サイバーレジリエンスのための コミュニケーション

～セキュリティ担当者に必要なコミュニケーションスキル集～

2024 年 8 月

独立行政法人情報処理推進機構
産業サイバーセキュリティセンター
中核人材育成プログラム　7 期生
サイバーレジリエンスコミュニケーションプロジェクト

まえがき

サイバーインシデントが発生したという報告を受けた時、セキュリティ担当者として次に何を考えるだろうか。サイバー攻撃に起因するシステムの侵害状況を確認する、使用している機器の脆弱性情報と照らし合わせる、事業に関係する顧客に対してプレスリリースの準備をすることや経営層に報告するなど、多岐にわたる対応が必要になると想像できる。

セキュリティ担当者はサイバーインシデントに関する情報を収集した後、被害拡大防止のための封じ込め対応、被害全貌の把握や復旧対応のために次に取るべき行動を決めていく必要がある。「封じ込めのために最初どのような指示を出すか」「どのような攻撃がされたか調べるためにフォレンジックが必要な端末をどうするか」「システム停止に伴う業務影響について経営層に判断を仰ぐ」などが挙げられるが、これらはセキュリティ担当者だけでは対応が完結しない。セキュリティ担当者としてサイバーインシデントに対応していくにはそのシステム担当部署や経営判断を行う経営層などの他の専門性を持つ部署との連携が必要不可欠である。

このような他部署と連携していく一刻を争うサイバーインシデント対応の際に「他部署の人が思ったように動いてくれない」「必要な情報が手に入らない」と感じたことはないだろうか。

サイバー攻撃の被害者が目の前に出現した未曾有の出来事に困惑し、何もわからず恐怖を感じているという状況の中で、セキュリティ担当者は迅速に復旧するために関係各所とコミュニケーションを取りながら対応を進めなければならない。コミュニケーションをとる相手は、システム担当者、顧客向けサービス担当者、製造現場の担当者、法務担当者、経営層まで幅広い。これらの部署と迅速にスムーズに連携し、サイバーインシデントの対応力や回復力を強化し、組織全体の強靭化を図ることを「サイバーレジリエンス」と呼ぶ。

本書では、組織でサイバーレジリエンスを実施していくために、セキュリティ担当者と他部署のコミュニケーションに着目し、「サイバーレジリエンスのためのコミュニケーション」としてセキュリティ担当者が認識すべきコミュニケーションスキルをまとめている。

この本を通じてセキュリティ担当者のサイバーレジリエンスのためのコミュニケーションを強化し、組織全体でサイバーインシデントに対応していくことを期待している。この本はセキュリティ担当者の視点で書かれているが、サイバーレジリエンスに取り組む組織全体の課題を解決するための参考となれば幸いである。

目次

本書の想定読者

本書ではサイバーインシデント対応の中心を担う人と、セキュリティ以外の部署とのコミュニケーションについて記載している。そのため、サイバーインシデント対応の中心を担う人に加えて、セキュリティ部署以外の方々も、自部署にサイバー攻撃が発生した場合にセキュリティ担当者とどのようなやり取りをすればいいのかを理解するという視点で読んでいただけると幸いである。

本書の構成

第 1 章では、セキュリティにおけるコミュニケーションの特徴とその課題について記載する。セキュリティ担当者と他部署担当者のサイバー攻撃に対する認識の違いや、部署ごとの文化や価値観の違いなどにより発生するコミュニケーション上の課題について本書における見解を述べる。

第 2 章では、サイバーレジリエンスの定義と、本書におけるコミュニケーションの定義について説明する。サイバーセキュリティにおけるレジリエンスの考え方について記載した上で、サイバーレジリエンスのためのコミュニケーションとして本書で述べる内容について記載する。

第 3 章では、第 2 章の考えをベースにして、サイバーインシデント対応のフローから他部署との連携対応の中でも特に重要なものを洗い出している。コミュニケーション上の留意点や平常時からできるコミュニケーションの内容について述べ、サイバーインシデント対応の中心である SIRT とサイバーインシデントの報告者、バックオフィスや経営層などのサイバーインシデント対応における関係者との間で行われるコミュニケーションについて記載している。なお本書では CSIRT、FSIRT、PSIRT を総称して SIRT と記し、IT 環境を担当する SIRT を ITSIRT、OT 環境を担当する SIRT を OTSIRT としている。

第 4 章では、第 1 章から第 3 章まで述べたサイバーレジリエンスのためのコミュニケーションの総論を述べている。

免責事項

- 本書は独立行政法人情報処理推進機構および産業サイバーセキュリティセンターの意見を代表するものではなく、本プロジェクトの見解に基づいて作成されている。
- 本書は単に情報として提供され、内容は予告なしに変更される場合がある。
- 発行元の許可なく、本書の記載内容を複写、転載することを禁止する。
- このドキュメントに誤りがないことの保証や、商品性または特定目的への適合性の黙示的な保証や条件含め明示的または黙示的な保証や条件は一切無いものとする。
- 本書の利用によるトラブルに対し、本書作成者ならびに監修者は一切の責任を負わないものとする。

なお、本書を利用するにあたって、前提知識として「IT パスポート試験合格程度」の知識を有することを推奨する。

第 1 章

サイバーインシデントにおける コミュニケーションの特徴

1.1　サイバーインシデント対応におけるコミュニケーションの重要性

近年、サイバー攻撃は増加の一途をたどっており、攻撃技術も絶えず高度化している。サイバー攻撃の被害は組織内の情報システムだけでなく、工場に設置されている制御機器なども含め、ビジネス全体におよぶ事例も見られるようになった。このように、サイバー攻撃により企業が運営する事業やサービス、あるいは企業が持つ資産に被害が出ることは「サイバーインシデント」と呼ばれる。昨今のサイバーインシデントの状況をみると、企業が「全てのサイバー攻撃を完全に防ぐこと」は困難であるといえる。

そこで、**「サイバー攻撃を受けても事業が止まらないようにする」「被害が出ても速やかに事業を回復する」ことが重要と考えられるようになり、これらの考え方は「サイバーレジリエンス[1]」 と呼ばれている。**サイバーレジリエンスを実現するためには前準備を含め、サイバーインシデントの各段階にて必要な対応を取っていく必要がある。たとえば、NIST SP800[2] コンピュータセキュリティインシデント対応ガイドではサイバーインシデントの対応を以下のように定義している。

- **準備**
  サイバーインシデントに備え、サイバーインシデント発生前から対応計画などの策定を行うこと。
- **検知と分析**
  サイバーインシデントと影響を受けるシステムを特定すること。
- **封じ込め、根絶、復旧**
  さらなる被害を防ぐためにサイバーインシデントを封じ込めること。また、原因となる事象を根絶やし、元の状態に稼働状態に戻すこと。
- **事件後の対応**
  教訓を得て、次の対応へ活かすために実施すべきことの収集。

サイバーインシデントが発生した時、セキュリティ部署だけで上記のプロセス全てを対応することは非常に困難である。サイバーインシデントは企業内のどの部署でも発生する可能性があり、インシデント発生時には当該部署に状況のヒアリングなどを行いながら情報連携をして対応を進めていく必要がある。また、被害拡大を防ぐために封じ込めの対応や、一部のシステムやサービスを停止させるような場合もセキュリティ部署の独断で対処ができるケースは稀である。このため、**サイバーインシデント発生の際には、セキュリティ部署が他部署と連携して対応にあたること、すなわち他部署の担当者と綿密にコミュニケーションを取ることが必要になる。**

---

[1] NIST, SP800-160 Volume2, Revision1, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf

[2] NIST, SP800-61r2 Computer Security Incident Handling Guide, 2012, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

1.2　サイバーインシデントに対する認識の違い

一企業の中であっても、部署ごとにその雰囲気や文化が違うことは想像に難くない。サイバーインシデント時における必要な諸対応においても、部署ごとの文化や価値観の違いなどから、部署間でサイバーインシデントに対して完璧な共通認識を得た上で対応していくことは難しいと考えられる。本書では、サイバー攻撃、およびその被害に対するイメージにおいて、セキュリティ部署とセキュリティ以外の業務に従事する他部署とで乖離があることが原因と考え調査を行った。

企業の営利活動に影響を与える事象とその特徴を整理し、サイバーインシデントでの被害と比較した。ここで、サイバーインシデントの印象と比較対象とする事象には多くの日本人にとって身近である地震や台風等の自然災害を選択した。特徴を調査してまとめたものが表 1.2.1 である。自然災害は日常に流れるニュースでも報道されることが多いため、ほぼ全員が被害のイメージを共有していることが考えられる。自然災害に関しては、事業に被害があった場合に備えて事業継続計画（BCP）を定めている企業も多い。これらの理由から自然災害は誰もが「大変なこと」と認識できているからこそ、BCP に記載されている対応を迅速に行おうという意識がどの部署にも共通認識としてあることが考えられる。一方で、地震や台風のような自然災害と比較すると**サイバーインシデントは「被害が目で見てもわかりにくい」「公開する情報とタイミングの管理が必要」などの特異な特徴がある**ことがわかる。

つまり、サイバー攻撃による被害に関する情報は限定的であり、侵害状況の全容を知ることが難しいという特徴がある。また、侵害状況の全容を知ることができたとしても視覚的なイメージを他人に共有することが難しいという特徴を持っている。以上から、サイバーインシデント時において、セキュリティ部署が他部署と円滑に連携するためには、**「サイバー攻撃が起こるとどれだけの被害が発生するのか」「目に見えない被害にいかに早く気づき共有することが重要か」の認識を部署間で統一化する必要がある**と考えた。

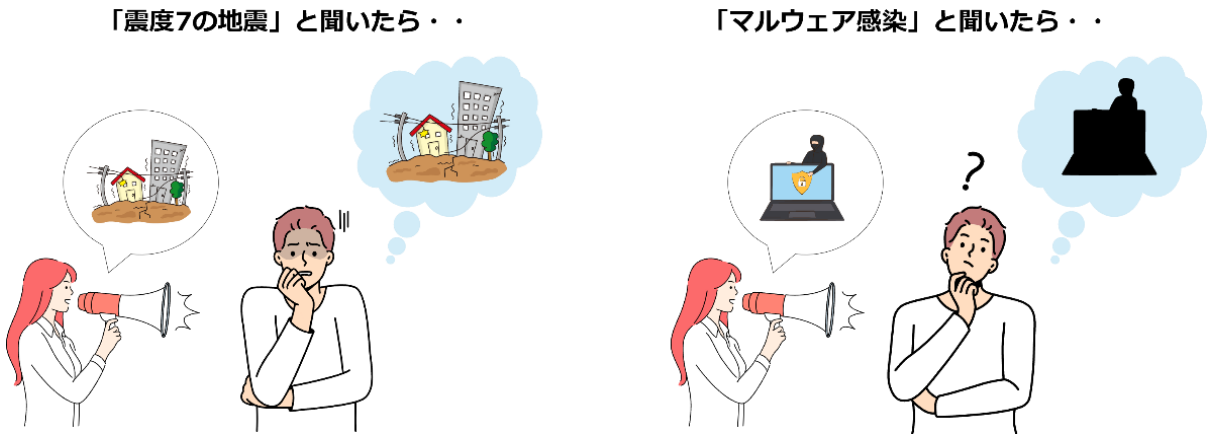

図 1.2.1　自然災害とサイバーインシデントで比較したイメージのしやすさの違い

表 1.2.1 サイバーインシデントと自然災害の特徴の比較

	自然災害	サイバーインシデント
被害範囲	被害が見てわかる	被害が目で見てもわかりにくい
復旧の対応	物理的な復旧	悪性ファイルのアンインストールなど非物理的な復旧
情報の開示	被害の迅速な公開が必要	公開する情報とタイミングの管理が必要
情報源	気象庁や自治体などの 公的機関	脅威インテリジェンスなど特定の企業に向けた 機密性の高い非公開情報

