのアクセス権を変更していない、特権の使用に対する監視が十分にできていないなど）が事件を誘引していると考えられる。

---

<sup>3</sup> 企業にとって価値を有する情報そのもの（企画、製品開発や営業などの情報、顧客情報、知的財産などのデータベース、資料など）と、その情報を可用化する環境（ソフトウェア（アプリケーション、システムソフトウェア、ユーティリティ）、ハードウェア（コンピューター装置、通信装置、メディアなど）等）を指す。（経済産業省「企業の情報セキュリティガバナンスのあり方に関する研究会報告書」、2005/03）

<sup>4</sup> 望ましくない単独もしくは一連の情報セキュリティ事象、または予期しない単独もしくは一連の情報セキュリティ事象であって、事業運営を危うくする確率および情報セキュリティを脅かす確率が高いもの。（ISO/IEC TR 18044:2004）

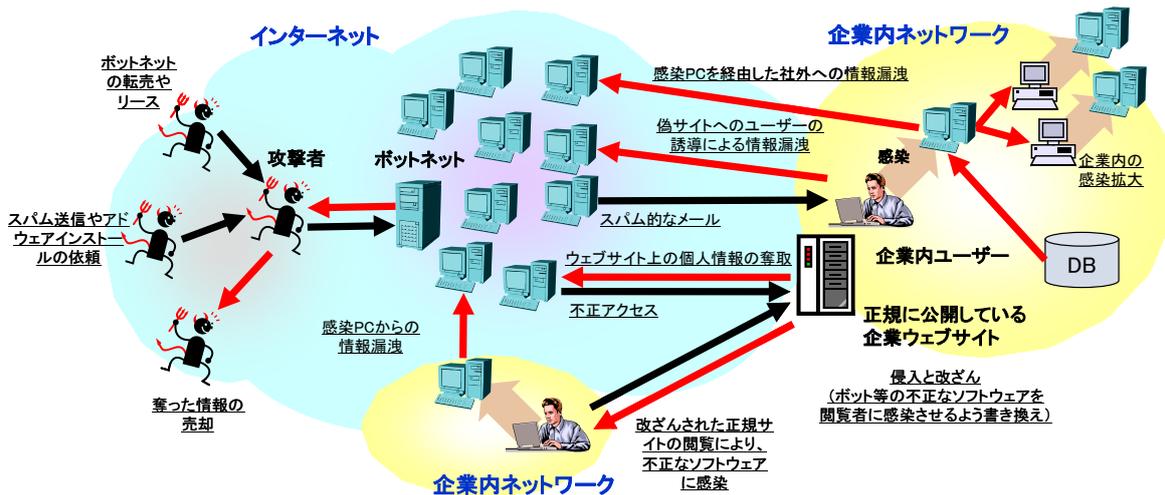
[表 1-1 内部不正インシデントの事例]

| 発生時期     | 概要  |
|----------|---|
| 2014年7月  | 顧客データベースを保守管理する業務委託先の社員が、約3,504万件の個人情報を不正に持ち出し転売した。   |
| 2019年11月 | 秘密情報を含むハードディスクドライブの廃棄処理を委託した会社の担当者が当該ハードディスクドライブを不正に持ち出しオークションサイトで販売した。購入者によってハードディスク内のデータが復元され情報流出が発覚した。 |
| 2021年3月  | 金融サービスのシステム開発や運用の委託先企業の従業員が顧客情報を不正に取得し、過去2年以上に渡り顧客の金融資産を売却して詐取していた。                                       |
| 2021年8月  | 業務委託するITベンダが再委託する国外企業の従業員が、委託元の営業秘密を含む情報を許可なくPCへダウンロードし、外部クラウドサービス上へアップロードしていた。                           |

(出典：各種報道をもとに作成)

### (3) 不正アクセス等

コンピューターウイルスに感染した多数の PC をネットワーク化 (ボットネット) して一斉攻撃や脅迫、迷惑メールの大量送信等を行う行為や、顧客情報の詐取やウイルス頒布のための踏み台化を狙い企業の Web サイトへの侵入を試みる行為が増加している。Web サイトの攻撃は自動化され、目に見えない形で改ざんされるため、今や正規サイトでも信用できない状況にある。2005年5月には、カカクコムが運営する価格比較サイトが不正アクセスによりウイルスを埋め込まれ、アクセスしたユーザーが感染するなどの被害が発生、当該サイトを10日間閉鎖した結果、同社の同年4-6月期は対前四半期約40%の減収となり、同社のサイトに情報提供していたショップの売上にも大きな影響を及ぼした。また、2008年7月に、通販サイトの不正アクセスを受けたサウンドハウスでは、最大97,500件のクレジットカード番号やパスワード情報が漏洩、大手クレジットカード会社から契約を解除されている。さらに、攻撃対象を特定の企業や人物に限定した「標的型攻撃」の脅威や「APT (Advanced Persistent Threat、先進的で執拗な脅威)」の脅威も高まっている。2015年に発生した日本年金機構における侵害事案は APT 的な高度な攻撃手口が用いられたと考えられており、これ以降も、国内の多数の企業や組織において標的型攻撃や APT による侵害が発生している。



[図 1-3 不正アクセス等の攻撃イメージ]

#### (4) システム障害

2000 年代以降、金融機関や証券取引所、航空会社等といった社会インフラを支える重要機関において、システム障害に起因するサービス停止が度々発生するようになった。

2007 年 5 月に発生した航空会社のチェックインシステムの障害は、国内線 130 便の欠航、464 便以上の遅延という事態を招き、約 4 億 5000 万円の減収をもたらしたとされる。

また 2005 年 11 月には、証券取引所の株式売買システムの障害により約 3 時間全銘柄の取引を停止するという、当時は海外でも前例のない異常事態に陥った。さらに、その翌月には証券会社において誤発注問題<sup>5</sup>が発生し、同取引所の社長とシステム担当役員が更迭されるなど、システム障害が同社の経営そのものを大きく揺るがすことになった。

こうした障害の原因は、合併に伴うシステム統合、ソフトウェアバグ、操作ミスなどの内部的要因だけでなく、近年では DoS 攻撃やマルウェアによる破壊行為といった外部からの攻撃に起因する障害も数多く発生しているが、いずれのケースにおいても結果的に深刻な社会的影響をもたらしている。この背景には、業務の IT 依存が高まっていること、情報システムの複雑化・複合化・ブラックボックス化が進み、システム全体の管理が困難になりつつあること、ネットワーク化によりトラブルが思わぬ形で他システムに伝播していくことなどが指摘されている。加えて、事業継続の観点から見たシステムリスクの分析が十分でないことも問題を深刻化させている。

<sup>5</sup> 証券会社が誤って大量の買い注文を出したが、東京証券取引所のシステムの不具合によりその誤発注を取り消すことができず、約 400 億円の損失が発生した。

[表 1-2 大規模なシステム障害の事例]

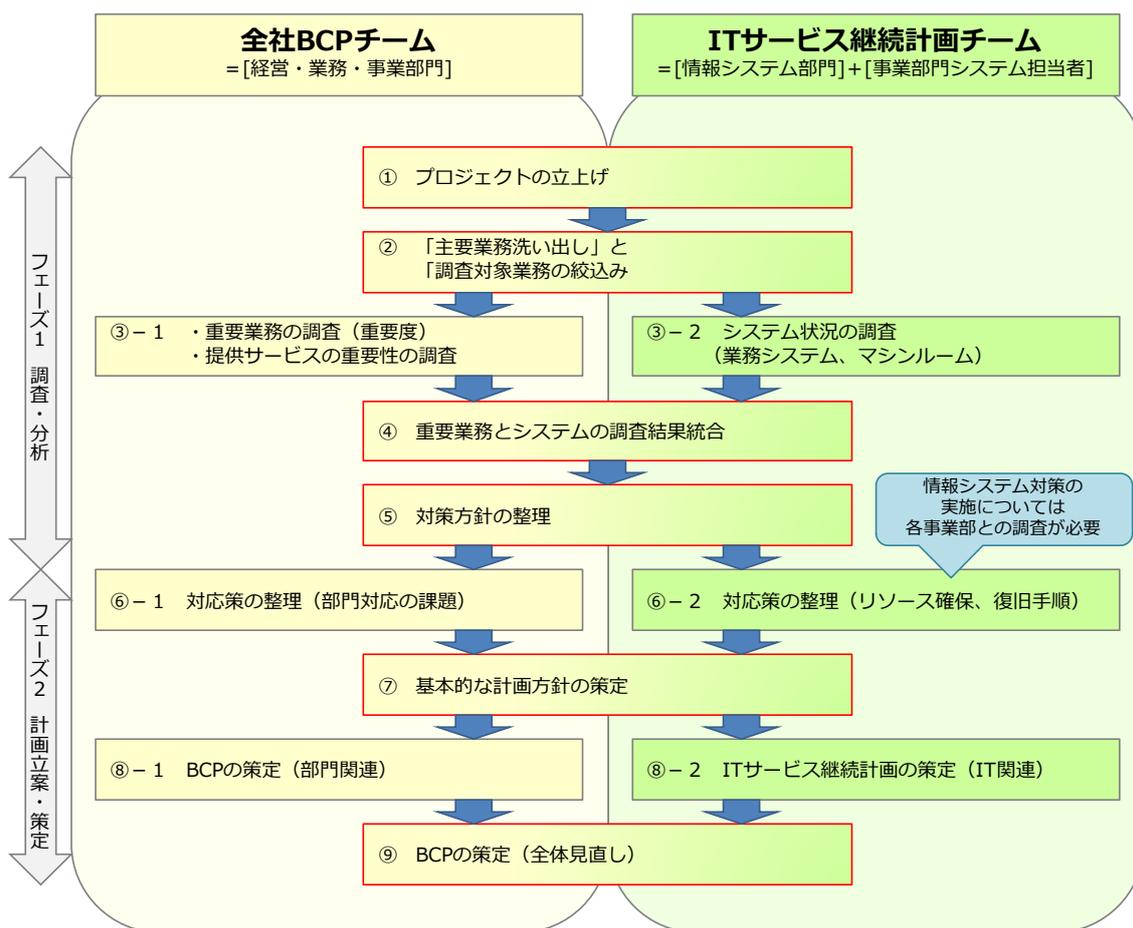
| 発生日             | 事例                      | 被害内容   | 被害範囲・規模   | 原因   |
|-----------------|-------------------------|--|---|--|
| 2002年4月1日       | みずほフィナンシャルグループ大規模システム障害 | 統合後、開業初日からATMの障害、公共料金の自動引き落としなどの口座振替に遅延が発生。                          | 02年5月24日 前田社長は決算発表の記者会見でシステム障害に伴う損害が18億円程度にのぼる見通しを公表。                             | <ul style="list-style-type: none"> <li>修正ミス (ATM)</li> <li>データの不備、プログラムのバグ</li> <li>不十分なテスト</li> <li>システム統合方針決定の遅れ</li> <li>開発スケジュールの遅れ等</li> </ul>  |
| 2005年11月1日      | 東証が一時全機能停止              | 株式売買システムに障害が発生。  | 東証1部、2部、マザーズなど全2520銘柄が停止。(過去最大)   | <ul style="list-style-type: none"> <li>プログラム改変</li> <li>注文数の増大に対応するためのシステム増強でプログラムミスが発生。</li> </ul>  |
| 2006年9月～2008年7月 | NTTグループの光電話に障害          | NTTグループのひかり電話が接続不能。  | 2006年9月には、80万人の利用客に影響。  | <ul style="list-style-type: none"> <li>呼制御サーバのプログラム不具合</li> <li>ひかり電話対応VoIPアダプター部機種のファームウェアの不具合</li> </ul>   |
| 2007年10月12日 早朝  | 首都圏の自動改札におけるシステム障害      | 首都圏のJR東日本、私鉄、地下鉄の合計662駅で自動改札機が作動しないシステム障害が発生。                        | 合計662駅(※)で自動改札機が作動しない。<br>※Suicaを発行する3事業者192駅1328台、Pasmoを発行する13事業者470駅3050台の自動改札機 | <ul style="list-style-type: none"> <li>ネガデータ(不正カード情報)を自動改札機に配信する際、データ量によって2分割することがあるが、配信時に「データ量が特定の値である場合」に読み込みができなくなるものだった。</li> <li>10月12日朝はこの「特定の値」になってしまった。</li> <li>元データを分割したいことを理解して実行すべき処理が実行されず、読み込み不能になった。</li> </ul> |
| 2008年9月14日 早朝   | 全日空のシステム障害              | 14日の始発便から、全国にある51空港のチェックイン端末が認証エラーとなって利用不能。                          | 53便が欠航し、277便が1時間以上の遅延となった。  | <ul style="list-style-type: none"> <li>サーバ側の端末認証プログラムの有効期限が9月14日1時44分までとなり、以後の端末での暗号化機能が作動しなくなった。</li> </ul>   |
| 2012年6月20日      | ファーストサーバー社レンタルサーバーサービス  | レンタルサーバーサービスを利用して約5700件の顧客のメールデータやWebページデータなどを消失。大半のデータについて復旧不可能となる。 | サービスの契約企業約5,700社においてデータ消失   | <ul style="list-style-type: none"> <li>サーバーの保守作業に用いたプログラムに不具合</li> <li>作業手順の不備</li> </ul>  |
| 2015年9月5日       | NTTデータCAFISシステム         | 店舗とクレジットカード会社、金融機関を結ぶシステムに障害。カード決済が不能となる。                            | 約45万件のカード決済処理が停止  | <ul style="list-style-type: none"> <li>大量処理を振り分けるFEPサーバの障害</li> </ul>  |

(出典：各種報道をもとに作成)

なお、経済産業省では、IT事故を対象とした「事業継続計画(BCP)策定ガイドライン」<sup>6</sup>(2005年3月)、またBCMに必要なITサービス継続を確実にするための枠組みと具体的な実施策を示した「ITサービス継続ガイドライン」(2008年9月初版、2014年9月改定版<sup>7</sup>)を公表し信頼性の高い情報システムの構築に向けた取り組みを促している。

<sup>6</sup> [https://www.meti.go.jp/policy/netsecurity/docs/secgov/2005\\_JigyokeizokuKeikakuSakuteiGuideline.pdf](https://www.meti.go.jp/policy/netsecurity/docs/secgov/2005_JigyokeizokuKeikakuSakuteiGuideline.pdf)