1.3 セキュリティ担当者が感じている課題

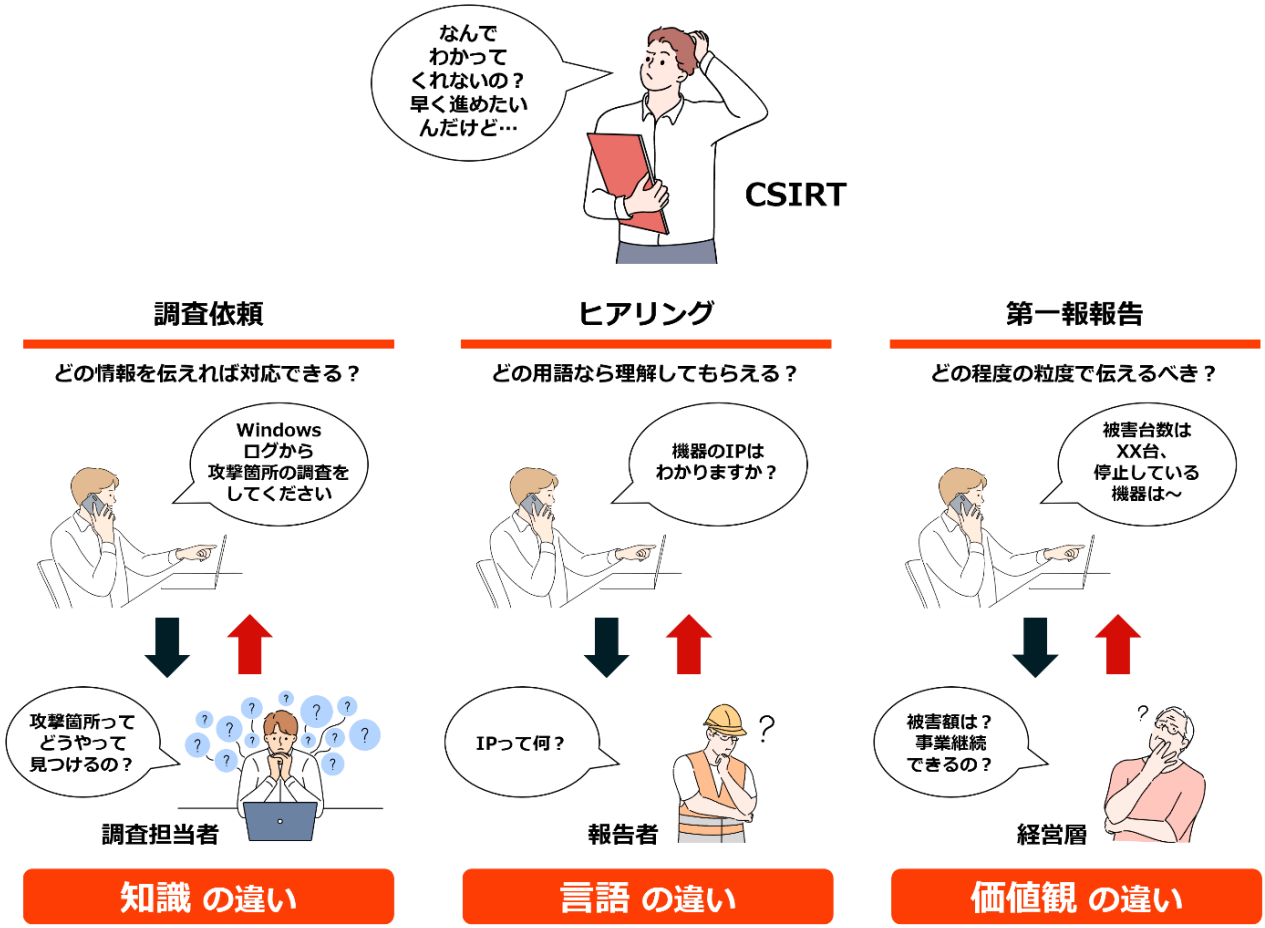

図 1.3.1 セキュリティ担当者と他部署とのジレンマ

「1.1 サイバーインシデント対応におけるコミュニケーションの重要性」にて、本書でコミュニケーションに着目した旨を説明した。本章では、セキュリティ担当者がサイバーインシデント対応を実施するにあたり、他部署とのコミュニケーションにおいてどのような課題を持っているのか調査を行った結果を述べる。中核人材育成プログラム[3] を修了した 1 期生～6 期生を対象にサイバーインシデント対応におけるコミュニケーションに関する 6 つの質問をし、合計 110 名分の回答を収集した。全体の回答例は別途 Appendix に掲載しているが、ここではそのうち 3 つの質問に対する回答とその分析結果を紹介する。

【質問(一部抜粋)】

① サイバーインシデント時に他部署とのコミュニケーションを取るにあたり、文化や価値観のずれによって意図した通りに伝わらないと感じられたことはありますか？
② サイバー攻撃の被害の大きさや重大性の認識が組織間によって違うと感じられたことはありますか？
③ サイバーインシデント発生部署側は、セキュリティ部署の指示を正確に理解し、セキュリティ部署が求めている対応スピードで、必要な対応を行動に移せている/移せると感じられますか？

①の問いには、「そう思う」が 44%、「ややそう思う」が 41%で、回答者の 85%が質問に対して共感の回答をした。②の問いには、「そう思う」が 49%、「ややそう思う」が 37%で、回答者の 86%が共感していた。反対に③の問いに対しては、「そう思う」が 5%、「ややそう思う」が 29%で、全体の 34%のみに共感の回答が留まった。これらの結果より、**セキュリティ担当者がサイバーインシデント対応において、他部署との情報連携やコミュニケーションで課題を感じていることが示された**。

このような課題がある中で、セキュリティ担当者はサイバー攻撃による被害（事業やサービスの停止、情報漏洩、Web サイトの改ざんなど）の範囲や原因を正確に特定し、今起きている異常を速やかに解消して通常の状態に戻すことが求められる。つまり、**セキュリティ担当者は突然発生するサイバーインシデントからの復旧を迅速かつ正確に進めていく中で、普段関わりが少なく、文化や価値観が違う部署とコミュニケーションをとっていく必要がある**。

[3] 情報処理推進機構,中核人材育成プログラム,
https://www.ipa.go.jp/jinzai/ics/core_human_resource/about.html

1.4　本書の狙い

本書では、1.3 節で述べたセキュリティ担当者が持つ課題の解決方法を導き出すアプローチの 1 つとして、セキュリティ担当者としての業務に必要な他部署とのコミュニケーションに着目した。他部署とやり取りをする際にどのような点に留意すべきかを明らかにすることによって、「情報がうまく引き出せない」「対応依頼がうまく伝わらない」といったコミュニケーション上の課題を解決し、結果的に企業のサイバーインシデント対応能力の向上に貢献できると考えのもと、本書にまとめている。

本書は、サイバーインシデント対応時にとるべきコミュニケーションだけでなく、サイバーインシデントが起こっていない時、すなわち平常時にとるコミュニケーションも含めて、**サイバーインシデントを速やかに解決するためにセキュリティ担当者がとるべきコミュニケーションを示し、セキュリティ担当者としての必要なコミュニケーションスキルを実践しやすい形で提案する。**

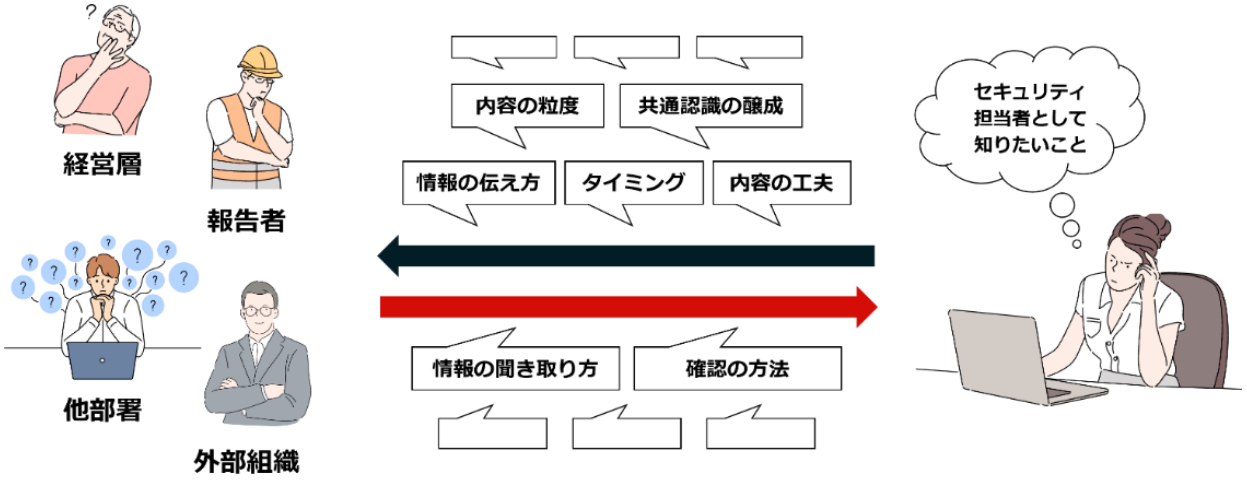

図 1.4.1　本書が対象とするセキュリティ部署と他部署のコミュニケーション

第 2 章

サイバーレジリエンスのための コミュニケーションとは

2.1　サイバーセキュリティとレジリエンス

サイバーインシデントが発生するとシステムが停止する、または意図した設計通りに動かなくなる事象などが発生する。このような場合、セキュリティ担当者として被害を少なくすることや、どのように事業やサービスを復旧するかを検討する必要がある。このように、**これから発生することを予測し、事態を収束させ、いち早く機能を復旧させる能力を「レジリエンス」という**[4]。サイバーセキュリティの観点でも、サイバーインシデント時には、システム稼働をどのように維持していくかを検討するとともに、ビジネス継続のためにどのように暫定復旧対応、恒久対策を進めるかというレジリエンスの観点の対策を検討しなければならない。サイバーセキュリティにおいてレジリエンスの考え方はシステム稼働だけでなくビジネスの観点からも重要な項目である。

2.2　サイバーレジリエンスとは

米国立標準技術研究所　（NIST：National Institute of Standards and Technology）は、サイバーレジリエンスとは「サイバーリソースを含むシステムに対する悪条件・ストレス・攻撃、または侵害を予測し、それに耐え、そこから回復する・適応する能力」と定義している[5] 。独立行政法人情報処理推進機構（以下、IPA） が 2018 年から開催している「責任者向けプログラム業界別サイバーレジリエンス強化演習」においては、サイバーレジリエンスを「部署・部門のサイバーセキュリティに関する対応力・回復力を強化し、企業組織全体の強靭化を図ること」[6] と定めている。

これらを参考にし、本書ではサイバーレジリエンスを「企業において、システム復旧までの時間やサービス低下範囲を組織一体となって改善していくこと」と定義する。サイバーレジリエンスの向上は、セキュリティ部署を中心に、経営層、事業部門やバックオフィスなど社内関係者を巻き込み、その企業全体でサイバー攻撃に対する耐性が強まることを意味する。

---

[4] 芳賀茂, レジリエンスエンジニアリングの安全マネジメントへの応用のための課題と実践セーフティⅡを目標とする安全マネジメントの実践, 日本原子力学会誌, Vol.63 , No.10, 2021 https://www.jstage.jst.go.jp/article/jaesjb/63/10/63_708/_pdf

[5] NIST, SP800-172, 2024, https://csrc.nist.gov/glossary/term/cyber_resiliency

[6] 情報処理推進機構, 責任者向けプログラム業界別サイバーレジリエンス強化演習（CyberREX） 事業内容, https://www.ipa.go.jp/jinzai/ics/short-pgm/cyberrex/index.html

2.3　本書におけるコミュニケーションの定義

本書では「コミュニケーション」という言葉を、業務に関する情報を伝えること、およびその伝える内容を意味するものとして使用している。

業務の中で行われるコミュニケーションについては、そのコミュニケーションをとるタイミングや交わす内容についてさまざまな分野で研究がされている。これらの研究では、意図した通りに内容が伝わらなかったことや、何らかの理由から伝えることができなかったというコミュニケーションエラーにより、重大な事故につながる側面もあることが明らかになっている[7]。

このような背景から、本書ではセキュリティ業務においてもコミュニケーションに関する認識の齟齬が発生し、業務に影響を与えているのではないかという考えのもと、調査内容をまとめている。

2.4　サイバーレジリエンスのためのコミュニケーションとは

本書では、**「発生したサイバーインシデントに迅速かつ柔軟に対処するために、セキュリティ担当者が中心となって取るべき他部署との情報連携」のことをサイバーレジリエンスのためのコミュニケーションとして定めた。**セキュリティ部署を中心として、異なる部署間で交わされるセキュリティに関するコミュニケーションの頻度や内容を改善し、部署間のつながりを強化していくことによって結果的に企業としてのサイバーレジリエンスが向上すると考えている。

3 章からはサイバーレジリエンスのためのコミュニケーションを阻害する要因を攻略し、セキュリティ担当者がサイバーインシデント対応に不可欠な部署間を横断したコミュニケーションの改善を目指すための内容を記載している。

---

[7] 厚生労働省　重要事例情報―分析集(指示時のコミュニケーションエラー)
https://www.mhlw.go.jp/topics/bukyoku/isei/i-anzen/1/syukei6/9b.html

第３章

サイバーインシデントにおける部署間のコミュニケーション

3.1 インシデント対応におけるコミュニケーションの「つまずきやすさ」

第 1 章で述べたように、サイバーインシデント対応をセキュリティ部署だけで完結させることは難しい。サービスや事業を回復させるには、情報システム部や工場など他部署との連携は必須である。加えて顧客にまで影響がおよぶ場合には、社外への対応のために広報部・法務部などのバックオフィスや経営層とのやりとりも必要になる。

セキュリティ部署と他部署とのやり取りの際には、「1.3 セキュリティ担当者が感じている課題」で紹介したアンケート調査の結果が示した通り、セキュリティ担当者はサイバーインシデント対応において他部署との情報連携やコミュニケーションで課題を感じている。とくに、企業の事業規模が大きければ構成する部署の数も多くなるため、部署間の価値観のずれや専門性の違いが一層浮き彫りになり、「意図が伝わらない」「情報が正確に得られない」といった事態が頻繁に発生すると考えられる。そのような事態の頻発は、**サイバーインシデントの発生現場の状況把握を遅らせ、結果的に封じ込め対応の遅れや大幅な事態の悪化につながってしまう可能性がある**。

このように、サイバーインシデント対応におけるセキュリティ部署は、緊迫した状況下であるにもかかわらず、価値観や使う専門性が違う部署を相手にコミュニケーションをとる必要がある。また、このことに加えてサイバーインシデントではその対応の迅速さと正確さが求められる。本章では、セキュリティ部署が他部署とコミュニケーションをとる上で「つまずきやすい」ポイントをサイバーインシデント対応時のフロー図から洗い出し、分析を行った結果を紹介する。

この**「つまずきやすさ」とは「速く正確にコミュニケーションをしなければならないが、セキュリティ部署との間に大きな業務ギャップがあるためにコミュニケーションエラーが発生する可能性が高い」**ことと本書では定義している。「業務ギャップ」という言葉は、部署ごとの業務内容の違いのみを指すのではなく、その業務におけるビジネス目標や起こってほしくないビジネスリスクへの理解に乖離があることを表すものとして定めたもので、本書で独自に定義しているものである。

「3.2　IT 環境と OT 環境におけるサイバーインシデント対応フロー」では、IT 環境と OT 環境それぞれのサイバーインシデント対応時のフローを示し、実施されるサイバーインシデント対応について説明する。「3.3　留意すべき情報連携とその関係者」では、サイバーインシデント対応フローの中で「つまずきやすい」ポイントについて、登場する関係者を整理した上で、その関係者との間に生じる 「つまずきやすさ」を解消するためにできるコミュニケーションを紹介する。

3.2 サイバーインシデント対応フローとコミュニケーション

本節では、IT 環境と OT 環境それぞれのサイバーインシデント対応フロー図を明示し、その中でつまずきやすいコミュニケーションについて取り上げていく。ここで紹介するサイバーインシデント対応フローは、JPCERT/CC が公開する一般的な企業を想定したサイバーインシデント対応フロー[8] を参考に、本書で独自に検討し作成したものである。

IT と OT のそれぞれの対応フローとそこで「つまずきやすい」コミュニケーションを説明するにあたり、共通して登場する部署の役割と機能について以下に詳述する。なお、本書で紹介するフローの中における役割名を記載しているが、企業によって名称は異なるため、一読されたのち、自身の企業の部署に当てはめていただきたい。また、本書で提示するサイバーインシデント対応フローは、1 つの例として示していることをご留意いただきたい。加えて、本フローでは他部署とのコミュニケーションにおいて「つまずきやすい」ポイントを明らかにして分析することを目的としたため、判断によって後続の行動が変わるフローの分岐点は概ね省いている。たとえば、IT 環境のフロー図では、被害確認の段階でサイバー攻撃の封じ込めに成功した場合や、システムを停止しなかった場合は記載していない。サイバーインシデント対応において、攻撃の検知、調査、封じ込め（システム停止）、経営層・バックオフィスへの報告、暫定復旧という一連のプロセスを経ているという点をご留意いただきたい。

【各組織役割】

- **インシデント発見当事者**
  自社の従業員で、サイバーインシデントと疑われる事象を発見した人物。
  またはサイバーインシデント発生の報告をうけた上司などを指す場合もある。

- **経営層**
  セキュリティにかかわる人的、システム的なリソースの手配、サイバーインシデント対応も含めたセキュリティ施策の最終判断と責任を持つ。

- **バックオフィス**
  サイバー攻撃の被害が社外におよんだ場合、法対応やプレスリリース等の準備を行う。

[8] JPCERT/CC インシデント対応マニュアル
https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20211130.pdf

3.2.1　IT 環境のサイバーインシデント対応フロー

IT 環境にて想定されるサイバーインシデントのリスクには、マルウェア感染、内部不正や操作ミスによる情報漏洩などが考えられ、これらは法令違反や訴訟の原因となることがある。また、ランサムウェアの感染による業務の停止、業務継続ができないことによるビジネスチャンスの損失、顧客対応の質の低下、さらには攻撃者による他社（顧客）や個人への間接的攻撃も懸念される。これらのリスクに対処するために保護すべき主要なこととして、社内外の個人情報、重要なビジネス情報（営業秘密や知的財産など）、そして事業の継続性が挙げられる。

これらを踏まえると、IT 環境におけるサイバーインシデント対応においては、**事業の停止や情報漏洩など社外への影響を防ぐことを最優先とし、事業活動への影響を考慮しつつ、システムの一時停止といったような判断を行っていくことが必要**と考えられる。この考え方に基づき作成した IT 環境におけるインシデント対応フローを図 3.2.1 で示す。また、フロー内の「つまずきやすい」ポイントを★にて表している。このフローは、事業継続とセキュリティインシデント対応のバランスを保ちながら、サイバー脅威から組織を守るための戦術的アプローチを体系的に示している。

【各組織役割】

- **SIRT/SOC**

  SIRT はサイバーインシデントが発生した際に、対応の中心となりうるチームおよび部署。社内調整や対応方針の検討、広報業務を行う場合もある。

  SOC は 24/365 体制でネットワークやデバイスの監視を行い、サイバー攻撃の検出や分析を行うチーム、組織、部署。内部に設置する「内部 SOC」、外部の専門企業に依頼する「外部 SOC」がある。本書ではセキュリティに関する事象を専門的に扱う役割として「SIRT/SOC」として記載する。

- **IT システム担当者**

  各種システムの運用・構築・開発業務を担う部署。

  また、システムへの各種対応依頼の宛先となる部署。

- **外部専門組織**

  JPCERT/CC や IPA など、サイバーインシデントに関する相談窓口となる公的機関。

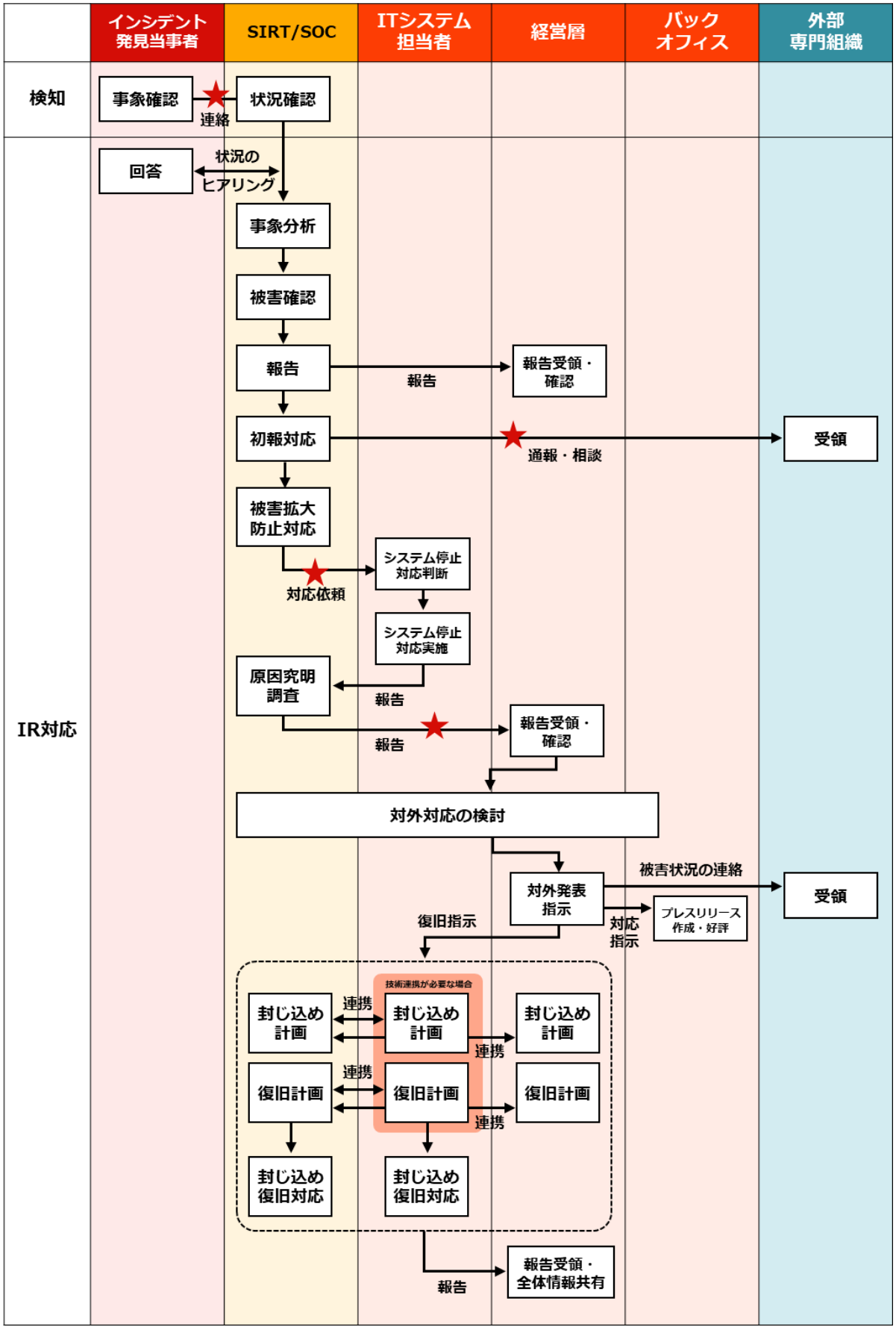

図 3.2.1　IT 環境のサイバーインシデント対応フロー図

3.2.2　OT 環境のサイバーインシデント対応フロー

OT 環境においてもっとも重視されるリスクは人命への影響である。次に生産活動の継続や可用性の維持が重要な要素として挙げられる。とくに重要インフラを運営する企業においては、その事業が数時間停止することが社会への影響は甚大であるため、可能な限りシステムを稼働させ続けることが求められる。このため、システムの変更や更新には極めて慎重な判断が必要である。

想定されるサイバー攻撃に関するリスクには、マルウェア感染などに起因する事故、工場の停止、ビジネス機会の損失、顧客への納品遅れなどが含まれる。さらに、マルウェア感染が製品品質に悪影響をおよぼす可能性や攻撃者が制御システムを利用して他社や個人への間接的な攻撃を行う可能性に加えて、生産データの漏洩により競争力の低下を引き起こすこともリスクとして挙げられる。

これらを踏まえると、OT 環境におけるサイバーインシデント対応では、**「システムを本当に停止させる必要があるか」を、セキュリティ部署と事業部門側の部署、あるいは経営層と十分に議論を重ねなければならない**と考えられる。もし停止が避けられないほど重大な問題である場合は、生産品質と安全が確実に確保されるまで慎重に復旧を進める必要がある。このような OT 環境におけるサイバーインシデント対応フローを図 3.2.2 に示し、「つまずきやすい」ポイントを★にて表している。

【各組織役割】

- **工場長**
  サイバーインシデントの情報を工場担当者から収集し、OTSIRT へ情報共有する。
  また、工場担当者に指示を行い、状況を管理する。

- **OTSIRT**
  平常時、サイバーインシデント対応時に制御システム側で発生したサイバーインシデントを統括する。工場からの連絡の受付、工場への報告・指示、トリアージ、サイバー攻撃の調査や解析を行う。必要であれば、経営者への説明や ITSIRT との情報共有を行う。

- **ITSIRT**
  平常時、サイバーインシデント対応時に情報システム側で発生したインシデントを統括する。必要であれば、経営者への説明や OT-SIRT との情報共有を行う。