<sup>7</sup> [https://www.meti.go.jp/policy/netsecurity/docs/secgov/2011\\_InformationSecurityServiceManagementGuidelineKaiteiban.pdf](https://www.meti.go.jp/policy/netsecurity/docs/secgov/2011_InformationSecurityServiceManagementGuidelineKaiteiban.pdf)



[図 1-4 全社 BCP & IT サービス継続計画の連携例]

(出典：経済産業省「ITサービス継続ガイドライン」, 2012)

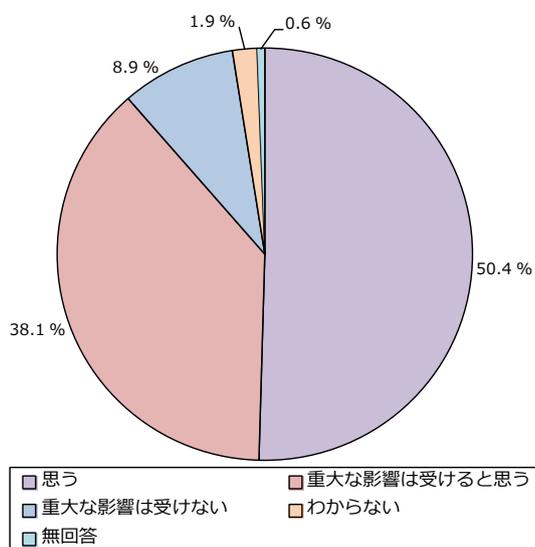
英国では、2006年8月、BCI（Business Continuity Institute）がITに特化した事業継続マネジメントの規格としてPAS 77（IT Service Continuity Management）を発行、これをもとにしたBS 25777:2008がBSIから発行されている。

### 1.3. 情報資産に係るリスク管理

従来、企業では、情報技術（IT）の適用領域が部分的・限定的であったことから、1.2.に例示した情報セキュリティインシデント（情報流出やシステム障害等）が発生しても、その都度、総務部門や情報システム部門、運用サービス会社が場当たりの対応する形でしのいできた。

しかし 1.1.に示したように、近年の社会情勢の変化によって、企業が抱える情報資産に係るリスク<sup>8</sup>は多様化・変質しており、そうしたリスクへの対処を誤ると、金銭的損害や訴訟、信用失墜といった企業経営を揺るがす事態にまで発展しかねない。

少なくとも企業の情報システム部門には、このような状況が認識されていると考えられる。財団法人日本情報処理開発協会（JIPDEC）の調査<sup>9</sup>によると、88.5%もの企業が、情報資産に係るリスクによって経営的に重大な影響を受ける可能性を認識していることがわかる。ただし、それが経営層まで浸透しているかという論点については、意見の分かれるところであろう。



[図 1-5 情報資産に係るリスクが経営に重大な影響を与えるか（情報システム部門）]

（出典：JIPDEC「平成 17 年度情報セキュリティに関する調査報告書」, 2006/03）

情報資産に係るリスクを具体化すると、以下のように整理される。

<sup>8</sup> 「リスク」の定義には文献によって幅があるが、本書では「ある脅威が、資産又は資産のグループの脆弱性につけ込み、そのことによって組織に損害を与える可能性」（JIS Q 13335-1:2006「情報通信技術セキュリティマネジメントー 第 1 部：情報通信技術セキュリティマネジメントの概念及びモデル」）、「企業にとってのリスクとは、狭義には『企業活動の遂行を阻害する事象の発生可能性』と捉えられる」（経済産業省「リスク新時代の内部統制 リスクマネジメントと一体となって機能する内部統制の指針」, 200/06）、「何らかの要因により金融機関等の業務にとって好ましくない事象が発生し、それにより金融機関等の経営、ひいては社会に損失を及ぼすかもしれないという不確実性」（財団法人金融情報システムセンター「金融機関等のシステムリスク管理入門」, 2008/06）などを引用する。

<sup>9</sup> <https://www.jipdec.or.jp/archives/publications/J0001236>

### (1) 情報資産の流出・喪失リスク

従来から情報資産に係るリスクの中心として挙げられていた事項であり、自社の従業員の管理ミスや不正アクセス、コンピューターウイルス感染など自社の問題が流出・喪失の原因であった。

しかし、近年は、自社の情報管理だけでなく、サプライチェーン傘下の企業間、また、受委託の関係企業間における情報共有が脆弱点となって、技術情報をはじめとする情報資産の流出・喪失リスクが高まっている点が懸念される。つまり企業においては、取引先や関係会社等との戦略的提携に基づき、円滑かつ創発的な情報共有を実現し、効果的・効率的にバリューチェーンを形成する必要がある。その一方、相手の情報資産管理に問題がある場合、情報流出を回避して企業価値を守ることは企業として当然の選択である。特に、取引先の機密情報やユーザーの個人情報・機微（センシティブ）情報<sup>10</sup>などの重要情報を共有する場合、委託元は委託先との契約でその保護を要請するだけでなく、委託先において必要なセキュリティレベルが確保されているか、何らかの手段で担保することも必要となる。

すなわち、情報資産の流出・喪失リスクを抑制しつつ、バリューチェーンの価値を最大化する取り組みが要求される。

### (2) 法令違反・モラル違反のリスク

法令違反のリスクとしては、個人情報保護法や金融商品取引法、不正競争防止法<sup>11</sup>など、情報管理と密接な関係にある法制度だけでなく、労働法や派遣法といった労務管理の法制度と情報セキュリティポリシーの間で矛盾が生じトラブルを招く可能性にも留意する必要がある。

また、ITサービスの多様化に伴い、違法ではないが適正とは言い難いケースも増えていくと考えられる。例えば、顧客情報の流出が発覚した際、原因究明とさらなる流出を防ぐため Web サイトの運用を一旦停止すべきところを営業上の理由で継続したケース、公知の脆弱性を内包したソフトウェアを頒布したケースなどが挙げられる。

さらに、適正性の観点から、企業は、情報セキュリティインシデントが発生した場合に、取引先や顧客、株主等の利害関係者に対して適切に説明することを求められる。例えば、機密情報の流出が発覚した場合、経営者は個人の問題として片付けるのではなく、情報管理体制の何が問題でこうした事態に陥ったのか、同様な問題を二度と起こさないためにどのように改善するのかといった点に言及し、利害関係者に説明することが重要である。

<sup>10</sup> 「政治的見解、信教（宗教、思想及び信条をいう。）、労働組合への加盟、人種及び民族、門地及び本籍地、保健医療及び性生活、並びに犯罪歴に関する情報」（経済産業省「経済産業分野のうち信用分野における個人情報保護ガイドライン」）

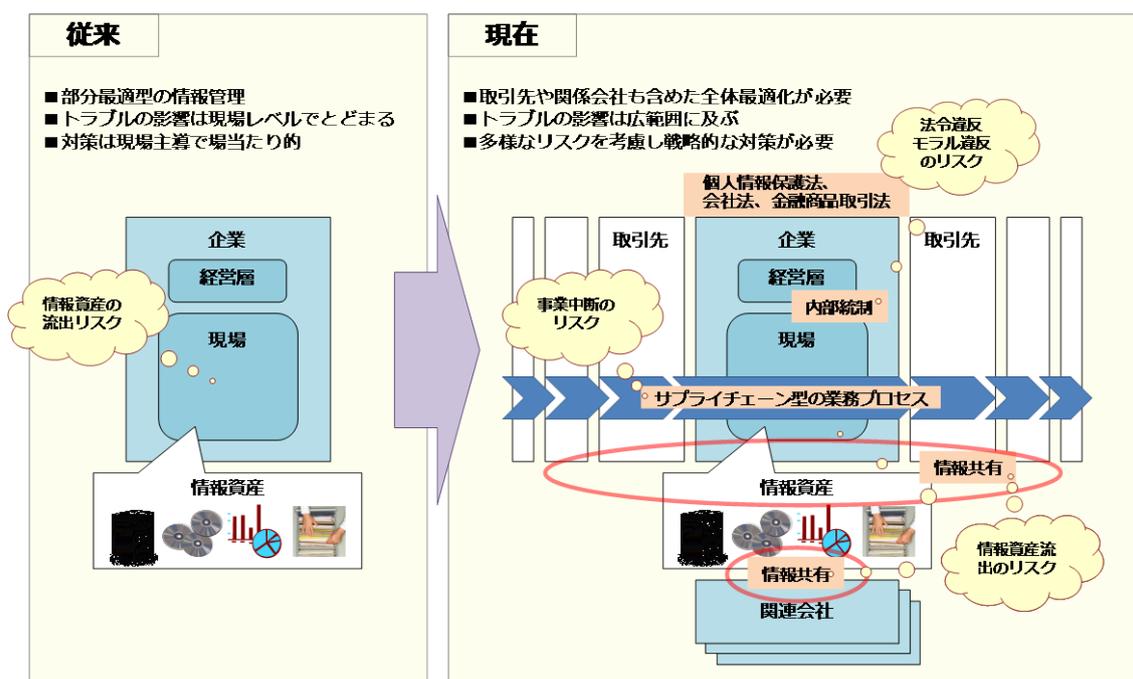
<sup>11</sup> 不正競争防止法については、被害企業が法令違反となるわけではないが、そうした事象がマスコミ等で取り上げられて、情報管理が脆弱な印象を与えてしまうこともリスクとして想定している。

### (3) 事業中断リスク

1.2.で例示したように、システム障害などの問題で事業が停止すれば、取引先や顧客に大きな被害を与え、自社の経営を危うくすることも考えられる。社会的影響の大きい重要インフラ業種だけでなく、最近では製品製造・販売の一連の業務プロセスを構成するサプライチェーン傘下の企業の部品供給がボトルネックになるケースも見られる。

また、IT 統制のオーナーシップに基づき、情報インフラは情報システム部門主導、アプリケーションは現場主導の形で責任を分担している企業の場合、各所の業務効率化が優先され全体最適のための情報セキュリティ対策がなごりにされたり、アプリケーションレベルのトラブルに対する迅速な対処が困難な状況<sup>12)</sup>に陥る可能性がある。

(1)～(3)に示した情報資産に係るリスク変化のイメージを [図 1-6] に示す。



[図 1-6 情報資産に係るリスクの変化]

情報セキュリティ対策とは、上記のような情報資産関連のリスクをコントロールするための方策である。すなわち、これから起こるかもしれない問題に備える対策であり、どのような対策を選択するかは企業のリスク管理の方針に基づいて判断すべき事項である。極端に言えば、リスクの存在を無視して対策そのものを行わないという選択も、リスクを過大評価して必要以上の対策を打つ選択も、リスクの存在を許容せず IT の利活用や重要情報の保有そのものを放棄するという選択もありうる。いずれにせよ、そうしたリスクに関する対応方

<sup>12)</sup> 例えば、情報システム部門は業務やデータの重要性が判断できず、現場はトラブルシューティングのためのスキルや知見がない場合、両者が連携できるスキームがないと、問題解決には時間を要する。

針を示すことは経営判断の範疇であり、現場任せ・情報システム部門任せにしては、経営責任を果たせないことを十分理解しなければならない。

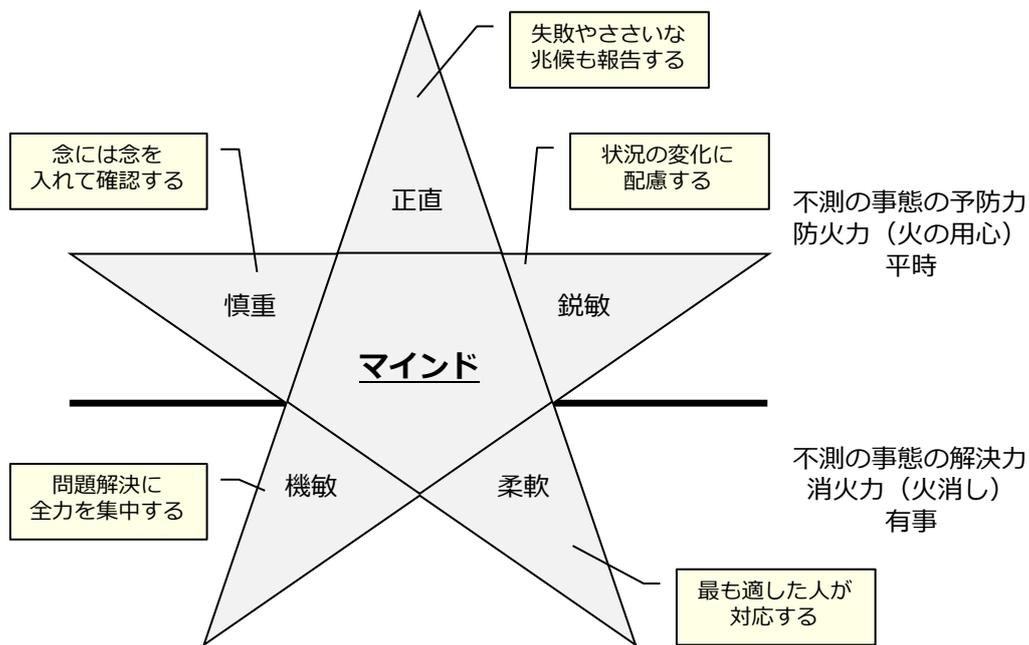
産業構造審議会 情報セキュリティ基本問題委員会「中間とりまとめ～企業における戦略的な情報セキュリティガバナンスの確立に向けて～」<sup>13</sup>（2008年6月，経済産業省）では、「企業経営の主目標は、株主、顧客、取引先、従業員、社会等の利害関係者に対して責任を果たすこと、つまり、『企業価値の向上』及び『社会的責任の遂行』にあり、これを支える重要な取組の一つにリスク管理が位置づけられる。様々なリスクのうち、情報資産に係るリスクの管理を狙いとして、情報セキュリティに関わる意識、取組及びそれらに基づく業務活動を組織内に徹底させるための仕組み（経営者が方針を決定し、組織内の状況をモニタリングする仕組み及び利害関係者に対する開示と利害関係者による評価の仕組みを指す）を構築・運用することを情報セキュリティガバナンスと位置づける。」として、経営層がリスク管理の一環として情報資産に係るリスクを把握し、適切に方針を決定するとともにそうした取組みを開示する、情報セキュリティガバナンスの確立を提唱している。

---

<sup>13</sup> [https://www.meti.go.jp/policy/netsecurity/docs/secgov/2008\\_TyukanTorimatome.pdf](https://www.meti.go.jp/policy/netsecurity/docs/secgov/2008_TyukanTorimatome.pdf)

#### 1.4. 強化・実現すべき機能 — 危機管理／緊急対応

明治大学 中西（2007 ほか）の研究によると、「高信頼性組織<sup>14</sup>」の条件として、平時の対応力（不足の事態の予防力、防火力（火の用心））とともに、有事の対応力（不測の事態の解決力、消火力（火消し））が挙げられている（〔図 1-7 参照〕）。



〔図 1-7 高信頼性組織の組織プロセス的要件〕

（出典：中西晶「高信頼性組織の条件 その理論と実装」,OR 学会安全・安心研究会資料, 2008/08/29）

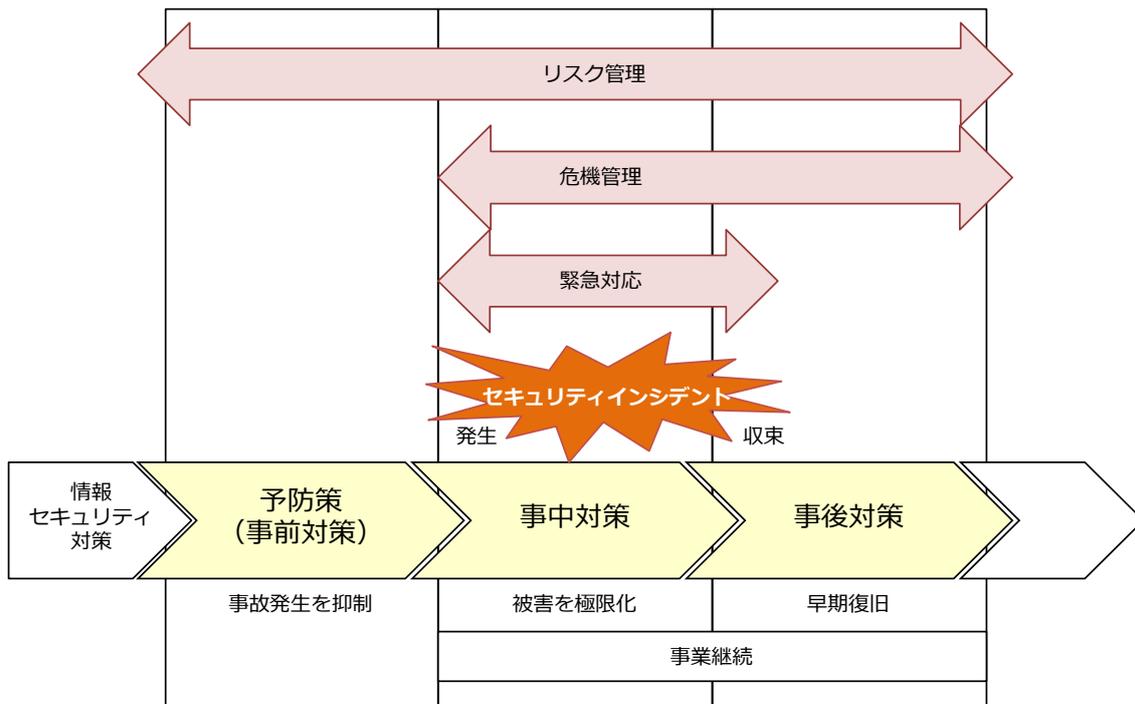
したがって、企業が情報セキュリティ対策に臨む方針として重要なのは、リスクがゼロにならないことを受け入れ、費用対効果に配慮した適切な予防策（情報セキュリティインシデントの発生を抑制する対策）を選択するとともに、「不測の事態は常に起こりうるもの」すなわち「事故前提」の考え方にに基づき、インシデント対応に重点を置いた事中・事後対策（被害の局限化、早期復旧、事業継続）を打ち出すことにある<sup>15</sup>。

ただし、これまでの事中・事後対策は、予防策に比べその場凌ぎの印象が否めない。今、求められているのは、情報セキュリティインシデントに対処するための戦略的・計画的な機能、すなわち危機管理／緊急対応体制の確立である。内部統制やリスク管理体制、事業継続、利害関係者への説明責任を念頭に社内の情報セキュリティに関するルール・体制を見直し、望ましい危機管理／緊急対応体制を強化・実現すべきであろう。

〔図 1-8 にリスク管理と危機管理／緊急対応、情報セキュリティ対策の関係を示す。〕

<sup>14</sup> 中西晶（2007）『高信頼性組織の条件』生産性出版

<sup>15</sup> 特に、攻撃側の動機が近年、愉快犯から金銭目的のビジネスへとシフトしていることや、特定の組織・個人を狙った攻撃（標的型攻撃）、未公表の脆弱性を悪用するゼロデイ攻撃など、攻撃手法が高度化していることを考慮すれば、すべての攻撃から全従業員を守りきることは非常に難しい状況にある。



[図 1-8 リスク管理、危機管理、緊急対応の位置づけ]

## 2. 危機管理／緊急対応体制の実現に向けて

1章では、企業経営の観点から、危機管理／緊急対応体制の必要性について述べた。本章では、こうした機能を実現するための方針、体制、手順等について説明する。

### 2.1. 危機管理／緊急対応体制の概念

#### (1) 危機管理（インシデントマネジメント）

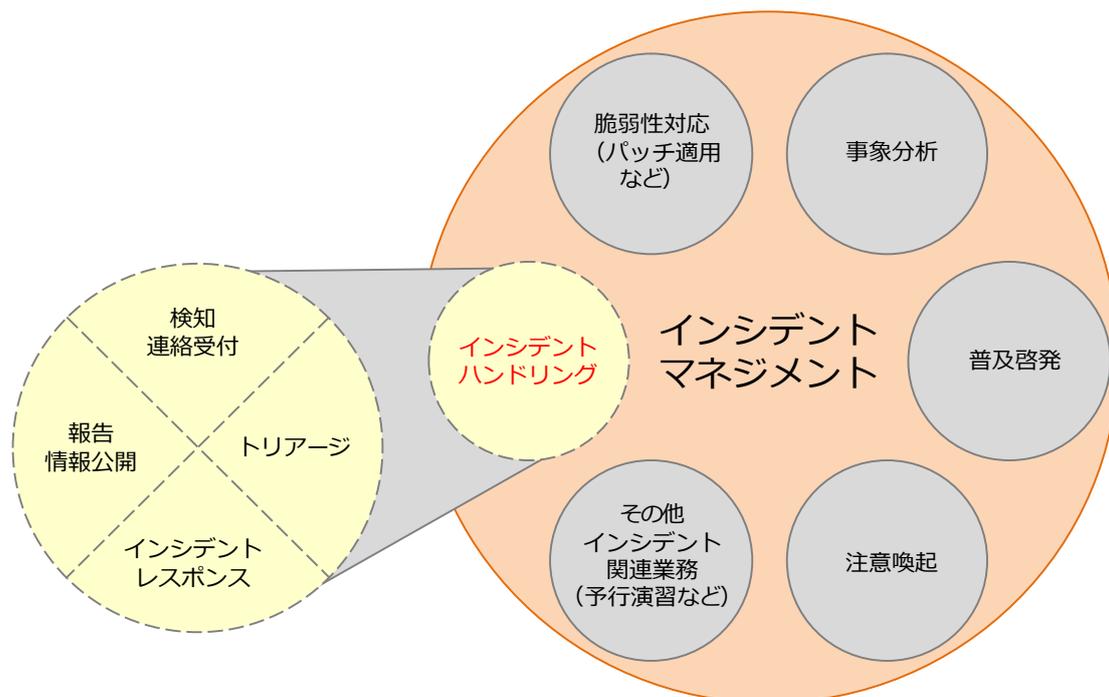
一般に「危機管理」とは、企業経営や事業活動、ブランドに、重大な損失をもたらす、もしくは社会一般に重大な影響を及ぼすと予想される事態を「危機」と考え、万一危機が発生した場合に損失を極小化するための活動と位置づけられる。

情報セキュリティ上の危機管理体制（インシデントマネジメント）には、そうした危機管理を実現するために、次のような機能の提供が期待される。

- ・ **脆弱性対応（パッチ適用など）**  
脆弱性情報を収集し、自組織のシステムに対する脅威を分析して、必要に応じてパッチ（修正ソフト）の適用や設定変更を行う。
- ・ **緊急対応（インシデントハンドリング）**  
情報セキュリティインシデントが発生した際に、通報を受け、状況を踏まえ対処方針を決定し、問題解決を行い、インシデントを収束させる。
- ・ **事象分析**  
発生した情報セキュリティインシデントに関するデータを分析し、原因や再発防止のための改善点を明らかにする。
- ・ **普及啓発**  
情報セキュリティインシデントの発生を低減するため、エンドユーザーである従業員向けに教育・啓発活動を行う。
- ・ **注意喚起**  
情報セキュリティインシデントに繋がるミスや情報セキュリティインシデントの発生時に、関係先に必要な注意喚起を行い、インシデントの被害拡大を防ぐ。
- ・ **その他のインシデント関連業務（予行演習など）**  
例えば、対処計画が適切に機能するか確認するため、模擬的に情報セキュリティインシデントの発生を設定し、関係者の行動を検証する演習を行うことが考えられる。

中でも、「事故前提」の観点から企業において強化・実現すべき機能として、情報セキュリティインシデントの発生から収束までの対応を行う「緊急対応（インシデントハンドリン

グ)」が注目される。



[図 2-1 危機管理（インシデントマネジメント）と緊急対応（インシデントハンドリング）]

## (2) 緊急対応（インシデントハンドリング）

緊急対応（インシデントハンドリング）は、主に以下の4つの機能で構成される。

### a) モニタリング（事象の検知、報告受付）

リスク管理体制を実装する上での課題の一つがモニタリングである。リスク管理の一環として、情報資産に係るリスクの状況を把握する方法は、ITの業務利用環境や社内の管理体制によって大きく異なる。ただし、一般に情報セキュリティインシデントについてはユーザー部門や情報システム部門でも状況把握が困難なケースが多く、実害が生じるまで発覚しにくい傾向がある。また、関連部署のスタッフが予兆に気づいても、相談・報告すべき先がわからず、結果的に放置されることも考えられる。

したがって、情報セキュリティインシデントを検知、あるいはその報告を集約して、意思決定者の判断を支援するよう状況を分析するモニタリング機能が必要となる。

### b) トリアージ（事実確認、対応の判断）

事業継続性を重視する企業組織では、全体フレームであるBCP（事業継続計画）を策定し、事故発生時にはその手順に則って対処することが一般的である。ただし、その際、実務上問題となるのはBCPの発動基準である。物理的被害が明らかな場合にはBCP発動の判断が

容易だが、情報セキュリティインシデントの場合、事象そのものの事実確認や判断に手間がかかるため、BCPの発動が遅れるケースが想定される。

また、BCPにおいては、中断による影響が大きい事業・業務を中心にBIA (Business Impact Analysis) を行い、対応の優先順位をあらかじめ明確にしておくが、情報セキュリティインシデントの対応方針を適切に判断する体制がなければ、そうした優先順位に沿った対応の実行性が損なわれることは否めない。

#### c) インシデントレスポンス（分析、対応、エスカレーション、連携）

被害の局限化、早期復旧、事業継続を実現するために最も重要なのは、インシデントの分析や対応等のインシデントレスポンス機能である。しかし実際には、情報インフラの運用を担当する情報システム部門に割り付けられ、事業における当該システムの役割や復旧の条件、情報流出時の影響規模などを把握しないまま、権限もなく対応を迫られているケースが少なくないと考えられる。

適切なインシデントレスポンスを行うためには、トラブルシューティングの技術だけでなく、関係者間の連携や合意形成、内部統制を考慮したエスカレーション<sup>16</sup>の手続きなど、調整能力とそれを支えるルールが不可欠である。

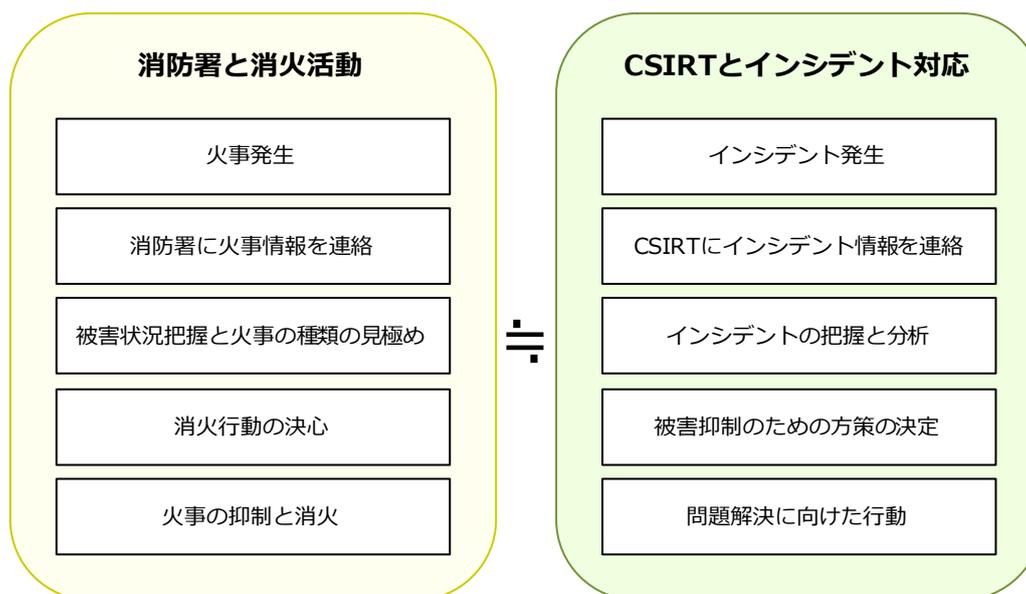
#### d) リスクコミュニケーション（報告・情報公開）

インシデント対応は、ともするとインシデントが発生したことの隠蔽も含む、内向きの処理に終始しがちである。しかし、適法性だけでなく適正性にも配慮すれば、利害関係者に対しリスクの存在やインシデントの影響、原因分析や再発防止策を積極的に説明することは極めて重要である。したがって、インシデント対応に関する報告や情報開示など、リスクコミュニケーションを適切に行う機能を強化することが望ましい。