- **警察/監督官庁**
  国交省、総務省など自社事業の所管となる官庁

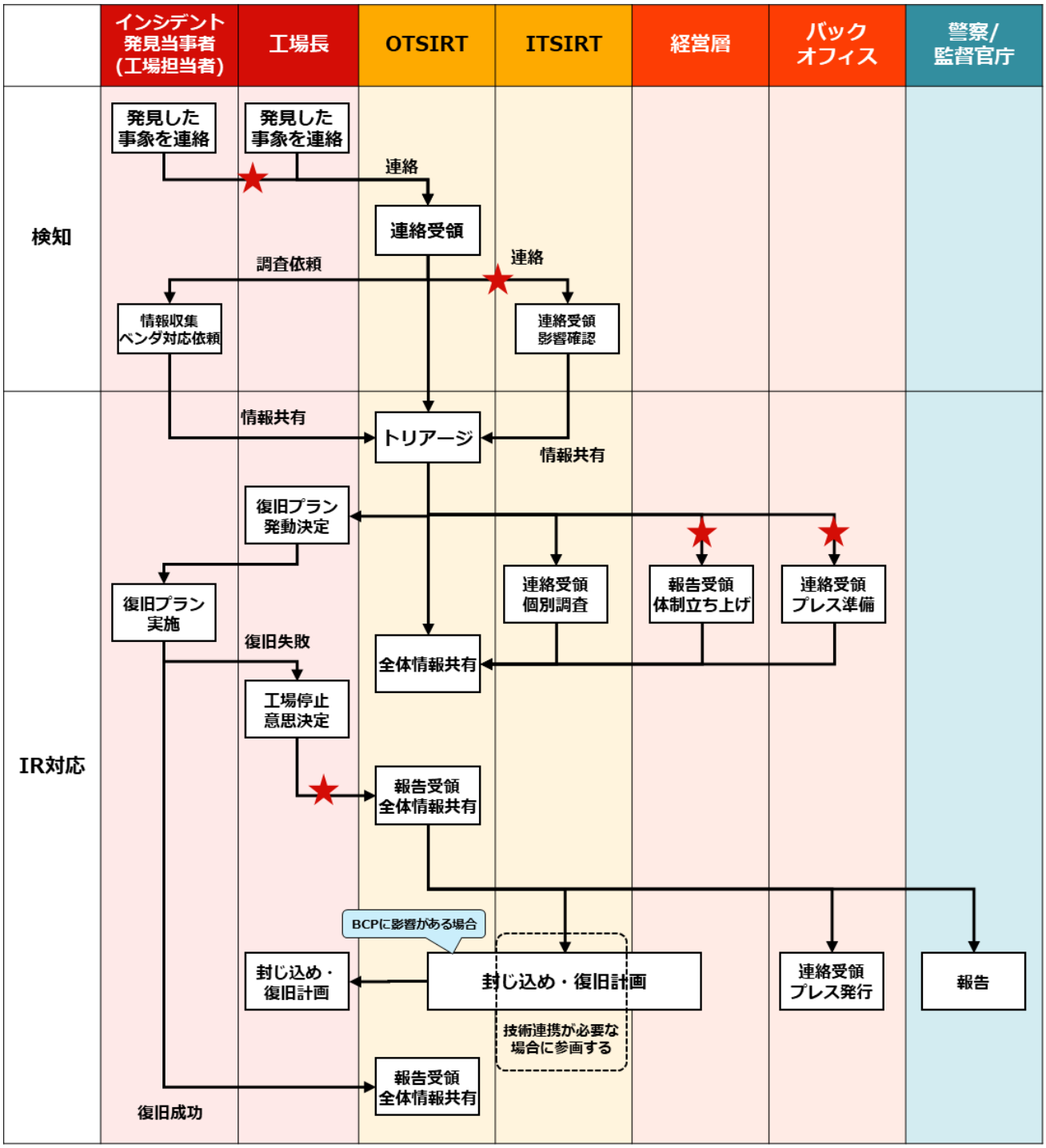

図 3.2.2　OT 環境のサイバーインシデント対応フロー図

3.3　留意すべき情報連携とその関係者

3.2 節で示されたフローを基に、セキュリティ担当者にとって「つまずきやすい」ポイントについてさらに詳細を分析する。「つまずきやすい」ポイントとは、3.1 節で定義した「速く正確にコミュニケーションをしなければならないが、セキュリティ部署との間に大きな業務ギャップがあるためにコミュニケーションエラーが発生する可能性が高い」箇所であり、3.2 節で示したフロー図にて、★マークを付けた連絡経路である。本節では検討結果を踏まえて、**コミュニケーションを円滑に行う上で留意すべき点と、「つまずきやすさ」を解消するために平常時からできるコミュニケーションの取り方について、関係者ごとに記載する**。

➢　**サイバーインシデント対応における主要部署間の関係性**

「つまずきやすさ」の掘り下げのために、IT 環境と OT 環境のサイバーインシデント対応フローにおける関係者について整理した。★マークを付けた連絡経路に該当する関係者に絞り、図 3.3.1 にまとめている。関係者を整理する中で、ITSIRT と OTSIRT はどちらも経営層、バックオフィス（広報・法務）、そしてサイバーインシデント発見当事者とやり取りするため、IT および OT の区別なく連携する部署を「共通」というカテゴリに分類している。

IT 環境では、セキュリティ業務を担当する SIRT と、自社のインフラシステムやアプリケーションの運用を担当するシステム担当者間のコミュニケーションが中心となる。OT 環境では、製造現場のセキュリティを担当する OTSIRT と、工場での生産責任を持つ工場長間のコミュニケーションが重要である。なお、OTSIRT がない企業の場合には、本社セキュリティ部門や工場内 IT 部署が担当するケースもある。

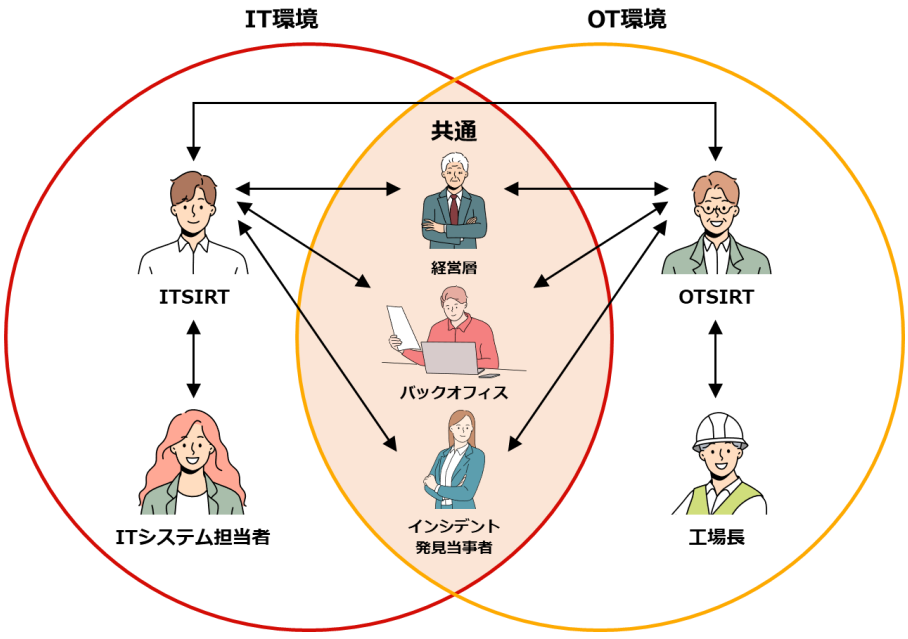

図 3.3.1　サイバーインシデント対応においてコミュニケーションが発生する関係者

- **サイバーインシデント対応における主要部署間のコミュニケーションにおける留意点、および平常時から行うべきコミュニケーション**

次節からは、サイバーインシデント対応フローの中で★マークをつけた、セキュリティ担当者が「つまずきやすい」コミュニケーションについてまとめている。**他部署とのコミュニケーションにおいて「つまずきやすさ」を解消するために、①両者間の考えの違い、②(両者間で)交わされるやり取り、③コミュニケーションの留意点、④平常時のコミュニケーション、⑤セキュリティ担当者の声の 5 つの観点からのコミュニケーションの工夫を記載する。**取り上げた主要部署としては SIRTー報告者、SIRT―経営層、SIRT―バックオフィス、SIRT―システム担当、SIRT―工場長、ITSIRT―OTSIRT である。主要部署間の平常時のコミュニケーションにも言及する理由としては、中核人材育成プログラム修了生へのアンケート調査や各企業のセキュリティ担当者へのヒアリングの結果から「共通認識の熟成」「連絡事項の取り決め」「互いの業務への理解」等の取り組みを「平常時」から実施することが重要であるとの回答を多く得たためである。サイバーインシデント対応時のコミュニケーションの課題を解決するためには、サイバーインシデント時のその場の取り組みだけでは十分でなく、サイバーインシデントが発生していない平常時からの取り組みが必要であることが調査より示されたため、本書では留意点として取り上げ、以降の説で取り組みの詳細について解説している。

【本書の見方 1】

① 両者間の考えの違い

サイバーインシデント対応における SIRT と、コミュニケーションをとる相手の間で発生するやり取りを対比表で表している。対比表には、同じ項目に対する両者の間の考えの違いを示している。

② 交わされるやり取り

SIRT がインシデント対応の中で、コミュニケーションをとる相手との間で交わすやり取りの内容を記載する。イラストと対比表で表していた、SIRT と相手の認識の違いについて文章で記載している。

③ コミュニケーションの留意点

サイバーインシデント下において、SIRT が相手と取るコミュニケーションで留意するポイントを記載する。ここで挙げる留意点に注意しなければ、相手とのコミュニケーションに支障が生じる可能性がある。

④ 平常時のコミュニケーション

サイバーインシデント対応時の留意点を解消するために、日常的に行うことが推奨されるコミュニケーションについて記載する。

⑤ セキュリティ担当者の声

本書作成にあたって訪問した企業のセキュリティ担当者のヒアリングから抜粋したものを記載する。実際のセキュリティ担当者が行なっている取り組みの工夫として参考にされたい。

【本書の見方 2】

3.3.1 SIRT – インシデント発見当事者のコミュニケーション

サイバーインシデント対応は、SIRT または報告者が発見した通常とは異なるシステムの異常検知から始まる。いずれの場合でも SIRT はサイバー攻撃の実態を把握するため、発見者/報告者と連絡を取り合い、現状把握や作業指示を行う。以下に報告者とのコミュニケーションのポイントについてまとめる。

SIRT		インシデント発見当事者
まずは早めに連絡がほしい	被害の連絡	何を話せばいいのかわからない
指示した通りに対応してほしい	応急対応の指示	現場側の都合も考えてほしい 指示された内容がわからない
正確な情報がほしい 被害に遭ったとは思えない	詳細なヒアリング	目の前で起きていることしかわからない 正直に話すと評価が下がるかもしれない

① ② ③ ④ ⑤

交わされるやり取り -インシデント発生時の必須コミュニケーション

✓ **被害の連絡**

サイバーインシデントが発覚すると、SIRT は報告者から連絡を受ける場合もあれば、SIRT から報告者に連絡を入れる場合もある。報告者側は**ある日突然業務を止めざるを得ない事態が発生した状態となり、報告を躊躇してしまう恐れがある。**

✓ **応急対応措置の伝達**

被害を最小限に封じ込めるため、SIRT から報告者に応急措置を指示する。SIRT としては指示内容の通りに報告者に動いて欲しいが、報告者としては突然他部署から指示がなされ、困惑しながらの対応となる。

✓ **被害詳細のヒアリング**

SIRT は正確な情報の収集を望んでおり、仮に報告者のミスが原因であろうと責める意思はない。一方で、報告者は目の前で起きていることの説明で手一杯となっており、**ヒアリングの回答によっては自分の人事評価にマイナスに影響することを危惧する恐れがあると考えられる。**

27

コミュニケーションの留意点 -コミュニケーションでのつまずきやすいポイント

✓ **専門用語を使わない**

報告者はセキュリティの専門用語を知っているとは限らないため言い換えなどをして、**理解しやすい表現を使うことが望ましい。**「ランサムウェア」ではなく「データファイルを見ることができない形にして、金銭を要求するサイバー攻撃」と説明するなどの工夫が必要である。

✓ **攻撃の情報は文字だけでなく画像でも集める**

セキュリティの専門家である SIRT に対して、報告者が自発的に適切な形でサイバーインシデント情報を連携することは基本的に困難である。SIRT は、文字だけでなく、被害に遭った機器の写真やスクリーンショットの提供を求めたり、OT 側の制御機器などでは現地に赴いての直接の目視確認やリモート通話ツールを使ったりするなど、**情報の取り方を工夫することによって事態の正確な把握につなげることが必要となる。**

✓ **SIRT の都合を押し付けない**

SIRT は、報告者に SIRT 側が求めるスピードで正確に対応してほしいと考えている。しかし、業務が停止している可能性もあり、そのような場合、**報告者にとって優先するべきは自分の業務を早く再開することである。**報告者側の都合により迅速に指示を実行に移せない可能性があることを SIRT 側は把握しておき、急な対応を求めるのであれば報告者側の業務の都合を正確にヒアリングして優先度の判断を下すことが推奨される。

平常時のコミュニケーション -つまずかないための普段からの工夫

✓ **連絡事項の事前準備と周知**

SIRT への連絡時に連携すべき項目を事前に取り決め、社内に周知しておくことによって、報告者の負担を軽減し、また対応フローを円滑に進めることが期待できる。誰が・いつ・何を・どこで、発見したかの 4 点を意識して情報を回収すると、基本的な状況の把握がしやすくなると考えられる。可能であれば、**業務影響や事業継続の有無、現状がどうなっているか、報告するまでに何を実施したかの情報までを報告事項に含めておくとより詳細な情報が集まる。**

✓ **些細なことも連絡しやすい環境づくり**

サイバー攻撃は一見すると機器やシステムの異常/故障と見分けがつかない場合も多い。とくに OT 環境の場合、たとえば制御装置が攻撃されて製造設備が停止すると最初は設備異常を疑うことが考えられる。**実際はサイバー攻撃ではなかったとしても「何かおかしい」と感じたら SIRT に相談してもらうような組織風土作りが必要**である。

セキュリティ担当者の声

- セキュリティ部署が出す通達などは、他部署にとっては面倒事であるかもしれないことを念頭に置く。両者の関係性が成熟していないと、依頼したチェックシートの提出が遅れることや、できていないことを隠すことを行い、積み重なると大規模インシデントにつながる恐れがある。**被害の少ない段階で問題を解消するには、他部署との良好な関係が欠かせない。**
- グループ会社を含めたリスク管理規定がある。誰が決断したか明確になり、アナウンスも総務や広報が最終決定をすると決めている。
- セキュリティ部署が全てのシステムを監視することはできず、現場側で異変を見つけることも多いので、**日頃から会話をしてお互いに相談しやすい関係を構築している。**たとえば、不審な通信をしている端末の IP がわかれば、それしかわかっている情報がなくても、相手の顔がわかっていると細かい情報を聞きやすい。今は関係性ができて、ボヤケースでも情報共有してもらえるようになった。**現場側から「サイバー攻撃ではないかもしれないけど情報共有しました！」という報告が挙がってくる。**

3.3.1　SIRT – インシデント発見当事者のコミュニケーション

サイバーインシデント対応は、SIRT または報告者が発見した通常とは異なるシステムの挙動を知得することから始まる。SIRT はサイバー攻撃の実態を把握するため、発見者/報告者と連絡を取り合い、現状把握や作業指示を行う。以下に報告者とのコミュニケーションのポイントについてまとめる。

SIRT		インシデント発見当事者
まずは早めに連絡がほしい	**被害の連絡**	何を話せばいいのかわからない
指示した通りに対応してほしい	**応急対応の指示**	現場側の都合も考えてほしい 指示された内容がわからない
正確な情報がほしい 被害に遭った人は悪くない	**詳細なヒアリング**	目の前で起きていることしかわからない 正直に話すと評価が下がるかもしれない

交わされるやり取り　**-インシデント発生時の必須コミュニケーション**

✓　**被害の連絡**

サイバーインシデントが発覚すると、SIRT は報告者から連絡を受ける場合もあれば、SIRT から報告者に連絡を入れることもある。報告者側は**ある日突然業務を止めざるを得ない事態が発生し、必要な情報連携や報告を躊躇してしまう恐れがある**。

✓　**応急対応措置の伝達**

被害を最小限に封じ込めるため、SIRT から報告者に応急措置を指示する。SIRT としては指示内容の通りに報告者に動いて欲しいが、報告者としては突然業務であまり関わってこなかった他部署から指示がなされ、困惑しながらの対応となる。

✓　**被害詳細のヒアリング**

SIRT は正確な情報の収集を望んでおり、仮に報告者のミスが原因であろうと責める意思はない。一方で、報告者は目の前で起きていることの説明で手一杯となっており、**ヒアリングの回答によっては自分の人事評価にマイナスに影響することを危惧する恐れがあると考えられる**。

コミュニケーションの留意点　-コミュニケーションでのつまずきやすいポイント

✓　専門用語を使わない

報告者はセキュリティの専門用語を知っているとは限らないため言い換えなどをして、**理解しやすい表現を使うことが望ましい**。「ランサムウェア」ではなく「データファイルを見ることができない形にして、金銭を要求するサイバー攻撃」と説明するなどの工夫が必要である。

✓　攻撃の情報は文字だけでなく画像でも集める

セキュリティの専門家である SIRT に対して、報告者が自発的に適切な形でサイバーインシデント情報を連携することは基本的に困難である。SIRT は、文字だけでなく、被害に遭った機器の写真やスクリーンショットの提供を求めたり、OT 側の制御機器などでは現地に赴いての直接の目視確認やリモート通話ツールを使ったりするなど、**情報の取り方を工夫することによって事態の正確な把握につなげることが必要となる**。

✓　SIRT の都合を押し付けない

SIRT は、報告者に SIRT 側が求めるスピードで正確に対応してほしいと考えている。しかし、業務が停止している可能性もあり、そのような場合、**報告者にとって優先するべきは自分の業務を早く再開することである**。報告者側の都合により迅速に指示を実行に移せない可能性があることを SIRT 側は把握しておき、急な対応を求めるのであれば報告者側の業務の都合を正確にヒアリングして優先度の判断を下すことが推奨される。

平常時のコミュニケーション　-つまずかないための普段からの工夫

✓　連絡事項の事前準備と周知

SIRT への連絡時に連携すべき項目を事前に取り決め、社内に周知しておくことによって、報告者の負担を軽減し、また対応フローを円滑に進めることが期待できる。誰が・いつ・何を・どこで、発見したかの 4 点を意識して情報を回収すると、基本的な状況の把握がしやすくなると考えられる。可能であれば、**業務影響や事業影響の有無、現状がどうなっているか、報告するまでに何を実施したかの情報までを報告事項に含めておくとより詳細な情報が集まる**。

✓　些細なことも連絡しやすい環境づくり

サイバー攻撃は一見すると機器やシステムの異常/故障と見分けがつかない場合も多い。とくに OT 環境の場合、たとえば制御装置が攻撃されて製造設備が停止すると最初は設備異常を疑うことが考えられる。**実際はサイバー攻撃ではなかったとしても「何かおかしい」と感じたら SIRT に相談してもらうような組織風土作りが必要**である。

セキュリティ担当者の声

- セキュリティ部署が出す通達などは、他部署にとっては面倒事であるかもしれないことを念頭に置く。他部署との関係性が成熟していないと、依頼したチェックシートの提出が遅れることや、できていないことを隠すなどの事象が発生し、積み重なると大規模インシデントにつながる恐れがある。**被害の少ない段階で問題を解消するには、他部署との良好な関係が欠かせない。**
- グループ会社を含めたリスク管理規定がある。誰が決断したか明確になり、アナウンスも総務や広報が最終決定をすると決めてある。
- セキュリティ部署が全てのシステムを監視することはできず、現場側で異変を見つけることも多いので、**日頃から会話をしてお互いに相談しやすい関係を構築している。**たとえば、わかっている情報が少なくても、相手の顔がわかっているとより細かい情報を聞きやすい。関係性ができてくると、ボヤのようなケースでも情報共有してもらえるようになる。今では**現場側から「サイバー攻撃ではないかもしれないけど情報共有しました！」という報告が挙がってくる。**

3.3.2　SIRT – 経営層のコミュニケーション

サイバーインシデントの被害の大きさはさまざまで、被害影響が一時的な場合もあれば事業が停止するまで被害が拡大する場合もある。SIRT は自社に起きている状況を経営層に共有し、必要に応じて投資判断や経営判断を仰ぐ必要がある。以下に経営層とのコミュニケーションのポイントについてまとめる。

SIRT		経営層
状況を正確に伝えないといけない わかりやすいように数字を多めに含めよう	**対応状況の報告**	細かく説明されてもわからない 結局何を判断してほしいのか？
早く判断してもらわないと 被害がますます広がってしまう	**事業・サービス停止等の経営判断**	いくら損害が出るのか？ いつまでに回復できそうなのか？
事業影響があったことを世間にも公表しておかないといけない	**対外発表**	何を話せばいいのか？

交わされるやり取り　-インシデント発生時の必須コミュニケーション

✓　**サイバーインシデント対応状況の報告**

サイバーインシデントはシステムの侵害後も状況が常に変化する。SIRT は状況を追跡しつつ、被害規模や被害影響に関する情報を集め、復旧に向けて動いていく必要がある。一方、経営層としては被害台数や攻撃者についての細かい情報を、経営層としてすべき判断の材料としてうまく活用できない場合もある。SIRT と話す時間も限られているので、**経営判断に必要な最低限の情報を多く求める**。

✓　**事業・サービス停止等の経営判断**

サイバー攻撃は、時間が経過するにつれてその被害を拡大させていくことが多い。被害の拡大を途中で食い止め、封じ込めるためにシステムや設備を停止することは取り得る手段の 1 つである。SIRT としては、被害を早急に封じ込めるために可能であればシステムの停止を行おうとする。システム停止は提供しているサービスの停止、製品の製造停止のような業務および事業への重大な影響が伴う。これらは企業の営利活動へのマイナス要因のため経営判断が必要になる。経営層としては簡単に判断ができるものではないので、**十分な情報を基に適切な判断をしたい**と考える。

コミュニケーションの留意点　-コミュニケーションでのつまずきやすいポイント

✓　経営層は経営の観点で評価する

SIRT が経営層に報告する際には、互いの観点に差があることを意識してコミュニケーションをとる必要がある。SIRT はサイバーリスク対応の観点から、サイバーインシデント被害の把握と拡大の防止が目的なので、被害台数や攻撃の種類、拡大防止のための対策検討を行う。**経営層はビジネスリスク対応の観点から、企業活動の最大化、サイバーインシデントに伴う企業活動の鈍化に伴う機会損失、賠償金やレピュテーションリスクが重要**であり、そのことに関する情報の収集が必要と考えている。

✓　判断は Yes/No で回答可能な状態にしておく

経営層に判断を仰ぐ際は、経営の観点から分析を行った結果を示し、経営層が Yes/No で判断・回答できる状態まで SIRT 側で提案を練り上げることが望ましい。SIRT としては負担が大きいが、このような検討を行った上でコミュニケーションをとることによって**経営層を巻き込んだ迅速な対応**が可能となる。

平常時のコミュニケーション　-つまずかないための普段からの工夫

✓　SIRT 活動の定期報告

サイバーインシデントが起こっていない平常時からも SIRT の活動をアピールすることが重要である。経営層に対しては平常時も、SIRT の活動を月次程度の頻度で報告することが望ましい。たとえば、**同じ業界のサイバー攻撃の詳細や件数、攻撃のトレンドや他社重大サイバーインシデントの自社への影響分析結果などの活動を報告し、SIRT と経営層の信頼関係を構築**しておくことが重要である。

✓　経営層のプロファイリング

経営層に所属する人が持つ業務背景やその担当領域によって、どのような内容を気にするかは異なる。技術系出身であれば、被害の台数やサイバー攻撃の特徴などの詳細情報に関心を持つ場合もある。一方で、生産など事業部門出身の経営層であれば、事業にどの程度影響があるのか、いつ再開できるのかを気にすることが考えられる。サイバーインシデント対応において、レジリエンスの観点から経営判断を含めた速やかな判断が早期収束に必要であるため、判断をくだす経営層に、どの話題に需要があるのかを把握しておくのは有効な手段の 1 つである。日常的な SIRT の活動報告を通じて、経営層がどの点に関心を持つのかを把握することによって、**需要を考慮した内容を含めた報告をして速やかな決裁を受けることができる**。

セキュリティ担当者の声

- **セキュリティ部署が、提案の内容からお金の話まですべて含め、**これでいきますけど問題ないですよね？というレベルまでもっていく。
- **経営者にはセキュリティ組織の成果（我々がどれだけ攻撃を防御しているのか、これだけ貢献しているのか）等を伝える。**経営層は頻繁に変わるので、日常的にどれだけ自分たちをアピールするか、どれだけ理解してもらえるかの取り組みが重要。

3.3.3　SIRT – システム担当者のコミュニケーション

SIRT からシステム担当者への依頼事項として、ネットワークやシステムの変更・停止・復旧に関するものが多い。両者は業務で取り扱うものが比較的近いので、情報は伝わりやすいが、業務の優先度などで認識の違いは発生する。以下にシステム担当者とのコミュニケーションのポイントについてまとめる。

SIRT		システム担当者
サイバー攻撃の分析に役立つような証跡を渡してほしい	**ログ等の証跡の収集**	セキュリティの専門ではないから必要としているデータがわからない
サーバーの停止やネットワーク隔離を速やかに実行してほしい	**被害拡大防止の処置**	ユーザ連絡も必要だがシステム部門としてどこまでやればよいのか？

交わされるやり取り　-インシデント発生時の必須コミュニケーション

✓　**ログ等の証跡の収集**

サイバー攻撃の経路や特徴を判別するために、SIRT としては攻撃を受けた端末からログファイルを収集することや、攻撃が発生した時間帯のネットワークトラフィックのデータを確認するなどの対応を行う。しかし、SIRT としてすべての証跡を集められるわけではないので、一部はシステム担当者にこのような証跡の収集作業を依頼しなければならない。システム部門はセキュリティおよびサイバーインシデント対応の専門家ではないことから、**証跡収集の方法やその授受方法まで経験がないことが多く、サポートを求められることも考えられる**。

✓　**被害拡大防止の処置**

SIRT がシステム担当者に依頼することの具体的な処置として、被害拡大防止のための処置や、システム停止、および再稼働の調整が必要である。例えば、侵害されたサーバの隔離、ネットワークトラフィックの監視強化やセキュリティパッチの即時適用などである。システム側としては**通常業務の途中で、突然発生した SIRT からの依頼に対応しなければならず**、対応のための緊急要員や現行業務との調整を急遽行わなければならない。

コミュニケーションの留意点　-コミュニケーションでのつまずきやすいポイント

✓　指示内容の明確化と緊迫感の共有

システム担当者は SIRT の指示する作業内容は理解できたとしても、それをどの程度の温度感でいつまでに実施すればよいのか、何に注意すればいいのかまでは分からない。**SIRT がシステム担当者に指示を出す場合には、期限や留意事項を伝え、両者の間で、作業内容の認識の食い違いが発生しないように努めるのがよい**。また、システム担当者の業務の間に割り込む以上、なぜその対応が必要か、その理由を明確に伝えると相手の納得感も得られることが考えられる。

加えて状況の緊迫感を共有することも重要である。業務に重要なシステムが標的にされている場合、時間との戦いであることを理解してもらう必要がある。

✓　継続的なサポートと責任の共有

対応依頼を出した後も、**SIRT が継続的にサポートをする姿勢を見せることは、システム担当者との信頼関係を維持する上で必要となる**。「進行中に不明な点があれば連絡をいつでも受ける」など自分が「味方」であると伝える。システム担当者側が対応状況について随時情報共有をしていくことで、SIRT は必要に応じて追加の対策を講じることができるようになる。また、システム担当者側は実施した対応が適切だったかどうか、次に何をするべきかの連携がスムーズになる。

平常時のコミュニケーション　-つまずかないための普段からの工夫

✓　依頼事項の事前説明

緊急時にシステム担当者との対応がスムーズに行われるように、SIRT はサイバーインシデント時に依頼する事項について事前に共有しておくことが望ましい。使用される専門用語やシステム特有の単語など、細かい点についても認識を合わせておくとよい。SIRT はシステムの仕様や運用体制が理解でき、システム側としてもセキュリティに関する知見が得られるので、双方にメリットがある。そのためにも、窓口となるシステム担当者を決めておき、**SIRT から日常的にコミュニケーションをとり、密な情報連携を行う体制を整えておくことが重要となる**。