これら4つの機能の一部もしくは全部を有し、インシデントハンドリングの実務を担う体制のことを、「CSIRT: Computer Security Incident Response Team」と呼ぶ。CSIRTは、発生した事象を検知およびその報告を受け、組織におけるインシデントと判断でき、解決に向けた対応および調整ができる機能あるいはチームであり、特にインシデントの発生抑止あるいは解決のため、外部との技術的な連携ができる機能あるいはチームでもある。CSIRTのイメージは、例えば火事に対する「消防署」と位置づけられる。

---

<sup>16</sup> 業務に関連する事項について、より上の階層に報告し、対応すること。



[図 2-2 CSIRT の基本的な役割]

なお、CSIRT では上記のインシデントハンドリングだけでなく、組織の状況や方針に沿って、多様なサービス（例：脆弱性<sup>17</sup>ハンドリング、アーティファクト<sup>18</sup>ハンドリング、セキュリティ監査、監視、教育／トレーニング等）もカバーしているケースが見られる。例えば、CERT/CC<sup>19</sup>では、CSIRT のサービス分類例を [図 2-3 のように整理している。

<sup>17</sup> ソフトウェア等において、コンピューターウイルス、不正アクセス等の攻撃により機能や性能を損なう原因となり得る安全上の問題箇所。

<sup>18</sup> システムとネットワークの探査や攻撃に関与した、もしくはセキュリティ対策を無効化する目的で使用された可能性のある、システム内で発見されたファイルまたはオブジェクト。コンピューターウイルス、トロイの木馬プログラム、ワーム、攻撃スクリプト、ツールキットなどがある。

<sup>19</sup> Computer Emergency Response Team / Coordination Center。1988年11月のモーリス・ワーム (Morris worm) の流行を契機に、カーネギー・メロン大学 ソフトウェア工学研究所 (Software Engineering Institute) 内に設置された世界最初の CSIRT。

| 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   |
|--|--|--|
| <ul style="list-style-type: none"> <li>・アラートと警告</li> <li>・インシデントハンドリング                             <ul style="list-style-type: none"> <li>- インシデント分析</li> <li>- オンサイトでのインシデント対応</li> <li>- インシデント対応支援</li> <li>- インシデント対応調整</li> </ul> </li> <li>・脆弱性ハンドリング                             <ul style="list-style-type: none"> <li>- 脆弱性分析</li> <li>- 脆弱性対応</li> <li>- 脆弱性対応調整</li> </ul> </li> <li>・アーティファクトハンドリング                             <ul style="list-style-type: none"> <li>- アーティファクト分析</li> <li>- アーティファクト対応</li> <li>- アーティファクト対応調整</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>・告知</li> <li>・技術動向監視</li> <li>・セキュリティ監査または審査</li> <li>・セキュリティツール、アプリケーション、インフラ、およびサービスの設定と保守</li> <li>・セキュリティツールの開発</li> <li>・侵入検知サービス</li> <li>・セキュリティ関連情報の提供</li> </ul> | <ul style="list-style-type: none"> <li>・リスク分析</li> <li>・ビジネス継続性と障害回復計画</li> <li>・セキュリティコンサルティング</li> <li>・意識向上</li> <li>・教育 / トレーニング</li> <li>・製品の評価または認定</li> </ul> |

[図 2-3 CERT/CC による CSIRT サービスの分類例]

(出典：CERT/CC「コンピュータセキュリティインシデント対応チーム(CSIRT)のためのハンドブック」<sup>20</sup>)

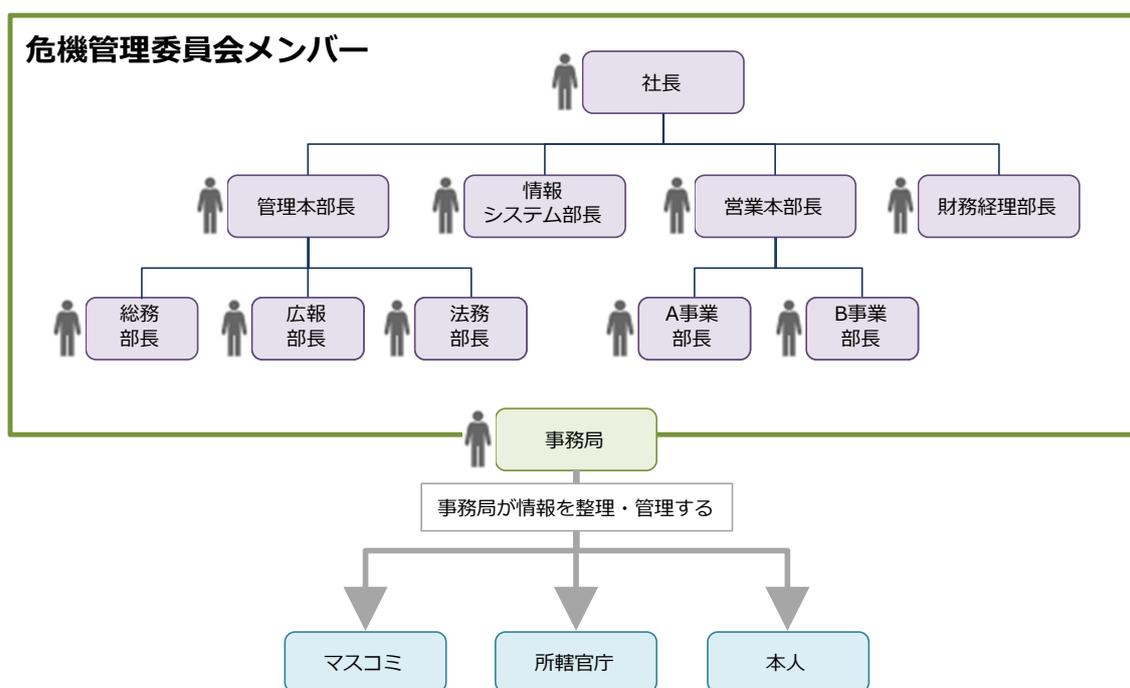
これらの詳細な解説については関連資料に委ねることにして、本書では、以降、CSIRT を中心に、危機管理／緊急対応体制を組織内に構築する際の考え方や留意点などを経営的観点から明らかにする。

<sup>20</sup> [https://www.jpcert.or.jp/research/2007/CSIRT\\_Handbook.pdf](https://www.jpcert.or.jp/research/2007/CSIRT_Handbook.pdf)

## 2.2. 危機管理／緊急対応体制の意義

### (1) 危機管理体制の意義

企業組織における危機管理の体制は、リスク管理体制に包含されている形態が一般的で、具体的には、委員会等の会議体が設置されるケースが多いと考えられる。これは、個人情報漏洩のような危機的事態の管理には、社長やリスク管理担当役員など経営層直轄の委員会において、組織の主要な部門の責任者が横断的に調整・連携する必要があるためである。委員会は常設とは限らず、インシデントの発生時のみ立ち上がるアドホックな体制であることも珍しくない。[図 2-4 に、委員会形式の場合の構成例を示す。



[図 2-4 危機管理委員会メンバー例]

(出典：丸山満彦「個人情報流出 有事のときの危機管理 第 2 回 情報漏えいに備えた社内体制の整備」<sup>21</sup>, ITmedia, 2005/03/03)

ただし、「日本企業の場合、生産や営業など各現業部門でトラブル処理を行うことが伝統的に進められてきており、遠い本部にあるリスク管理部門に人員を充実しても、いざというときに動けるのかという疑問もある。」<sup>22</sup>といった指摘もあり、情報セキュリティインシデントがもたらす影響の大きさ・深刻さについて認識が乏しい場合には、危機管理体制が適切に機能しない可能性もある。

<sup>21</sup> <https://www.itmedia.co.jp/enterprise/articles/0503/03/news003.html>

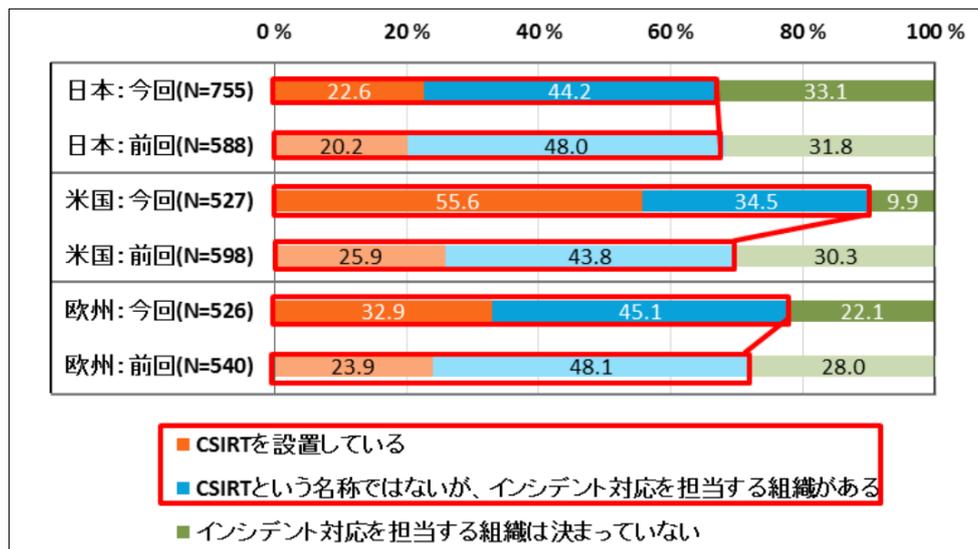
<sup>22</sup> 大村岳雄「備進む企業のリスク管理とコンプライアンス体制の現状と今後の課題について」, 一般社団法人リスクマネジメント協会 [https://www.arm.or.jp/pdf/resource/ronbun/2008/today\\_vol47\\_2\\_oomura.pdf](https://www.arm.or.jp/pdf/resource/ronbun/2008/today_vol47_2_oomura.pdf)

(2) 緊急対応体制の意義

a) 既存の体制の限界と CSIRT

企業における危機管理委員会などの危機管理体制の整備は、会社法に係る法令順守（リスク管理体制の整備）の一環としても有効である。

一方、緊急対応体制については、国内においても CSIRT やそれに準ずるインシデント対応体制の設置が進んできているもののその伸びは鈍化しており、未だ有効なインシデント対応体制を備えていない企業も多い（[図 2-5 参照]）。



[図 2-5 CSIRT の設置状況]

(出典：(独) 情報処理推進機構, 「企業の CISO や CSIRT に関する実態調査 2017」)

有効なインシデント対応体制を備えていない企業では、実際に発生した情報セキュリティインシデントへの対応を既存の枠組み・体制でカバーしていると推察される。実際には、情報セキュリティインシデントを「IT の問題の一つ」と位置づけて、情報システム部門に対応を求めることが多いと考えられる。このように、情報セキュリティインシデント対応についての責任や権限を明確にしないまま、消去法的に情報システム部門に背負わせている場合、経営層は次のような問題が顕在化することに留意しなければならない。

● 情報セキュリティインシデントに対処する情報システム部門のモチベーションが弱い

運用がミッションである情報システム部門にとって、情報セキュリティインシデント対応は「余計な」業務であり、その対応が適正に評価されないため、担当者の積極的な取り組みが期待できない。

● 情報システム部門に権限のない対処はできない

ユーザー部門で外部委託して構築した業務アプリケーションの場合、情報システム部門

にはアクセス権がなく、問題の切り分けや原因追及が困難である。また、複数の部署に影響するケースや対外的な調整・対応が必要なケースにおいても、十分な権限がなく、解決に向けた調整ができない。

## ●情報セキュリティインシデント対応に係る知見を共有できない

担当者が都度場当たり的に対処しているため、インシデント対応を通じて得られる知見・ノウハウが散逸し、スキルが効率化・高度化しない。特に、昨今の潜在化した攻撃により、調査分析は時間を要するため、対応する側のノウハウが乏しいと、業務を中断する状況に陥ることも考えられる。

## ●情報セキュリティインシデントの報告窓口が曖昧で、たらいまわしになる

現場で情報セキュリティインシデントを発見しても、報告すべき部署がはっきりしていなかったり、たらい回しにされるなどして、適切に処理が進まなければ、対応が遅れることになる。

したがって、経営層は、危機管理体制（危機管理委員会等）と連動する形で、緊急対応体制として情報セキュリティインシデント対応を担当する部署やチームの責任と権限を明確化し、事中・事後対策の強化を図ることが重要である。

また、情報セキュリティインシデントの種類・規模によっては、原因究明のためのサービス停止、法的観点からの対応指針の策定、対外説明、顧客へのお詫びなど、幅広い活動が求められることから、経営層のイニシアチブのもとで、関連部門との横断的な調整・連携が可能な体制を整えるとともに、その活動が通常の業務に優先して行えるよう、必要な権限を付与することが必要である。