✓　サイバーインシデント対応フローの共有

サイバーインシデント対応フローをシステム担当者と共有し、その内容について認識合わせを行っておくことが望ましい。**SIRT にとって、サイバーインシデント対応中に万が一の際にはこのフローに基づいて依頼をするため、事前にフローをしっかりと共有し、システム担当側の理解を得ておくことが重要である**。SIRT としては、システム担当部署はサイバーインシデント対応において、ログの収集やシステム停止などでもっともやり取りをする部署の可能性がある。定期的にサイバーインシデント訓練を実施し、フローの実践によって相互の理解を深めると同時に、フローの問題点を発見し、改善していくことも重要である。

セキュリティ担当者の声

- 基本的には地道なコミュニケーションで相互理解を深める。聞き慣れないシステムや機器の導入の話や詳細な設定値の話をされると、難色を示されることがあるので不明点を引き出す場を設定し、**丁寧なヒアリングの上、相手部署の事情を理解していく必要がある**。
- **現場には「自分たちのシステムでおきたら～」など、自分事になるように話すことが大事**。また全部のセキュリティ対応をやってもらうのではなく、まずはここからやりましょうとSTEP を踏んでもらうことが大事。
- **統計的な話をしながらセキュリティリスクの紹介をしてシステム導入の意義を説明する**。費用は誰がもつのか、決済はだれがするのかなど。組織全体で同意されているが、個別で同意が取れない時にはトップダウンにする。
- 社内に SIRT 体制を構築し、各部署へ周知している。また、各部署から迅速にサイバーインシデント情報がエスカレーションされるように、各部署におけるサイバーインシデント対応マニュアルの雛形を公開し、**サイバーインシデント時の各部署内の連絡フローを作成**いただいている。

3.3.4　SIRT – バックオフィス（広報・法務）のコミュニケーション

SIRT としての対応はサイバー攻撃の原因究明や封じ込めをするだけでなく、法律の観点から実施すべきことについてもハンドリングしていく必要がある。このような場合、SIRT の専門分野とは異なるため他の専門部署にその業務を依頼することが多い。

SIRT		バックオフィス
サイバーインシデントの内容を公表できる形にしてほしい	**社外に向けた発信**	伝えられた内容が専門的で理解できない
法律の中で留意すべきポイントを教えてほしい	**法律対応**	サイバーインシデントに関連する法律が分からない

交わされるやり取り　-インシデント発生時の必須コミュニケーション

✓　**社外発信のための調整**

企業が提供しているサービスや事業に一時的に被害があった、または情報漏洩があった場合には、顧客に対して説明を行う必要が出てくる。経営層から記者会見をするということになれば、何をどのようにどのタイミングで発表すればいいのかを決める必要が出てくる。

SIRT は社外対応を行うことが少ないので、広報部門にその業務を依頼することになる。SIRT は公表の範囲や発表の内容について、サイバー攻撃や被害の状況などを迅速にまとめなければならない。広報部門にとっては、**セキュリティという専門性の高い内容を対外発表に向けて理解・解釈する必要があり、フォローがない状態ではハードルが高い業務である**。

✓　**法律対応**

個人情報、機密情報の漏洩、業界特有の規制やサイバーインシデントにより契約先へ義務の不履行など、**サイバーインシデントの内容によって法律に抵触する事態が発生する可能性**がある。SIRT は法律の専門家ではないので、法務部門に対応を依頼することになる。法務部門はサイバーインシデントに馴染みがないため、どの法律が関連するのかを洗い出すには時間がかかる可能性もある。必要に応じて、IT やセキュリティに詳しい弁護士にも相談することを検討する。

コミュニケーションの留意点　-コミュニケーションでのつまずきやすいポイント

✓　部署ごとに伝わりやすい表現は異なる

SIRT が使用するサイバーセキュリティの用語は略称が多く、他部署への説明に適していない。**部署ごとの文化や背景知識が異なることを考慮し、相手に正しく伝わるように、相手の部署に言葉や伝え方を合わせる必要がある**。たとえば、広報部門はいずれマスコミに情報を伝えるため、マスコミにも理解しやすい言葉を使わなければならない。そのためには、SIRT 自身も自分たちの使う専門用語を正しく理解し、説明できる状態になっておく必要がある。

✓　相手に任せきりにしない

広報部門や法務部門の内容は SIRT の業務と内容が大きく異なっており、**業務をまったく知らないということもコミュニケーション上でつまずくリスクとなり得る**。そのため、SIRT がどこまでを対応して、広報や法務部門がどこまでを対応するのかなどの業務の線引きをしておくことが重要となる。SIRT にとって、相手の業務を理解して連携の準備をしておくことは、サイバーインシデント対応時の円滑なコミュニケーションにプラスになる。

平常時のコミュニケーション　-つまずかないための普段からの工夫

✓　サイバーインシデント対応訓練を通した改善点の洗い出し

サイバーインシデント時に速やかに連携が取れるように、サイバーインシデント対応訓練を実施し、どの部分で問題を抱えているかをお互いに把握し、継続的に改善をしておくことが必要である。**サイバーインシデント対応訓練は「SIRT の想定通り上手く実施できるか」を評価する手段ではなく、「想定通りにできないのはなぜか」に重点を置き原因を分析し、改善点を部署と議論する手段として実施するのが望ましい**。

✓　日頃から各担当部署と会話する

正しく SIRT の活動を理解してもらい、SIRT が各担当部署の味方であることを理解してもらう手段として、**些細な異変や問い合わせへの回答、セキュリティに関する業務への相談役として対応する**などが挙げられる。

✓　危機意識の共有化と協力体制の明確化

他社サイバーインシデント事例などを用いて、バックオフィスがサイバーインシデントの危険性に対して同じイメージを共有しておくことが必要である。**対応スピードや責任分界点を明確にしておくことで、サイバーインシデント時にコミュニケーションの齟齬が発生する可能性を下げる**ことができる。たとえば、「サイバーインシデント時のプレスリリースを作成方法」のような具体的な依頼をすることで広報担当者が何をすればよいのかが明確になり、合意しやすくなる。

セキュリティ担当者の声

- **相手に正しく伝わるように会話することが大事**。相手に伝わるように話題を合わせる。例えば、広報がマスコミに情報を伝える場合には、マスコミが理解しやすい言葉を使わなければならない。基本的にセキュリティの話が相手に伝わるように相手の立場に合わせてコミュニケーションをすることが重要である。
- **サイバーインシデント対応訓練をすることによって、サイバーインシデント時に部署がどういう動きをするのかを知ることができる**。事前に作られた社内ルールがあっても、全員が知らないこともある。訓練を通じてうまく機能していないルールを把握することができる。セキュリティ部署の観点でルールを作っているので、現場がルールを理解しづらい仕様になっていたことなども確認することができる。このようにして運用課題を見つけてルールを改善していく。
- サイバーセキュリティの話は専門性の高い言葉に聞こえるので犯罪的なイメージを受けられがちである。サイバー攻撃の観点からどういうリスクがあるのかカウンターパートの人ごとにどういう情報を共有し、どういうことをやってほしいかを意識しながらコミュニケーションをしている。**定期的にコミュニケーションをとる機会を開催することが重要で、月１回でもしっかりセキュリティの考えを伝える**。

3.3.5　OTSIRT –工場長のコミュニケーション

SIRT はシステムや設備へのサイバー攻撃の原因を調査するだけでなく、サイバー攻撃に伴う事業への影響を考慮した復旧計画を考えなければならない。そのためには、工場側に設備の復旧作業や、事業影響への分析、復旧計画の相談を行うことが必須となる。以下に工場長などの現場長とのコミュニケーションのポイントについてまとめる。

OTSIRT		工場長
現場のコントロールをしてほしい 現場の正確な状況が知りたい	**現場のコントロール**	何を優先させればいいのかわからない 何を伝えればよいのかわからない
事業影響を 正確に見積もってほしい	**事業影響の見積もり**	被害がどこまで広がっているのか わからないから見積もることができない
事業が継続できるのかどうかを 判断してほしい	**操業継続の判断**	判断までの猶予がわからない 自然災害と同じ復旧でいいのかわからない

交わされるやり取り　-インシデント発生時の必須コミュニケーション

✓　**工場側の状況**

SIRT は、サイバーインシデントの際に工場側と連絡を取りつつ、設備の切り替えや停止などの作業を行なってもらいたいと考えている。一方、工場長としてはサイバー攻撃のような馴染みのない事象の発生により、どの対処にどのように人を割けばよいかがわからない。また、**どのような情報を SIRT 側に渡せば工場が早く復旧するのかがわからない**。

✓　**事業への影響**

SIRT はサイバー攻撃を受けた機器や設備に起きた異常は把握できたとしても、その異常が事業にどの程度の影響があるかまではわからない。そのため、事業継続の可否とその決定のための必要条件を知りたいと考えている。一方で、**工場長としてはサイバー攻撃からの復旧方法はいつもと同じ復旧手順でよいのか、別の方法で復旧対応が必要なのであれば判断までの猶予はどの程度あるのかなど、スピード感や復旧方法決定のための判断材料が欲しい**と考えている。

コミュニケーションの留意点　-コミュニケーションでのつまずきやすいポイント

✓　事実は正確に伝え、正確に確認する

SIRT 側としては工場側との会話の中でサイバー攻撃からの復旧に必要な対応を共有しながら、SIRT 側と工場側で連携を繰り返し行っていく。スムーズな連携のためには、**すでにわかっている・決定している「事実」と、推測される事象や今後の予定は明確に分けて伝えていくことが重要である**。それは工場の状況をヒアリングする際にも同様である。

✓　工場側のスピード感をつかむ

SIRT は工場側はどういう動きをしているのか、どのような温度感・緊迫感で動いているのかをイメージできると良い。特に業務を行う箇所が物理的に離れているのであれば、コミュニケーションを阻害する原因の一つになりうる。SIRT は、**工場は企業の利益に直結する仕事をしており、設備が止まった際には、一刻も早い運転の再開を優先することを知っておく必要がある**。工場に優先的に対応してほしいことがあれば、工場側で実施している作業と比べてどちらが優先なのか、できない場合はいつまでに実施すればいいのかを伝えなければならない。

平常時のコミュニケーション　-つまずかないための普段からの工夫

✓　応急対応や復旧計画の事前共有

地震や台風などの自然災害と同じように、サイバー攻撃も BCP の対象に含めることを工場側には共有しておかなければならない。工場側の動きのすべてを SIRT で指示し、コントロールすることは難しいので工場側、とくに**工場長にはサイバー攻撃からの復旧計画を作成しておいてもらい、速やかに実行に移すことのできる体制を整えておく必要がある**。そのためには、サイバー攻撃によるサイバー攻撃の危険度や工場操業への影響などについて、平常時から定期的に工場側に情報発信、および工場側の事情の理解に努める必要がある。

✓　制御機器の特徴の理解

IT 系の SIRT においても**近年、制御機器を標的にしたサイバー攻撃も増加傾向にある以上、「わからないまま」の状況は避けるべきである**。OT システム、制御機器の特徴を把握しておくことで工場側とコミュニケーションが円滑に進む可能性がある。IPA [9]や JPCERT/CC[10] は制御システムセキュリティに関するガイドブックが公開されているため日常的に情報を収集しておくとよい。

---

[9] 情報処理推進機構, 制御システムのセキュリティリスク分析ガイド第 2 版, https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

[10] JPCERT/CC, 重要インフラのためのプロセス制御システム(PCS)のセキュリティ強化ガイド, https://www.jpcert.or.jp/research/2009/PCSSecGuide_20091120.pdf

3.3.6　ITSIRT – OTSIRT のコミュニケーション

IT 環境と OT 環境を横断したサイバー攻撃が発生した場合、OT 環境で起こった事象に関して IT 側に知見を求めたい場合など、ITSIRT と OTSIRT が連絡を取り合う場合が想定される。専門性が高い部署同士だからこそ、知見のギャップを補完するためのコミュニケーションは欠かせない。以下に SIRT 同士のコミュニケーションのポイントについてまとめる。

ITSIRT		OTSIRT
普段使っている用語が 違う意味に捉えられてしまう	**言語**	普段使っている用語が 違う意味に捉えられてしまう
優先するべきは システムの復旧、侵害内容の確認	**優先事項**	優先するべきは 安全性、操業の継続
IT環境のことは把握できる	**状況把握**	OT環境のことは把握できる

交わされるやり取り　-インシデント発生時の必須コミュニケーション

✓　**被害状況の共有**

たとえば、IT 環境から OT 環境に侵入し、制御機器を停止させるようなサイバー攻撃が発生したとすると ITSIRT と OTSIRT はそれぞれの環境の調査をし、情報を共有しながらサイバー攻撃の全容把握と復旧計画の立案に努める。ただ、ITSIRT は OT 環境のことを把握しておらず、逆に OTSIRT も IT 環境のことは把握していない場合もある。**被害の詳細を共有しても、具体的にイメージできない可能性がある**。

✓　**防御対策の実施の相談**

サイバー攻撃の被害拡大を食い止めるために、ネットワークの切断などの防御対策を検討する。この時、ITSIRT が気にすべきは攻撃の被害がどれだけ広がっているか、どうすれば早く復旧できるかである。一方で OTSIRT が気にすべきは、工場の安全や事業の継続性である。このように**復旧の際に優先する事項が異なると、実施する防御策とその実施タイミングに認識の齟齬が生じる**。

コミュニケーションの留意点　-コミュニケーションでのつまずきやすいポイント

✓　お互いの「当たり前」を知る

ITSIRT、OTSIRT はそれぞれ相手の特徴を知らないと話が噛み合わない時がある。たとえば、IT では専門用語を短縮したものが次々と登場し、ITSIRT は当たり前のようにその用語を使うが、OTSIRT には通じないことがある。たとえば、**ネットワーク図に「FW」という単語があったとき、IT では「ファイアウォール」と読み替えることが多いが、OT では「ファームウェア」と捉えることが多いこと**などが代表例である。IT 環境に従事する者にとってパッチを当てるなどの脆弱性への対応は当たり前だが、OT に従事する者にとってはパッチを当てることによって制御機器が停止する可能性があるので判断に検討に時間が必要である。

✓　防御対策に求めるものが違う

ITSIRT も OTSIRT もサイバー攻撃を受けないように防御対策を事前に実施しておき、正常状態を維持しようとする意識は共通している。**環境の特性の違いから、そもそも防御対策の要求仕様が異なっていることを認識しておかなければならない**。IT 環境では、サイバー攻撃者側の技術や手法の進化が速く、ある防御策をとっても時間が経てば役に立たなくなるという現象が頻繁に起こる。サイバー攻撃を受けた時は、機器の取り替えやネットワークからの遮断などの方法でカバーするというレジリエンス観点での対応も必要である。一方、OT 環境ではシステムや機器が 10 年、20 年と長く使われる傾向があり、物によっては 24 時間 365 日稼働しているので、IT のように交換やネットワークの接続を切るといったことが容易にできない。

平常時のコミュニケーション　-つまずかないための普段からの工夫

✓　IT と OT の価値観の認識合わせ

IT と OT ではセキュリティに求めるものが違うが、それぞれが求める仕様は両方とも正しい。サイバーインシデント時に ITSIRT と OTSIRT の連携を円滑にするためには、お互いの価値観を理解しておくことが必要である。とくに、サイバーインシデントを想定して決めておくべきことは多数ある。ITSIRT は何を OTSIRT に伝えればいけないのか、逆に ITSIRT には何を伝えるのか、事業影響がある判断はどちらの責任で行うのか、どの設備は停止できるのか、どのネットワークは停止できないのか、などのコミュニケーションが挙げられる。**責任分界点、停止判断など事前に基準を設けておかなければならないものは多種多様である**。これらを決めないままサイバーインシデントが発生するとその分、意思決定が遅れさらに被害が拡大する可能性がある。いかなる防御策をとったとしてもサイバー攻撃を 100%防ぐことは難しいが、日常的な情報交換によってお互いの価値観や優先事項を共有し、最適な着地点を模索していかなければならない。

セキュリティ担当者の声

- 詳細アセスメントの規模感は IT/OT では大きく異なる。そのためシステム毎にブレイクダウンしていってアセスメント内容を共通認識としていく必要がある。**共通認識とするために、部署に相談相手を作ってもらって週 1 回相談する、セキュリティがシナリオを作って相手に評価してもらうなどの試みをしていた**。

第４章

サイバーレジリエンスのための
コミュニケーション総論

ここまで、企業におけるサイバーインシデント対応時の他部署とのコミュニケーションとその留意点についてヒアリングおよびアンケートの内容を基に述べてきた。これらの調査から導き出された、企業において**サイバーレジリエンスを実施していくためにコミュニケーションの観点から必要な要素について大きく 3 つにまとめる**。

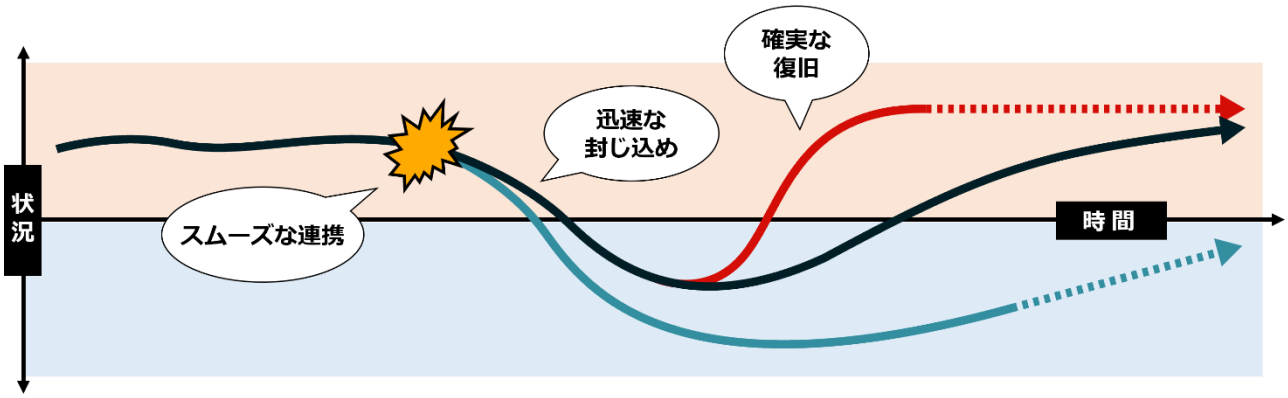

図 4.1 サイバーレジリエンスを実施していくために必要な 3 要素

1：サイバーインシデント対応フロー改善のためのコミュニケーション

サイバーインシデント対応時には対応フローに乗っ取った連携が基本として行われる。本書作成にあたって調査したヒアリングやアンケートの結果によれば、サイバーインシデント対応をスムーズにするためにフローを作成するだけでなく、**これらのフローを用いた連携のデモやサイバーインシデント対応訓練を行いフロー自体の改善活動を行っていた**。継続的なフローの改善によって部署ごとの連携のしやすさを維持するとともに、現実の業務に即したフローを作成・実現していることがわかった。

2：共通認識醸成のためのコミュニケーション

サイバーインシデント時には専門性の違いがある他部署との連携を強く求められることから、「セキュリティ以外の専門性の高い人材にセキュリティ教育を行う」ことにより、サイバーインシデント対応時の連携を強化するという工夫も見られた。これは、サイバーインシデント時に、セキュリティの知識を有する人材を配置し、**セキュリティにおける共通認識の醸成を平常時より行うことによって、コミュニケーションを取りやすくするという工夫であった**。また、ニュースで取り上げられた他社のサイバーインシデント事例や、世論の動向などを定期的に共有することにより、平常時からコミュニケーションをとり共通認識を図る工夫をしていることが明らかになった。

3：事業リスク理解のためのコミュニケーション

一つの企業の中でも取り扱うシステムにはその特性は多様である。とくに制御システムにおいては可用性の必要性やその業務影響範囲はさまざまである。また、異常が発生した場合の対応もそれぞれのシステムに依存する。**サイバーセキュリティ対策の観点からの封じ込め、復旧の対応を考えるために自社が保有するシステムとその事業リスクについて把握し、レジリエンスを実現する対応の確実な実行のために、あらかじめ経営層から現場までコミュニケーションをとることが重要である**。

<コラム>経営層とのコミュニケーション

下記コラムは IPA の開催する中核人材育成プログラムで開講された講義で教鞭を取られた元経営者の方に添削していただいた資料です。

- **経営層の会話プロトコル**

部長級以上の役職者、ここでは経営層と定義する人材と SIRT が会話するときの進め方を習得するために、まず経営層の思想と活動を理解する必要がある。

経営層の思想とは会社のあり方や経営者の振る舞いを決める哲学や経験法則、価値観や気づき、道徳心などに基づく言葉であり、思想である。例を挙げれば京セラ創業者の稲盛和夫氏の「動機善なりや、私心なかりしか」、元経団連会長の土光敏夫氏の「幹部はえらい人ではなく、つらい人だと知れ」、松下電器産業創業者の松下幸之助氏の「真使命を知る」などがある。それぞれの言葉には多様な背景があり、戒める対称人物や考え方が異なる。経営層に寄り添ったセキュリティ提案を実現するには、対話する経営層の「尊重する思想」を SIRT が学び、同調し、実践し、経営層が見据える企業のあるべき姿を SIRT 自身の中で共有する必要がある。このためには経営層への弛みないコミュニケーションが必要だ。

経営層の活動は大別して二つある。経営層の第一の活動は、自社のビジネス戦略を計画し上手く推進し、市場での競争優位性を向上させ、社会貢献すると共にステークホルダーに利益を還元することである。ここでの活動は短期および長期の業績や株価の推移などの数値により表明した事業計画に対する結果だけで評価される。経営層の第二の活動は、企業経営の透明性を維持・確保するコーポレートガバナンスである。コーポレートガバナンスはコーポレートガバナンススコアやコンプライアンス事象などの複数の指標で社会から評価される数値である。コーポレートガバナンスを軽視すると、株主のみならず社会からの信頼を喪失することになり、会社全体のレピュテーション（企業価値評価）の低下を招き、最悪、事業存続ができなくなる。

経営層は社会から評価され得られた数値を分析し、上記の二つの活動を行っている。ここで SIRT が経営層に寄り添って提案する際には「どの活動に対して」「どのような影響を与えるのか」を「数値」で表現する必要がある。

- **セキュリティ予算はコスト？投資？**

SIRT が経営層に対して要求する事柄の代表はセキュリティ施策を実施する予算である。SIRT からのセキュリティ予算要求後、経営層からセキュリティ予算要求を差し戻されることがある。なぜなら、経営層は予算がコーポレートガバナンスの観点から「コスト」であるのか「投資」であるのか判断に迷い、次に競争優位性の観点から可否判断ができないからだ。

SIRT の視点では分類がコストであっても投資であっても同じ予算だが、経営層の視点では予算の分類はコーポレートガバナンスの活動に関連しており、適切に分類できない予算は最終的に企業ポートフォ

リオに悪影響を与え、レピュテーションを低下させるリスクがある。また、予算を投じることは競争優位性の向上活動にも関連していて、予算の分類がコストであれば削減の対象である。投資であれば自社の経営戦略と照らし合わせる必要があり、良い影響がある場合には予算を承認し、大きな良い影響がある場合には予算増額の対象になりうるからだ。

経営層へ寄り添い改善されたセキュリティ予算要求を提案すると、提案は経営層の次なる懸念に直面する「この提案の費用対効果は妥当なのか？」

- **セキュリティ予算の費用対効果**

「セキュリティ効果を費用対効果で測れる訳がない」これは SIRT の考えであって、経営層に寄り添った考え方ではない。幸いなことにセキュリティ予算の根拠となる定量的な数値を含む資料は無数に存在するので客観的な根拠を提示し理解を促すことは難しくない。例えば、他社のサイバーインシデント事例対応を例示することで、流行している攻撃に対して提案が有効であることを示すことができ、被害金額や対応金額も定量的事実として説明することができる。他の提案方法として、バランスト・スコアカードを用いた分析を行うことで、経営戦略上のセキュリティ提案の立ち位置と関連性を示すことができ、組織へ与える影響と定量的な効果を説明することができる。

- **経営層を巻き込んだセキュリティを実現するには**

多くの場合、経営層は他社のサイバーインシデント事例を見聞きし、コーポレートガバナンスの観点から災害や事故などのリスクと同程度にセキュリティ施策に取り組まなくてはならないことを理解している。しかし、SIRT 活動に対する経営層の知識・理解不足から、適切な方針を示すことは難しい場合も多い。

SIRT の立場で経営層への寄り添い方を論じてきたが、SIRT 自身が経営層の思想と役割を理解できておらず、経営層の期待する提案ができていない可能性も大いに考慮しなくてはならない。セキュリティ提案は経営層が想定するコーポレートガバナンスを考慮しているだろうか？最近のサイバー攻撃方法や組織のセキュリティ施策の網羅性に偏重して、市場での競争優位性に悪い影響を与えてはいないだろうか？ 経営層を巻き込んだセキュリティには SIRT 自らが経営層に寄り添う姿勢を堅持し、技術的な手段だけに終始せず、経営層の理解不足を補完し、経営の目的を理解・共有することが必要である。これの実現のために、SIRT と経営層が密にコミュニケーションをすることで、経営に直結したセキュリティ施策を実現できる可能性が広がると考える。

あとがき

本書では、サイバーレジリエンスのためのコミュニケーションをセキュリティ担当者がコミュニケーションスキルとして活用していくためのポイントとその調査内容の解説を行った。

サイバーレジリエンスのためのコミュニケーションは、セキュリティ施策を展開するための活動をサポートするためのコミュニケーションスキルの概念であり、絶対的な正解が存在するわけではない。そのため、自社の持つ技術や環境要因を把握することとともに、他部署の業務を理解し、部署を跨いだ連携を意識したコミュニケーションを行うことが重要である。実際の業務の中では、担当者の人事異動やシステムに関連する技術の進化などもあることから、定期的にサイバーインシデントに関する現状の課題を洗い出し、その結果を元に将来的にどうありたいかを明確化することも重要である。「サイバーレジリエンスのためのコミュニケーション」は目的ではなく、組織としてさまざまなサイバー攻撃にレジリエントに対応していくためのコミュニケーションスキルとしての手段であることを理解していただきたい。

サイバーレジリエンスコミュニケーションを実施していくためには、さまざまな部署も、サイバーセキュリティの対応をする可能性があるということを理解してもらうとともに、サイバーセキュリティの脅威をいたずらに過大に伝えるのではなく、どのような準備、対応を行うことが迅速な対応に繋がるかを理解してもらう必要がある。そのため、サイバーインシデント対応訓練などを通して部署を跨いだ連携を経験し、コミュニケーションに必要な情報を経験してもらうような活動も重要である。