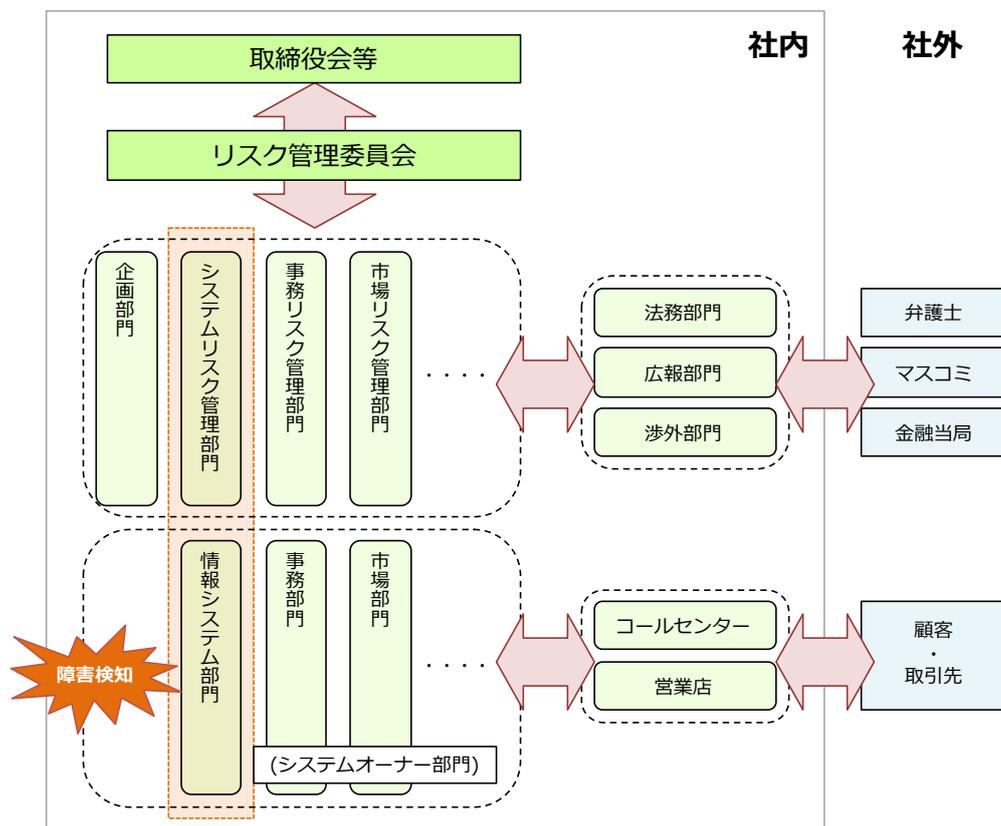
このような体制を具現化したものがCSIRTである。なお、CSIRTは「インシデント対応を専門に行う組織」である必要はなく、「インシデント対応を担当する機能」として設置することが重要である。実現化の形態もさまざま、専任スタッフを中心とした独立部署、企業・部署横断型の仮想チーム、数人の専任スタッフのみで構成するケースも見られる。

例えば、財団法人金融情報システムセンター（FISC）では、システムリスクを統括する「システムリスク管理部門」が、リスク管理の一環として障害情報<sup>23</sup>の把握、分析を担当するモデルを提唱している<sup>24</sup>。ここで、システムリスク管理部門は、独立の立場から情報システム部門等の他部門に対する牽制機能を働かせることが期待されており、「特に重大な障害等については、情報システム部門と協力しつつ、取締役会等・リスク管理委員会などへの報告を

<sup>23</sup> ここで扱う障害等には、システムのダウン・誤作動に限らず、不正アクセス、コンピューターウイルス等不正プログラムによる攻撃等意図的なもの、および火災・停電などの災害を含む。

<sup>24</sup> FISC「金融機関等のシステムリスク管理入門」,2008/06

適宜行うことが望ましい」とされている。



[図 2-6 障害発生時の対応体制 (例)]

(出典：FISC「金融機関等のシステムリスク管理入門」, 2008/06)

## b) 国際標準と CSIRT

ISMS (情報セキュリティマネジメントシステム) の国際標準である ISO/IEC 17799:2000 (JIS X 5080:2002) 「情報セキュリティマネジメントの実践のための規範」は、2005年に改訂され ISO/IEC 17799:2005 (JIS Q 27002:2006) となり、その後、ISO/IEC 27002:2007へと移行した。2005年の改訂では、11領域の一つとして「情報セキュリティインシデントの管理」が追記されている。

[表 2-1 JIS Q 27002:2006 における「情報セキュリティインシデントの管理」の構成]

|        |                         |
|--------|-------------------------|
| 13.    | 情報セキュリティインシデント管理        |
| 13.1   | 情報セキュリティの事象及び弱点の報告      |
| 13.1.1 | 情報セキュリティ事象の報告           |
| 13.1.2 | セキュリティ弱点の報告             |
| 13.2   | 情報セキュリティインシデントの管理及びその改善 |
| 13.2.1 | 責任及び手順                  |
| 13.2.2 | 情報セキュリティインシデントからの学習     |
| 13.2.3 | 証拠の収集                   |

(出典：JIS Q 27002:2006 「情報セキュリティマネジメントの実践のための規範」より引用)

13.2.1 では、情報セキュリティインシデントに対する対応を確実にするために、責任体制および手順を確立することが推奨されている。「情報セキュリティインシデントの管理」は、ISMS の認証基準である ISO/IEC 27001:2005 (JIS Q 27001:2006) 「情報セキュリティマネジメントシステム—要求事項」においては認証を取得するための要件の一つであるが、CSIRT の整備・活用することで、この項目を適正にクリアすることが期待できる。

また、「情報セキュリティインシデントの管理」については、他に技術文書として ISO/IEC 27035-1<sup>25</sup>および ISO/IEC 27035-2<sup>26</sup>が作成されている。同文書では、インシデント対応チーム (IRT : Incident Response Team) を軸に、

- ・ 情報セキュリティインシデントの検出および報告、査定
- ・ 影響の予防および低減、並びに、影響からの回復のための適切な管理策の活性化を含んだ、情報セキュリティインシデントへの対応
- ・ 情報セキュリティインシデントからの学習および予防的管理策の探求、情報セキュリティインシデント管理の総合的な取り組みに対する改善

といった取り組みを、プロセスモデル (計画準備段階、利用段階、レビュー段階、改善段階) を用いて確立することを示している。

#### c) 事業継続と CSIRT

BCM の実装における重要なポイントとして、インシデント対応体制の整備が求められている。例えば、BCMS の認証基準である ISO 22301 (1.1(3)参照) では、「事業継続手順の確立及び実施」の項において「Incident response structure (インシデント対応体制)」が挙げられている。つまり、ISO 22301 の認証を取得するためには、必要な能力を有するインシデ

<sup>25</sup> ISO/IEC 27035-1:2016 “Information security incident management — Part 1: Principles of incident management”

<sup>26</sup> ISO/IEC 27035-2:2016 “Information security incident management — Part 2: Guidelines to plan and prepare for incident response”

ント対応要員の特定や要員に求められる要件を明示した文書を用意することが要求される。ここで想定されているインシデントの種類は多岐に渡るが、情報セキュリティインシデントも対象に含まれることは言うまでもなく、業務のIT依存度が高い分野においては、BCMSの一環としてCSIRTを整備することが必須と考えられる。

また、BCMに必要なITサービス継続を確実にするための枠組みと具体的な実施策を示した経済産業省「ITサービス継続ガイドライン」(1.2(4)参照)では、「ITサービス継続計画」の構成要素の一つであり、緊急事態発生時における情報システムの迅速な復旧・再開に向けた体制および対応方法を定める「事後対応計画(緊急時対応計画)」の中の記載項目例として「緊急時対応体制」が挙げられている。

以上のことから、CSIRTはITに係る事業継続の観点から必要不可欠な機能と位置づけられているといえよう。

#### d) フォレンジック<sup>27</sup>とCSIRT

日本ネットワークセキュリティ協会(JNSA)が公表した「2018年情報セキュリティインシデントに関する調査報告書」によると、2018年に新聞やインターネットニュースなどで報道された個人情報漏えいインシデントの20.3%が不正アクセスによるものであり、2.9%が内部犯罪・内部不正行為によるものとされる<sup>28</sup>。こうした状況を背景として、情報セキュリティインシデントに関する情報や証拠の収集・保全を行うフォレンジック機能が注目を集めている。フォレンジック機能の存在を明示することによって抑止効果を得るとともに、組織のネットワーク内で発生したデータ侵害行為の追跡や、トラブルの際に従業員の無実を証明することも可能である。

情報セキュリティインシデントに関する証拠の収集については、ISO/IEC 27002:2007(JIS Q 27002:2006)においても推奨されているが([表 2-1 参照)、実装に際してはCSIRTの活動においてカバーするのが最も効率的である。逆に、今やCSIRTの役割となりつつある法的な問題の解決、情報詐取等の事実関係の確認のためには、フォレンジックが不可欠とされる。セキュリティベンダーが提供するフォレンジック調査サービスの利用はすでに広く行われており、また一部の大規模企業ではフォレンジック機能を実装したCSIRTが登場している。

なお、犯罪捜査への貢献を想定すると、裁判所で採用される立証可能な分析過程の管理を文書化する方法で行う必要がある。

---

<sup>27</sup> システムに加えられた変更を明らかにし、セキュリティの侵害に至った事象の流れを再構築できるように、セキュリティが侵害されたコンピューターシステムから証拠を収集、保全、文書化、および分析すること。

<sup>28</sup> JNSA「2018年情報セキュリティインシデントに関する調査報告書」  
<https://www.jnsa.org/result/incident/2018.html>

## 2.3. 組織内 CSIRT の事例

### (1) 国内の状況

わが国で最初の民間企業における組織内 CSIRT は、日立製作所において 1998 年にプロジェクトとして産声を上げ、2004 年 10 月にグループ全体の CSIRT として活動すべく組織化され、設立された「HIRT (Hitachi Incident Response Team)」である。

2007 年 3 月には、CSIRT 間の緊密な連携体制を実現し、共通の問題を解決することを目的とした日本国内の CSIRT コミュニティー「日本シーサート協議会 (NCA)」<sup>29</sup>が発足した。NCA は、発足当初は 6 チーム<sup>30</sup>であったが、国内企業での CSIRT 設置が進むにつれて加盟組織数を伸ばし、2021 年 10 月現在では 400 以上のチームが加盟している。発足当初は任意団体であった NCA は、CSIRT の普及と加盟組織数の伸びを背景に、2020 年 4 月に一般社団法人化してその活動の強化を図っている。

2011 年頃からわが国の企業を対象としたサイバー攻撃が確認され、企業におけるサイバーセキュリティ対策の必要性が徐々に認知されはじめた。以後、わが国政府が、対策の一環としての CSIRT 設置について言及するようになり、2015 年には経済産業省が「サイバーセキュリティ経営ガイドライン<sup>31</sup>」において、経営課題として CSIRT の整備の必要性に言及し、体制の整備を求めた。これらは企業における CSIRT 構築の大きな後押しとなった。

### (2) 海外の状況

日本国内において CSIRT の認知度は年々高まり、企業において組織内 CSIRT の構築が進んでいるが、海外でも CSIRT が多数存在している。

そうした CSIRT が集まる国際コミュニティも複数運営されている。に主要な国際 CSIRT コミュニティーを記す。こうしたコミュニティに組織内 CSIRT が参加する主な目的は、コミュニティ活動を通じて、相互の信頼関係を形成し、問題解決に必要な知見・ノウハウを共有することにある。

---

<sup>29</sup> <https://www.nca.gr.jp/>

<sup>30</sup> HIRT、IIJ-SECT、JPCERT/CC、JSOC (現在は LACERT と改称)、NTT-CERT、SBCSIRT

<sup>31</sup> [https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM\\_Guideline\\_v2.0.pdf](https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf)

[表 2-2 主要な国際 CSIRT コミュニティーの概要 <sup>32,33,34</sup>]

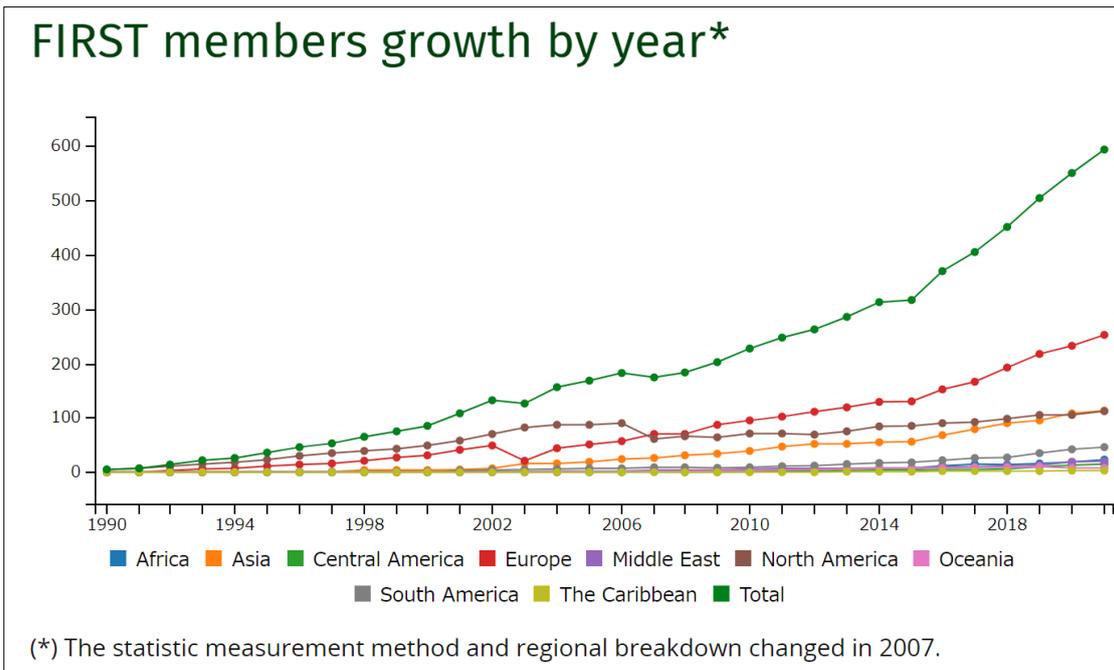
|  |   |
|--|---|
| FIRST (Forum of Incident Response and Security Teams)                  | 米国 CERT/CC を中心に 1990 年に設立された、世界各国の CSIRT が加盟するコミュニティ。メンバー間で技術情報、ツール、方法論、プロセス、ベストプラクティスの開発/共有や、インシデントレスポンスチーム創設に係る啓発活動を全世界的に行うこと等をミッションとしている。                                    |
| TF-CSIRT (The Task Force on Computer Security Incident Response Teams) | ヨーロッパを中心とした世界各国の研究教育ネットワークに関係する CSIRT などが集まるコミュニティ。欧州の研究教育用ネットワーク (NREN) の運用組織をメンバーとする連合組織 GÉANT のタスクフォースとして運営されており、メンバー間での知見の共有等を行っている。CSIRT のスタッフ向け教育教材「TRANSITS」を開発し、公開している。 |
| APCERT (Asia Pacific Computer Emergency Response Team)                 | 2003 年に作られた、アジア太平洋地域の CSIRT コミュニティー。地域内で発生したインシデントへの対応協力の円滑化やサイバー脅威等に関する情報共有・技術交流の推進を目的に活動している。メンバーは National CSIRT が中心だが、Corporate Partners として企業の組織内 CSIRT 等も加盟している。          |

[表 2-3 FIRST の加盟組織数の遷移]

<sup>32</sup> <https://www.first.org/>

<sup>33</sup> <https://tf-csirt.org/>

<sup>34</sup> <https://www.apcert.org/>



(出典 : <https://www.first.org/about/history> )

さらに、2008年3月には、日本国内のFIRST加盟10チームが中心となって、単独CSIRTでは解決が困難な事態に対してCSIRT間の強い信頼関係に基づいた迅速かつ最適な対応を実施する体制作りを推進するための意見交換の場となることを目指したワークショップ「Joint Workshop on Security 2008, Tokyo」<sup>35</sup>が開催された。

<sup>35</sup> <http://www.nca.gr.jp/ws2008/>

### (3) CSIRT 構築の狙い・期待効果

組織内 CSIRT を有する組織における CSIRT 構築の狙い・期待効果は、主に以下の 5 点が挙げられる。

#### a) 関連情報の集約と効率的活用

CSIRT をインシデント対処に係る指令と管理の中核として位置づけ、情報集約や対処活動の効率化を図るとともに、インシデント対応活動を通じて得られたノウハウを CSIRT に集約・蓄積することで、インシデントに強い組織を実現する。また、CSIRT を整備することによって、トラブルシューティングの円滑化だけでなく、経営層に対する効率的な報告のしやすさ、縦割りから横断型への体制転換といった組織改革にも寄与する効果が期待される。

#### b) 組織のセキュリティレベルの向上

CSIRT によりインシデントに対応するだけでなく、その再発防止を押し進め、組織内のセキュリティレベルを高める。CSIRT においてインシデントの原因分析から得られた改善方策を社内にフィードバックし、社内のセキュリティレベル向上を図る。また、そうした知見を他組織と共有したり、製品開発や顧客サービスのセキュリティレベル向上に反映する取り組みも見られる。

#### c) 社内外に向けたメッセージ

社内外に対する「安全・安心」のメッセージとして、CSIRT を活用する。例えば、顧客や取引先に向けた信頼のブランドイメージの確立や、関係機関に向けたコンプライアンスの姿勢のアピール、また内部統制・グループ統制強化の手段として、CSIRT が活用である。

#### d) 他組織との連携

自組織の CSIRT が CSIRT 間の連携体制における POC (Point of Contact) となることで、自らの経験だけでは解決困難な問題についても他組織の知見を活用することで対処が可能になる。また、CSIRT 同士の連携を通じて、適正なレベル感を相対的に把握することができる。

#### e) ビジネスへの展開

IT ベンダーやセキュリティサービスプロバイダー等の事業者においては、CSIRT の先進的な機能や専門性、インシデント対応経験を活かしたサービスを、セキュリティインシデント対応支援やセキュリティ監視 (SOC) 等のアウトソーシングサービスとしてビジネス展開できる可能性がある。

## 2.4. 実現方法

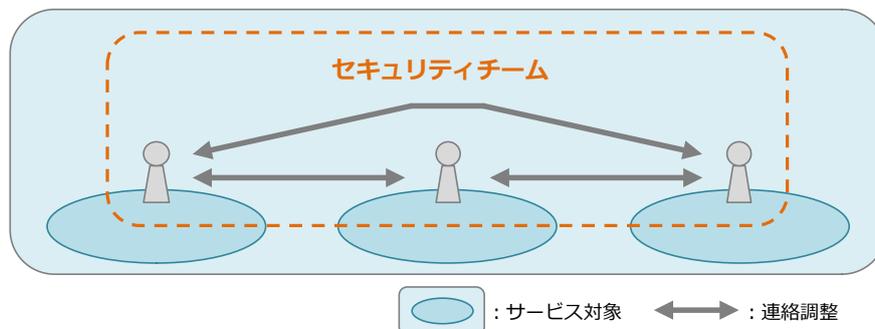
### (1) 組織内 CSIRT の実装モデル

組織内 CSIRT の実装に係る検討は、情報システム部門などに一任するのではなく、会社全体のプランニング・デザインに関わる経営企画部門・総務部門等が担当することが望まれる。なぜなら、CSIRT の実装により、経営層への効率的なレポート、ブランドイメージの確立といった全社規模の効果が期待できるためである。

組織内 CSIRT の実装形態は、以下のモデルに分類できる。

#### a) セキュリティチーム

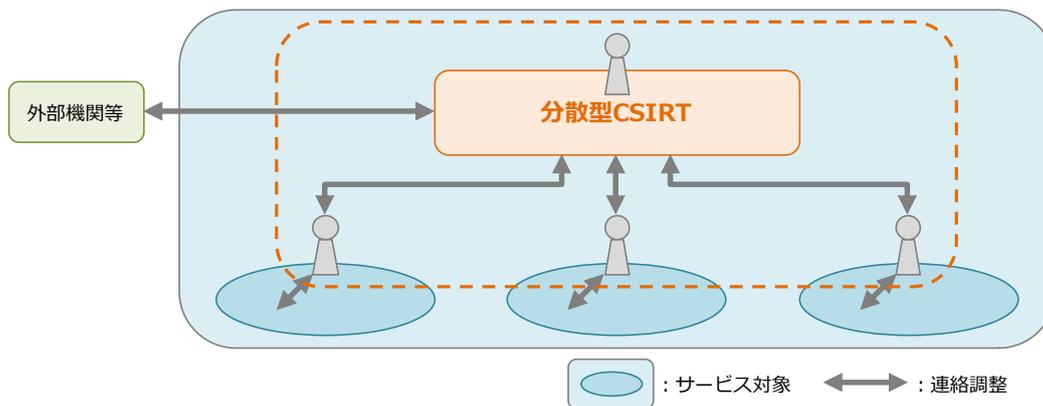
既存の IT 部門やセキュリティ担当チームを要員も含めほぼ流用する形で、要員は通常の業務の一部として、インシデントハンドリングの活動を行う。実際には、インシデントが発生する都度、対応チームが結成されるケースが多いと考えられる。設置に係るコストや手間は最も少なく実施が容易である反面、既存業務との調整や現場との力関係などが制約となっており、限定的な対応に留まらざるを得ないことが多い。



2-7 セキュリティチームのモデル]

#### b) 分散型 CSIRT

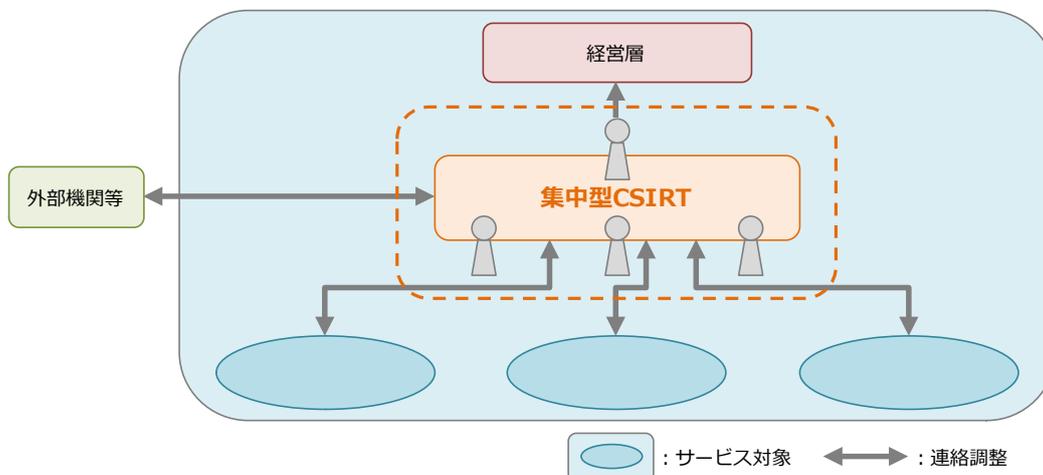
一部またはすべての下位組織の要員を仮想的に CSIRT の要員 (専任/兼任) として指定し、全体の統括・調整を一人の責任者 (マネージャー) が行う。要員は、それぞれの部門・部署をベースに活動し、インシデント発生時には CSIRT の要員として機能する。また、何人かは CSIRT の業務のみを専門とする。また、外部機関等とのやり取りは、全体の統括・調整を行う責任者が行う。



2-8 分散型 CSIRT のモデル]

c) 集中型 CSIRT

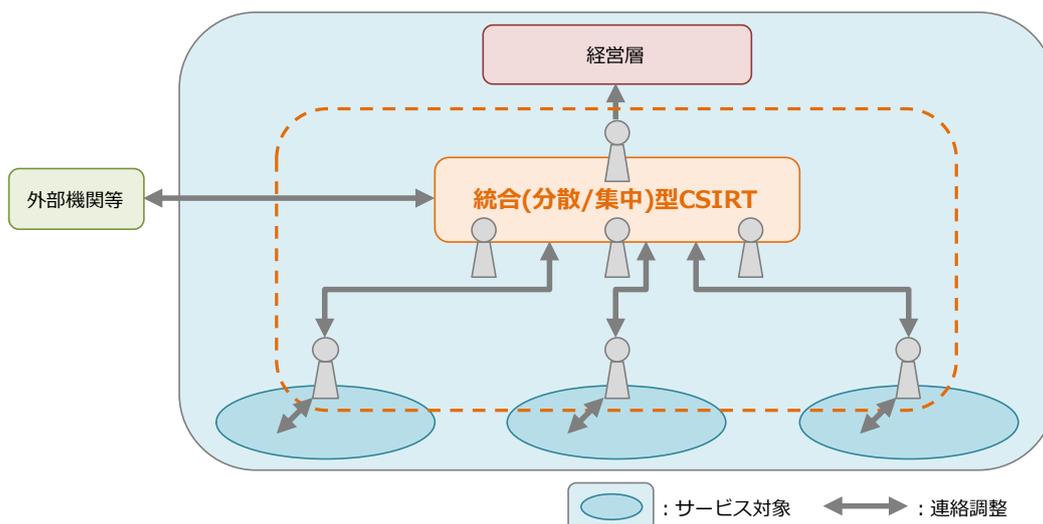
CSIRT が独立の正式な組織として設置され、専属の要員を中心に構成される。組織内で発生するすべてのインシデント対応への責任があり、責任者（マネージャー）や経営層（CIO など）に対する報告義務が伴う。



2-9 集中型 CSIRT のモデル]

d) 統合（分散／集中）型 CSIRT

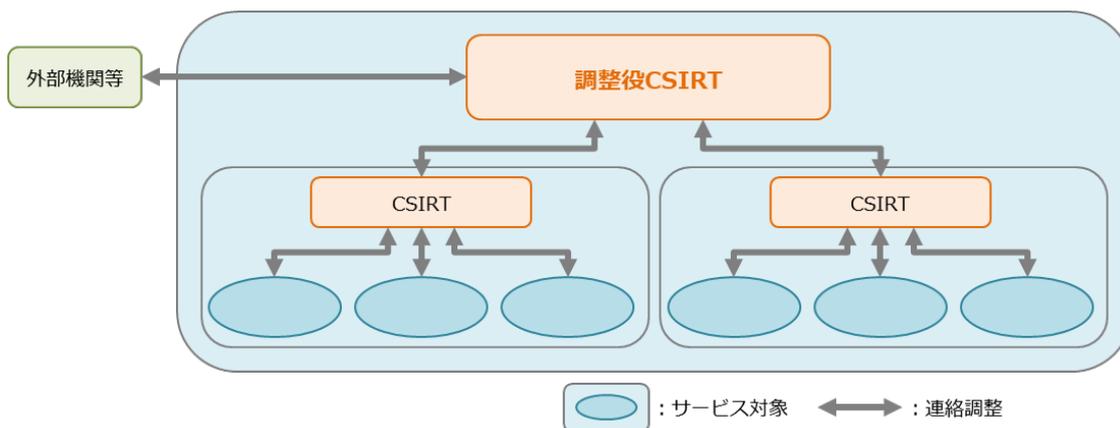
分散型と集中型を合わせたハイブリッド型のしくみで、中央集権型の機能を持ちつつ、下位組織への対応をきめ細かく行うことができる。ただし、情報セキュリティインシデントに対応できる体制を組織全体に整えるため、要員不足に陥る可能性もある。特に、インシデント対応を優先的に行う必要がある組織では妥当なモデルといえる。



2-10 分散/集中型 CSIRT のモデル]

e) 調整役 CSIRT

組織の内外に対するインシデントレスポンスの調整役を担うモデルで、例えば親会社の CSIRT が企業グループ全体を統括する立場から、個々のグループ企業の CSIRT を支援・牽引するような構造に適している。特に、情報の調整・流通を主な業務とし、インシデント対応の実務作業を行うことは少ない。



2-11 調整役 CSIRT のモデル]

これらのモデルはいずれも一長一短の特徴であり、組織の抱えるリスクや組織内 CSIRT の設置目的、組織構造、リソース、サービス対象の範囲等によって、最適なモデルは異なる点に留意する必要がある。

(2) インシデントレスポンス能力

インシデントレスポンスの能力を計測する基準として、CERT/CC から以下のフレームが提唱されている。

**a) 検知・認知 (Detect)**

「検知・認知」の能力については、情報セキュリティインシデントの対応部署だけでなく、実際にシステム・アプリケーションを利用する現場の従業員全員に期待されるものである。なぜなら、問題の兆候が顕在化しても、現場の当事者がそれをインシデントとして認識するのが遅れると、結果的に対応が遅れてしまうからである。

したがって、従業員全員に期待されるのは以下の能力である。

- 兆候や事象に気付く能力
- 適切な対応部署に報告する能力

また、対応部署には、以下の能力が求められる。

- 従業員から受領した報告を認識および把握する能力
- サーバーとネットワークの状態を監視および検知する能力
- 脆弱性情報や脅威（攻撃）などを収集および把握する能力
- 最新の対策（技術）情報を掌握する能力

**b) トリアージ (Triage)**

次に「トリアージ」の能力が挙げられる。具体的には、対応部署にインシデントがもたらす影響の大きさを見極め、作業の優先順位を判断する以下の能力が求められる。

- 事象をカテゴライズする能力
- 事象の対処の優先度を付ける能力
- 事象の対処プロセスを決める能力
- 事象をクローズする能力

**c) 対処 (Respond)**

最後に「対処」の能力が挙げられる。対応部署に求められる実務能力であるが、組織内の関係部署間の連携が必要不可欠という点で、組織全体にも求められる以下の能力である。

- 対処計画を策定する能力
- 技術的対処、危機（リスク）管理的対処、法的対処のいずれか、あるいはすべてを実行する能力
- 幾つかの対処が並行する場合、相互に連絡および調整をする能力
- 外部と連携する能力
- インシデントをクローズする能力(文書化、対処活動レビュー、告知および報告等)

### (3) CSIRT 構築の流れ

組織内 CSIRT を構築する際の手順は次のようになる。

- ① 経営層から理解を得る
- ② 組織内の現状把握
- ③ 組織内 CSIRT 構築活動のためのチーム結成
- ④ 組織内 CSIRT の設計と計画
- ⑤ 必要な予算やリソースの獲得
- ⑥ 組織内 CSIRT 関連規則類の整備
- ⑦ CSIRT 要員（スタッフ）への教育
- ⑧ CSIRT の告知と活動開始

### (4) 組織内 CSIRT 構築に係る課題

実際には、組織内 CSIRT 構築を進める上で、いくつかの問題に直面することが予想される。そこで、CSIRT の構築時に解決すべき典型的な課題を以下に示す。

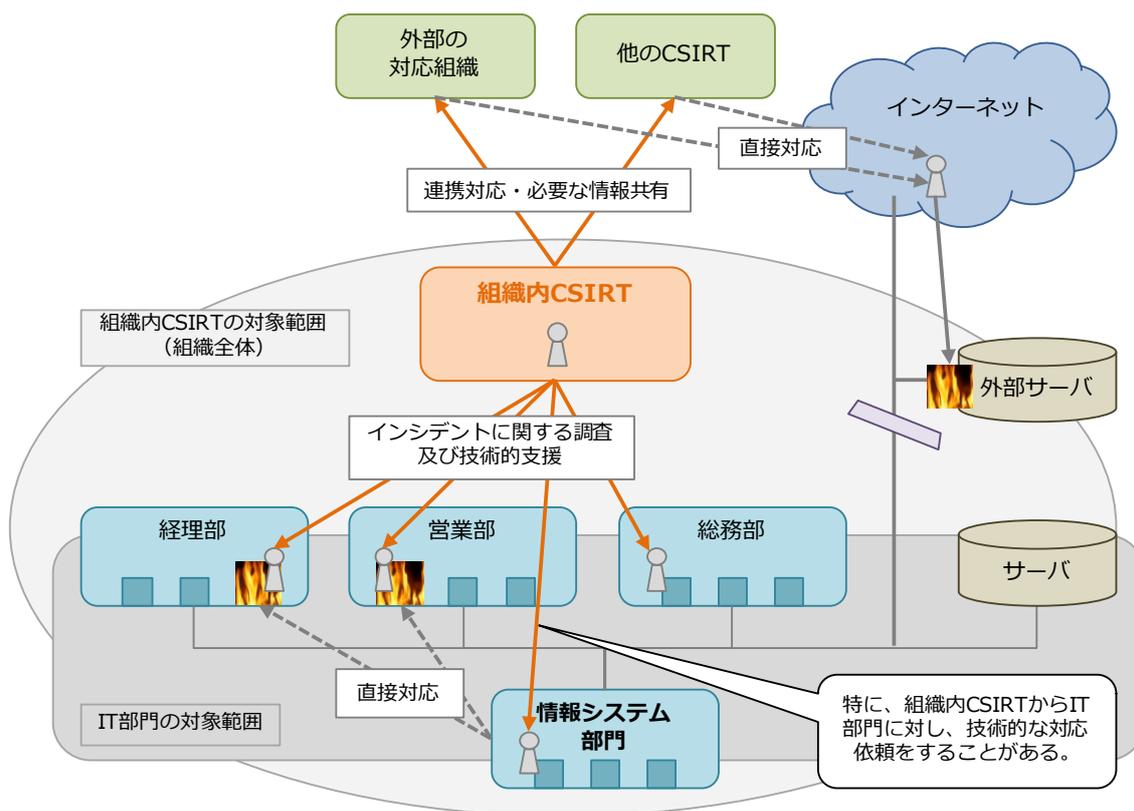
#### a) 経営層の理解

組織内 CSIRT の構築は組織設計・制度設計の問題であり、経営判断が必要となる。しかし、経営層が情報セキュリティインシデントについて知見が乏しい場合、CSIRT の整備を進めるためには、CSIRT の必要性やメリット、CSIRT がないことによる問題点、CSIRT 構築に必要なコストなどを明確にして説得しなければならない。特に CSIRT のコンセプトの理解を得る上で、既存の組織との違い、サービス対象の範囲とコストの関係といった点については、十分な説明が必要となる。

#### b) 情報システム部門との役割・責任の切り分け

複雑化・ブラックボックス化する企業の IT 環境において、情報システム部門のミッションはまず情報インフラの運用や障害対応であり、情報セキュリティインシデントへの対応は技術的・権限的に容易ではない。それにもかかわらず、企業が CSIRT 的な機能を情報システム部門に担当させている場合、深刻な問題が生じうることは、2.2(2)a)で示したとおりである。

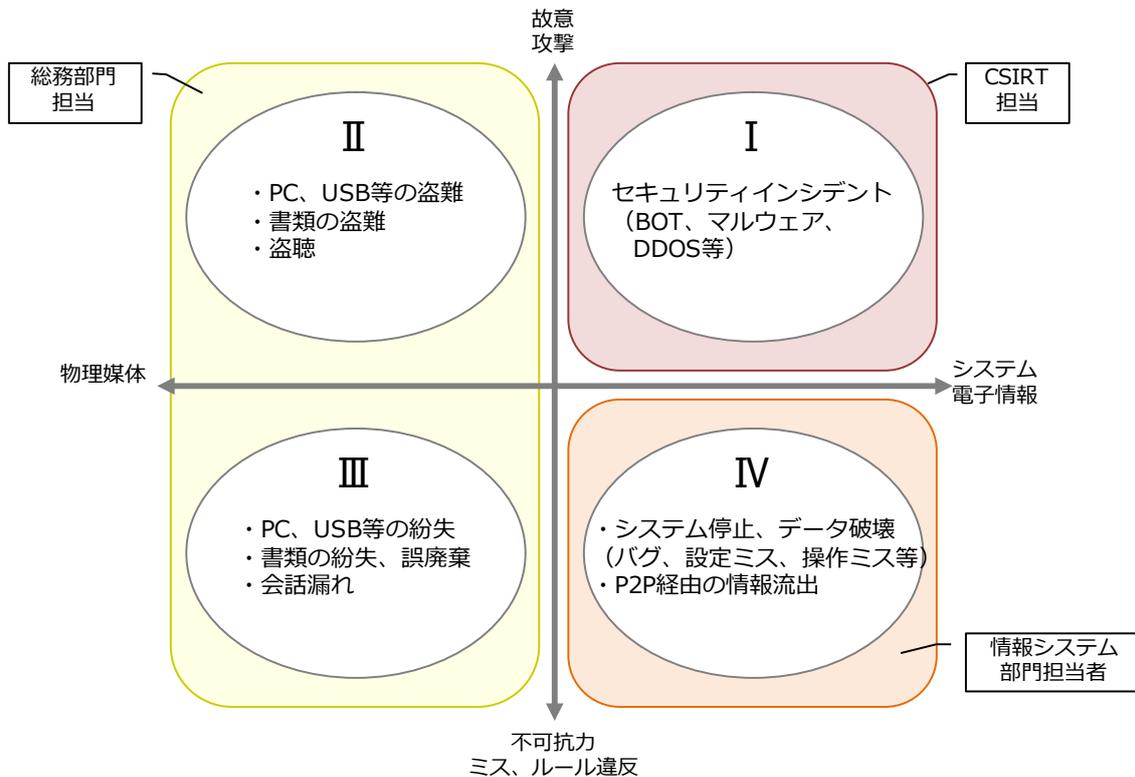
したがって、組織内 CSIRT の機能を確立する際には、既存の情報システム部門の活動範囲や役割、責任、権限等を明確にする必要がある。[図 2-12 に、組織内 CSIRT を情報システム部門とは別に設置した場合の活動範囲の関係の例を示す。



2-12 CSIRT と IT 部門の活動範囲の関係の例]

c) 既存の体制やルールとの整合

組織設計において、既存の体制との実務に係る整合性の確保は極めて重要である。情報資産に係る脅威別に対応を整理すると、[図 2-13 において、従来からⅡ・Ⅲは総務部門が、Ⅳは情報システム部門が担当しているが、Ⅰについては明確な担当部署がなく、その場凌ぎで対応してきた。しかし、昨今のリスクの高まりを踏まえ、事中・事後対策を強化する方策として、Ⅰに対応する CSIRT を設置することが有効と考えられる。さらに、事業継続を重視する場合には CSIRT がⅠとⅣを担当するモデル、情報漏えい防止を重視する場合には総務部門の傘下で CSIRT がⅠ・Ⅱ・Ⅳを担当するモデルもありうる。



2-13 情報資産に係る脅威の分類と対応担当]

また、組織の論理で導出された役割分担が、現場の従業員からどのように見えるかについても配慮が必要である。特に、脅威別に報告先が異なる場合、インシデントを発見した従業員側が混乱して、結果的に対応が遅れる可能性もあることから、報告先の各窓口における適切なルールの導入と組織内への十分な説明が必要である。場合によっては、報告先の窓口を一本化することも検討すべきであろう。

さらに、関係部署間の連携・調整手順についても、既存のルールとの整合に配慮しつつ、より円滑な対応を実現するため、最適化を図ることが望まれる。情報セキュリティインシデントの場合、当事者の部門や情報システム部門に加え、総務部門（内部犯行の際の対応）、法務部門（関係省庁・法執行機関との調整）、営業・渉外・広報部門（顧客・取引先等への説明）等との円滑な連携も必要になる。

このように組織横断的な調整を進める際には、トップダウンの推進が必要となることから、経営層のリーダーシップが期待される。

d) 経営層を交えた迅速な意思決定プロセスの確立

情報セキュリティインシデントに対応する上で、現場レベルでは調整が困難な場合、より上位の階層に報告し、対応する「エスカレーション」が必要となる局面が起こりうる。例えば、情報セキュリティインシデントが複数の部門に及んでいて調整が必要な場合、あるいは管理権限の制約上、意思決定が必要な場合には、エスカレーションを進め、判断が可能なレベ

ルで調整を図る必要がある。また、CSIRT の許容量以上のインシデントを抱えていたり、発表された対応期限内に間に合わせることができない状況においても、エスカレーションを適用することができる。

エスカレーションのしくみを適切に稼働させるためには、エスカレーションの適用を判断するための基準づくりが重要となる。具体的には、エスカレーションを適用する各レベルの設定（部署内→事業所内→部門内→部門間→企業間）、エスカレーションを適用する条件、適用を判断する権限の設定、適用のための手続き等を規定する必要がある。特に、複数の組織間での調整時にインシデント対応が円滑に進められるよう、十分な権限とルールを確立しておくことが望まれる。

#### e) CSIRT 要員の確保

[表 2-3 に、CSIRT の要員に一般的に求められるスキル構成を示す。実際には、このすべてを網羅する人材を必要数確保できるケースは少ないと思われ、何を優先するかを判断する必要がある。その際、最も重要となるスキルは、インシデントレスポンスにおける分析能力ではなく、サービス対象者や他の CSIRT を含む外部組織や機関との積極的な情報交換、すなわちコミュニケーションのスキルである点に留意する必要がある。

[表 2-3 CSIRT 要員に必要なスキル]

| タイプ      | スキルの概要   |
|----------|--|
| ヒューマンスキル | <ul style="list-style-type: none"> <li>・明確な指示や取り決めなどがなく、時間的制約がある状況下でも、必要なことを受け入れ、判断できること</li> <li>・業務内容の異なる部署や、外部組織との対話を円滑にできること</li> <li>・規則や取り決めなどに従うことができること</li> <li>・強いストレスのある状況下で業務を遂行できること</li> <li>・チームの評判を守る大局的な視点と行動ができること</li> <li>・勉強を続ける姿勢があること</li> <li>・問題解決能力</li> <li>・他のメンバとの連携能力</li> <li>・時間管理能力</li> </ul>  |
| テクニカルスキル | <ul style="list-style-type: none"> <li>・セキュリティ原則の理解（CIA、AAA、アクセス制御、プライバシー、その他の基本原則）</li> <li>・脆弱性とそれを悪用する攻撃についての理解（物理セキュリティ、設計・実装・設定上の問題、ユーザーによるエラー、さまざまなマルウェア、等）</li> <li>・インターネットに関する基本的な知識（技術、歴史、構造、インフラの構成など）</li> <li>・リスクに関する理解（インシデントがサービス対象にもたらすリスク）</li> <li>・ネットワークプロトコル（IP、TCP、UDP、ICMP、TFTP、HTTPS、SNMP、SMTP、その他のさまざまなプロトコル）</li> <li>・ネットワークアプリケーションとサービス</li> <li>・ネットワーク機器（アーキテクチャ、ルーター、スイッチ、ファイアウォール、IDS/IPS、等）</li> <li>・ホスト/システムのセキュリティ（システムの運用と管理）</li> <li>・暗号技術に関する知識</li> <li>・プログラミングに関する知識</li> </ul> |

また、CSIRT 要員については、「専任」／「兼任」という点も判断を要する。全体的なバランスを考慮すれば専任者を多数確保するケースは少なく、少数の専任者とその指示に応じる多数の兼任者という構成が主流と考えられる。また、2.3.(1)に示した事例のように、専任者の体制に、インシデントの種類によってアドホックに兼任者が加わる構成も可能である。こうした体制の選択は、要員の構成や能力、組織構造等を考慮して行うことになる。

さらにインシデント発生時の対応においてはさまざまな分野での専門性（技術的な対応だけでなく、情報収集、対外連携、広報対応、法的対応など）が必要になることを考慮すれば、上述のスキルに留まらない専門的知識やスキルを持つ者を CSIRT の機能に組み込む必要がある。日本シーサート協議会では CSIRT に求められるさまざまな専門機能についての説明とそれらを担う要員に必要なスキルについての解説資料を公表している。<sup>36</sup> 自組織内で賄えない専門機能についてはアウトソーシングによって補うことも検討すべきである。

---

<sup>36</sup> 日本シーサート協議会「CSIRT 人材の定義と確保」 <https://www.nca.gr.jp/activity/training-hr.html>

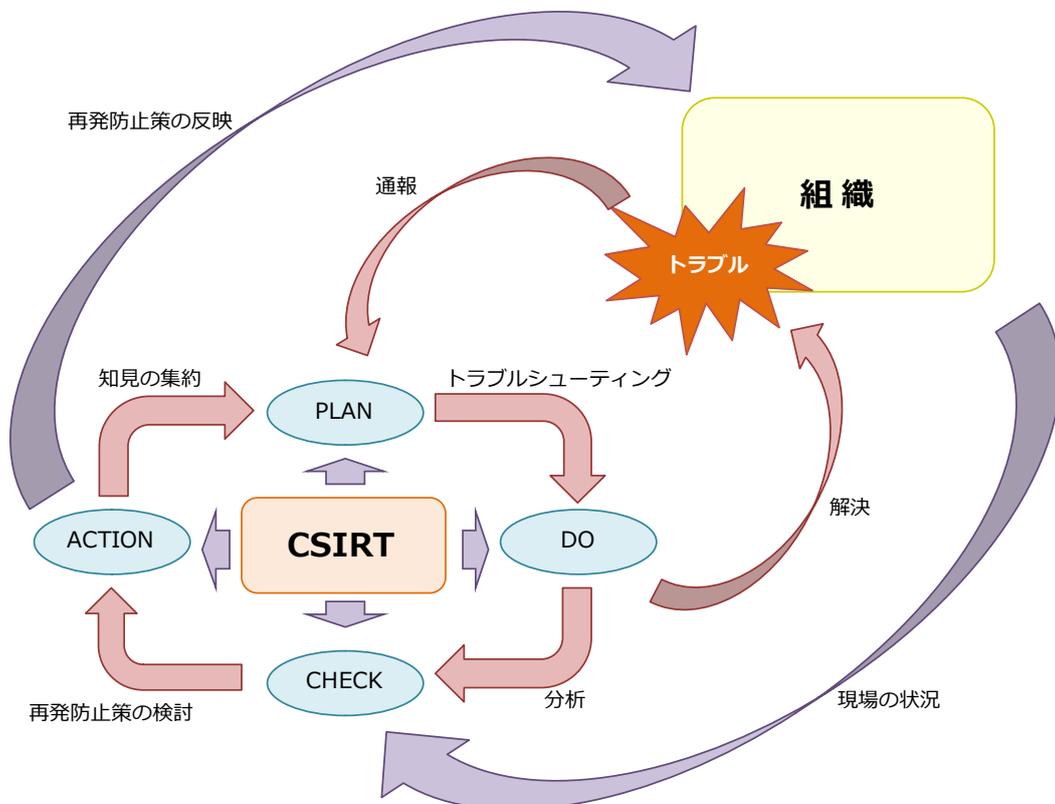
### 3. 危機管理／緊急対応体制の活用に向けて

#### 3.1. フィードバックによる組織強化

昨今、IT 基盤において予想を超えるトラブルが発生し、その被害規模も拡大していること、また、情報資産に対する攻撃が愉快犯から金銭目的の犯罪にシフトし、その手法も高度化・潜在化していることを考慮すれば、危機管理／緊急対応の観点から継続的に改善を進め、トラブルへの耐性を強化することが望まれる。

トラブルの再発防止策の適用は、本来、危機管理体制の役割であるが、危機管理体制の多くが実際には委員会等の会議体であることを考えると、実態的には緊急対応体制、すなわち CSIRT がその推進役を担う形が妥当である。経営層から見ても、CSIRT がトラブル処理だけでなく、組織強化に寄与することで、CSIRT を導入した効果が明確化し、対外的な説明も容易になるため、効果的な形態といえる。

具体的には、CSIRT の活動に PDCA サイクルの概念を導入し、トラブルシューティングの対応から得られた知見を抽出して、再発防止策を組織にフィードバックする構造が有効である。



[図 3-1 PDCA サイクルの適用]

例えば、[図 3-1 のように、CSIRT はトラブルシューティングを行うだけでなく、その内容

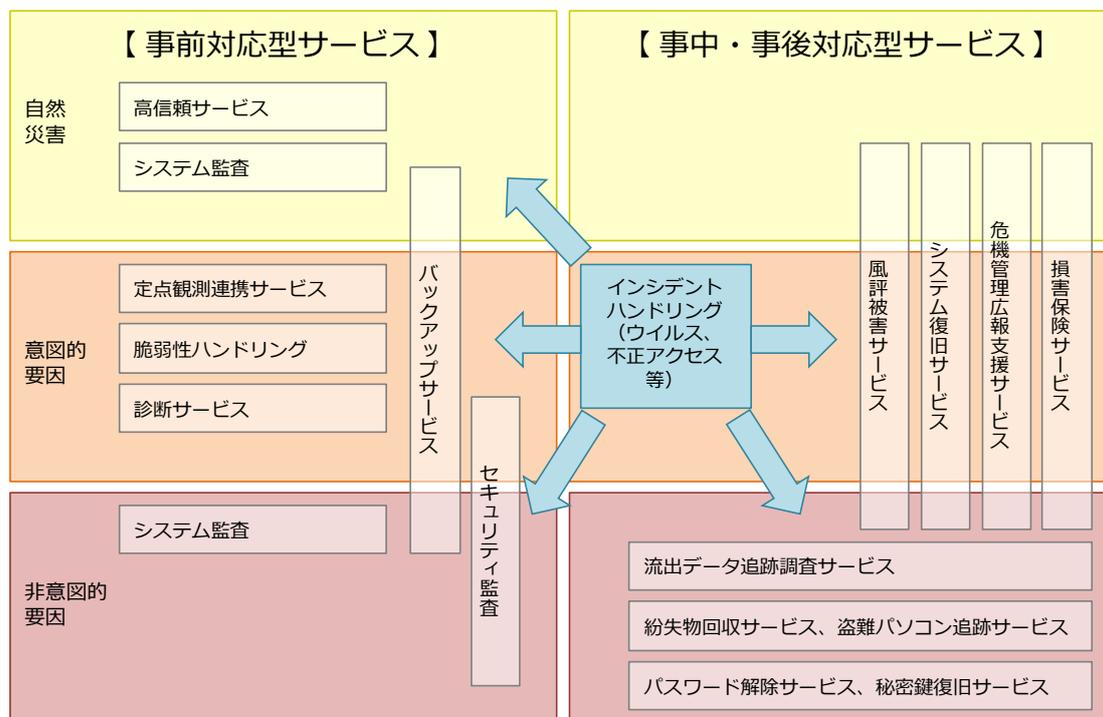
を分析し、再発防止策まで検討して、現場にそれを反映するとともに、得られた知見を集約し、今後の対応に役立てるという展開が考えられる。ここで、再発防止策は、効果という視点だけでなく、業務の継続性という視点を踏まえて導出しなければならない。加えて、CSIRTから提示された再発防止策が現場において着実に適用されるよう、改善の仕組みを組織内に整備することが望まれる。

### 3.2. アウトソーシングの活用とその限界

2.4(4) f)でも示したとおり、組織内 CSIRT の運営において問題となるのは要員の確保である。技術、コミュニケーションの両面で優れた要員を必要数確保することはそれほど容易ではないことから、中長期的には人材育成を進めるとして、短期的には社外の資源を活用する選択も考えられる。

現在、システムインテグレーターやセキュリティベンダー等を中心に、CSIRT 機能の運用をサポートするアウトソーシングサービスが提供されており、自社に必要な機能を組みあわせて選択することも可能である。

ただし、実際には、遠隔監視やインシデント分析・原因追及など、インシデントハンドリングやインシデントレスポンスの部分的な機能支援が中心で、全般的・総合的な CSIRT アウトソーシングモデルは実現していない。これは、トリアージやエスカレーション、組織内連携、リスクコミュニケーションなどの機能が、組織や業務の状況、事業環境等の内部事情を踏まえた上で処理すべきものであり、アウトソーシング化することが難しいためと考えられる。



[図 3-2 CSIRT 関連サービスの構成]

### 3.3. 適切な維持・運営のために

立ち上げた危機管理体制／緊急対応体制を継続的に維持・発展させていくためには、全体的なフレームやルールに加え、適切なメンテナンス策が必要である。例えば、一担当者が牽引する形で危機管理体制／緊急対応体制を立ち上げた場合、それが一種の依存構造になっていると、その担当者が何らかの理由で当該業務と距離を置いた途端に、処理プロセスが滞り、機能不全を起こすことも考えられる。

CERT/CCが発行した文書「Incident Management Capability Metrics Version 0.1」<sup>37</sup>では、重要なデータや資産の「防護 (protect)」、インシデントや脆弱性の「検出 (detect)」、インシデント発生後の「対処 (respond)」、インシデントマネジメントの「維持 (sustain)」の4つの視点から、CSIRTを含むインシデントマネジメント能力に関する評価指標を示している。「維持」においては、組織においてインシデントマネジメントが継続的かつ適切に機能するために確認すべき7つの評価項目と計25の質問事項を示している。これらは、CSIRTを含むインシデントマネジメントの機能を適切に維持・運営するための要点であり、組織に求められている物理面、制度面、組織面の取り組みである。

質問事項には具体的な対策（脆弱性検査、パッチ管理等）の運用レベルの観点も含まれるが、経営的観点から留意すべきなのはCSIRT要員や設備に係る環境整備についての項目である。例えば、CSIRT要員への教育に関する要求事項があることはもちろん、深刻な事案を想定して事業継続だけでなくCSIRT要員の安全確保にも配慮することが要求されている点に注目すべきであろう。また、表中には明確に言及されていないが、異常に気づいた際の対応や、CSIRT要員への協力、再発防止策の受け入れなど、従業員に向けたインシデント対応に関する教育・啓発も非常に重要な継続的課題である。

さらに、組織内CSIRTについて言えば、要求される専門性が高く教育が必要である一方、その単純な強化が事業全体にプラスに働くとは限らないことから、要員やITインフラ等、投入する資源のバランスに十分に留意する必要がある。また、継続的な運用という意味では、人事考課やキャリアパスの観点から、適切な評価制度を整えることが望まれる。特に、兼任担当者の評価方式が適切でなければ、現場業務との競合が発生した場合、十分に機能できなくなる可能性もある点に留意する必要がある。

<sup>37</sup> [https://resources.sei.cmu.edu/asset\\_files/TechnicalReport/2007\\_005\\_001\\_14873.pdf](https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14873.pdf)

[表 3-1 インシデントマネジメント能力の評価：「維持」に関する評価項目と質問]

| 評価項目                             | 質問   |
|----------------------------------|--|
| 覚書、契約類                           | <ul style="list-style-type: none"> <li>・ 公的な手続きを経て組織の長またはCIOが設計したインシデントマネジメント機能またはCSIRTがあるか。</li> <li>・ サービス対象に提供されるインシデントマネジメントサービスを特定する文書化された契約があるか。</li> <li>・ ネットワークに対する変更や計画的な停止を事前にサービス対象側から通知するよう、契約に明記されているか。</li> </ul>   |
| プログラム / プログラム管理                  | <ul style="list-style-type: none"> <li>・ インシデントマネジメント機能のための財務計画があるか。</li> <li>・ 組織の各所で展開される主要なインシデントマネジメント業務に関する明文化された役割や責任があるか。</li> <li>・ インシデントマネジメント要員に関するプログラム管理計画（労働力計画）があるか。</li> <li>・ 労働力の品質や製品・サービスの供給を保障する品質保証プログラムがあるか。</li> <li>・ インシデントマネジメント機能に関する災害復旧、再編、回復力を支援する、確立した事業回復計画があるか。</li> <li>・ インシデントマネジメント要員に関する安全計画があるか。</li> <li>・ インシデントマネジメントのITインフラはインシデントマネジメント能力を支援するのに十分か。</li> </ul>   |
| コンピュータネットワーク防御のための技術開発 / 評価 / 実装 | <ul style="list-style-type: none"> <li>・ インシデントマネジメント環境において利用するツールを安全にテストする能力があるか。</li> <li>・ インシデントマネジメント要員が危機管理技術の水準に達していることを保証するために、様々な媒体を監視しレビューする工程があるか。</li> </ul>   |
| 要員                               | <ul style="list-style-type: none"> <li>・ すべての要員が遂行するインシデントマネジメント業務のためのトレーニングプログラムの中に、確立した教育・訓練・啓発の要求事項や組織における最小限の権限レベルが含まれているか。</li> <li>・ インシデントマネジメント要員のための職能開発プログラムがあるか。</li> </ul>   |
| セキュリティ管理                         | <ul style="list-style-type: none"> <li>・ 適所にインシデントマネジメントのITシステム、設備、要員を守るための物理的な防御策があるか。</li> <li>・ セキュリティの最適化プログラムがあるか。</li> </ul>   |
| コンピュータネットワーク防御のための情報システム         | <ul style="list-style-type: none"> <li>・ インシデントマネジメントのコンピュータネットワークやシステムを強化する徹底した防御の戦略や方法論があるか。</li> <li>・ インシデントマネジメントデータや情報に関する機密性、完全性、可用性を支援するプロセスや技術があるか。</li> <li>・ インシデントマネジメント要員は自らのシステムやネットワークを監視するか。</li> <li>・ インシデントマネジメントのシステムやネットワークについて、リスク評価がなされているか。</li> <li>・ インシデントマネジメントのシステムやネットワークにおいて、脆弱性検査ツールが稼働しているか。</li> <li>・ インシデントマネジメントシステムのためにパッチ管理プログラムが適所に配置されているか。</li> <li>・ インシデントに関する通知や情報、他の警告を受理するための優れた通信システム（メール以外）があるか。</li> </ul> |
| 脅威レベルに応じた対応                      | <ul style="list-style-type: none"> <li>・ 脅威に応じた最新の組織や関連のガイダンス、手続きは、報告のプロセスや様式、直接的行動、セキュリティ対策を、利用しやすく、維持・継続するようになっているか。</li> <li>・ ローカルな脅威レベルに係る変化を踏まえ、意思決定の面でサービス対象が支援されているか。</li> </ul>   |

(出典：CERT/CC「Incident Management Capability Metrics Version 0.1」(2007/06)より作成)