また、本書で示したサイバーレジリエンスのためのコミュニケーションはあくまで情報連携の改善手段であり、それだけではサイバーインシデント対応が完了しないことに留意していただきたい。自社のサイバーセキュリティを担当している実務者としてサイバーセキュリティに関する知識技術を鍛錬した上で、それらのスキルを活用するためのコミュニケーションスキルである。企業単位でサイバーセキュリティをレジリエントに対応していくためには、部署間連携が不可欠であり、その手段であるコミュニケーションを味方にすることによって業務を進めやすくすることができるという考え方のもとに行っている。組織で一体となってサイバーインシデントに対応していくことを検討していく際に、どのような情報を各部署で連携しておくべきなのか、どのようなことに留意すべきなのかを検討するための必要な考え方を本書に詰め込むことができたと考えている。

なお、本書は 2024 年 8 月時点での考えのもとに執筆したものであることに留意していただきたい。サイバーレジリエンスを実現していくために、さまざまな部署と連携し、サービスを安定供給しつつ組織でセキュリティに対応していくために、その企業の事業内容や技術に留意して最新の情報や技術を常にアップデートしていく必要がある。

本書がサイバーセキュリティに関する部署連携の助けになれば幸いである。

Appendix

ICSCoE 修了生へのアンケート

本編で紹介した ICSCoE 修了生へのアンケートの結果を紹介する。

回答数：110 名

実施期間：2024 年 4 月 22 日　―　2024 年 5 月 18 日

- サイバーインシデント時に他部署とのコミュニケーションを取るにあたり、文化や価値観のずれによって意図した通りに伝わらないと感じられたことはありますか？

  そう思う：　48
  ややそう思う：　47
  どちらともいえない：　5
  あまりそう思わない：　8
  そう思わない：　2

- サイバー攻撃の被害の大きさや重大性の認識が組織間によって違うと感じられたことはありますか？

  そう思う：　55
  ややそう思う：　40
  どちらともいえない：　6
  あまりそう思わない：　9
  そう思わない：　0

- サイバーインシデント発生部署側は、セキュリティ部署の指示を正確に理解し、セキュリティ部署が求めている対応スピードで、必要な対応を行動に移せている/移せると感じられますか？

  そう思う：　6
  ややそう思う：　32
  どちらともいえない：　35
  あまりそう思わない：　29
  そう思わない：　8

- サイバーインシデント対応終了後、振り返りが行われ、その経験が社内に共有されていると感じますか？

  そう思う：　13
  ややそう思う：　41
  どちらともいえない：　27
  あまりそう思わない：　19
  そう思わない：　10

- サイバーインシデント対応時の判断基準やその責任範囲は、サイバーインシデントの種類,規模ごとにそれぞれ明確に定められていると感じますか？

  そう思う：　17
  ややそう思う：　38
  どちらともいえない：　17
  あまりそう思わない：　31
  そう思わない：　7

- 組織の中で部署を跨いだ連携、特に現場から経営層までの橋渡し人材としてサイバーインシデントに対応していくために特に必要だと思うことを３つ選択してください

項目	回答数
相手に配慮したわかりやすい説明	58
他部署、および他事業の業務理解	48
情報を正確に伝達する説明力	37
サイバーインシデント対応の経験	30
経営層目線の考え方	30
社内規則・規定の理解	21
セキュリティに関する問い合わせのしやすさ	17
攻撃対象になりうる機器・システムの技術的知識	17
適切なリスク管理能力	13
予算や人員を獲得するための交渉スキル	12
日ごろからのセキュリティ情報の発信	11
セキュリティ教育の充実	7
部署内のチームワーク	6
戦略的思考	4
愛嬌	3
倫理観	3
新しい技術への理解と意欲	2
最新技術に関する情報収集	1
社外セキュリティコミュニティへの報告・相談	0
その他	10

- サイバーインシデントを組織として対応していくにあたって課題として感じている問題点を解消するために、取り組みを実施したこと、または日頃から行なっている工夫・取り組みについて教えてください。※回答した修了生の属する企業の業界ごとに分類して紹介

電力業界

- サイバーインシデント発生時の発生箇所へのヒアリング内容のテンプレ化、およびテンプレ化した内容の都度のブラッシュアップ。
- 非セキュリティ人材の「サイバーリスク」に対する無関心を減らすこと。
- サイバーセキュリティの技術的な側面のみに偏ることなく、エンドユーザレベルに対しても注意喚起を促すのに有効な情報の収集、周知。
- 日頃からの部署を横断したコミュニケーションによる、いつでも些細なことでも相談しやすい関係作り。
- 社内規程の記載内容の具体化。
- セキュリティ教育の充実・攻撃対象になりうる機器・システムの技術的知識の習得を目的とした勉強会の実施。
- 従業員のサイバーセキュリティへの関心向上のため、興味を持ってもらえるよう身近なサイバーセキュリティに関するコラムを作成し紹介。
- 相談を躊躇する組織であってはならないよう、社内からの相談・問い合わせに対しては特に丁寧にフォローするような心掛け。

金融業界

- サイバーインシデントを想定した訓練の実施（担当者向けと経営層向け）。
- 現場などの Non-IT なスタッフのセキュリティについての意識、底上げが非常に重要と考える。セキュリティ対策の説明に、サイバーインシデント事例のニュース記事などを引用して紹介することをボランタリーに実施。サイバーインシデント事例を用いることで、具体的にその対策で何を防ぐことが出来るのかイメージしやすく、導入の必要性に説得力が増す。
- サイバーインシデント対応の経験の積み重ね（冷静さや先を見越した対応判断など）。

自動車業界

- 法務部署や人事部署、広報部署などはサイバーインシデント時に連携が必要になることが多いため、連携強化のためにサイバーインシデント時の役割合意や、定期的なサイバーインシデント事例の紹介による意識向上を実施。
- SIRT 活動の日次確認によるグループ会社対応状況の把握と是正。
- SIRT 活動の月次役員報告による経営層理解の促進とグループ統制の強化。
- サイバーインシデント情報は、部署内コミュニケーションツールで共有。
- 日常的に問い合わせを受ける立場にあるので、その中で各々の組織の役割を周知・啓蒙する。

情報通信業界

- 脆弱性情報やセキュリティ面の対応連絡など、メールやチャットツールなどによる連絡ルートを用意し、相互の情報連携を取りやすくする。
- サイバーインシデント時の役割を予め決め、発生時に素早く人を割り当て対応する。
- 全ての脆弱性に対応するのは不可能である前提で、自社のシステム環境やビジネスを考慮した上で脆弱性の影響度を定義し、対応フローを確立。
- 新しいセキュリティの取り組みを始める際は、文章だけでなく説明会を開催して意見をもらう。
- 常日頃からフローや連絡先の確認。
- 日頃から他部署とコミュニケーションを取り、なにか少しの異変が合った際は気軽に連絡を貰えるようにする。

鉄鋼・非鉄業界

- 社内の比較的大きな会議、報告会などの場でセキュリティに関する報告を行うことで、セキュリティは社として推進している活動という事の理解を推進。
- OT 部署内の検討会へオブザーバ参加することで、日ごろからセキュリティを身近に感じてもらうと共に、自身の目線を OT 部署の近くに置くようにする。
- 幅広い情報発信を実施。「IT に関する情報」ではなく、「リスク管理の関する情報」として、品質管理や人事などが主体となるリスクマネジメント関係の会議でも情報発信を行い、リスクのひとつとして情報セキュリティリスクがあることの浸透を図る。

鉄道業界

- イントラネットを使った、e-ラーニング研修やグループ会社向けに情報発信。
- FAQ を充実させることや、社内フォームで質問できるようにして、問い合わせのハードルを低くする。
- システム監査人として情報システムを所管する各部署（被監査箇所）がセキュリティ面で不適切な運用を行っている場合に情報システム部署に照会してもらい、適切なセキュリティの管理ができるような改善を働きかけている。

電機/産業ベンダー/製造業界

- 経営層への報告・判断を仰ぐ際、以下を徹底。
  - ・ 結論から伝える
  - ・ 専門用語は極力使わない
  - ・ 事実は事実としてはっきり伝える
  - ・ 曖昧な言葉は使わない（～と思います、～と考えられますなど）
- セキュリティ対策は新しい取り組みが必要であり、従来の部署のスコープわけでは対応しきらないため、仕事の押し付け合いが課題と感じる。解消するためには、新しい部署を創設するか、情報システム部署が柔軟に新しいことを受け入れる体制にしていく必要があると考える。
- 日ごろから、サイバーセキュリティ対策についてこれからは担当者のみが対応するのではなく、組織として対応する必要があることを上長に対してアナウンスする種まき活動を行う。
- セキュリティ意識を醸成し続けるために、世の中や社内の最新セキュリティ動向を踏まえた定期的な情報発信や社内教育、問合せ方法（仕方やしやすさ）を会社の仕組みとして整備・実践。
- インシデント通知メールの最初の返信で相手のスキルを判断して、出来そうなら任せ、難しいようであれば丁寧に対応する。
- サイバーインシデント対応に関する社内規則の整理（明文化）、専門組織の体制整備。
- 経営層のセキュリティへの理解が必須、加えて現場に落とし込むためには現場の業務理解（とくに、現場が何を大切にしているか）が必要であり、落としどころを上手に作る。

ガス業界

- サイバーインシデント発生部署と社内関係部署（経営層、広報部署、リスク管理部署等）ではものごとの見方、考え方に違いがあることを理解し、サイバーインシデント対応訓練等を通じて有事の際にサイバーインシデント発生部署が求められる対応、社内関係者に提供すべき情報が何かを日頃から把握する。

化学業界

- 経営層とのコミュニケーションパスの整備および定例報告、他リージョン／他部署などの業務内容に合わせた複数のサイバーインシデント対応訓練の実施、定期的なセキュリティ教育プレゼンの開催。
- サイバーインシデント対応を行う際、組織や事業所の生い立ち・業務所掌・関連法規・国(海外の場合）等を俯瞰して対応する。
- 役員を巻き込み、味方につける。
- 組織対応、対策製品の導入などを行う際、大風呂敷を広げず、出来る所から実践していく事が、結果として近道となりうる。
- サイバーインシデント発生時の対応をリアルに考えてもらうために、相手の業務で起こることを丁寧に説明する。そのために、一般の知識ではなく、自社の業務を正確に理解するために、

普段からコミュニケーションをはかるようにする。

- 制御系のセキュリティアセス等を通して、事業所・工場関係者とのコミュニケーションを大切にしている。結局、出来るだけ対面で話をする機会を設け、相手の日頃の業務をリスペクトし理解する事が重要と感じる。お互いに相手が分かれば、電話連絡もスムーズになる。

不動産/住宅/建築業界

- e-ラーニング等により、個人情報漏洩時等、報告スピードの重要性を理解いただくよう周知している。また、類似したサイバーインシデントが発生した際は、同一事象発生防止のため、速やかに全グループ周知を実施。
- セキュリティ事象発生時の連絡先を記載したセキュリティ連絡カードの社員への配布。
- 四半期毎の各部署長への情報セキュリティ報告。

その他

- セキュリティ専門部署以外の部署の人間がセキュリティ専門部署に相談するハードルを下げることを意識し、担当者間では些細な内容であっても情報共有するように努めている。
  ただし、セキュリティ専門部署の業務負担を増大させないよう、セキュリティ専門部署以外の部署の担当者には、サイバーインシデントで当該部署に求めている事柄や、セキュリティ関係のトピックなどを情報共有時に併せて伝えることを通じて、少しずつ、彼らに判断力を養ってもらうようにしている。
- 怪しい事象を覚知した時点で、他部署と情報共有や相談をするフローの整備。
- セキュリティに関する相談は絶対に断らない。なぜなら、他に誰も答えられる人がいないし、断った段階で二度と相談されないため。
- ホールディングス組織のため、企業のビジネス理解と各社固有リスクの識別を行うこと。また、企業やステークホルダーの良き支援者であること。具体的には、1on1 などを通じて先方の情報セキュリティ統括責任者も含む方々との対話を定期的に行っている。

謝辞

本書作成にあたりまして、ICSCoE 修了生の皆様にはセキュリティに関するコミュニケーションの考え方についてヒアリングさせていただくなど、多大なるご支援、ご尽力を賜りました。お世話になりました皆様にこの場を借りて御礼申し上げます。

また、産業サイバーセキュリティセンター中核人材育成プログラムの講師であられる、満永拓邦先生、門林雄基先生、佐々木弘志先生には本書の元となるサイバーレジリエンスコミュニケーションプロジェクトのメンター・講師としてご指導、ご助言とともにご支援を賜り続けてきました。改めて御礼申し上げます。また、IPA 中山室長にも、ヒアリング調整やサポートなどの支援をいただきました。御礼申し上げます。

そして本書の作成や、本プロジェクトを共に実施した下記メンバーの皆様にも感謝を伝えたいと思います。

〈サイバーレジリエンスコミュニケーション PJ メンバー〉

【リーダー】

西澤優里

【サブリーダー】

辰巳大祐　中角直毅

【メンバー】

鵜飼大介　北島稜平　齋藤祐理奈　谷口智哉　谷原侑馬　永淵亘　間木平伊織　皆吉遥

参考文献

1: NIST, SP800-160 Volume2, Revision1,
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

2: NIST, SP800-61r2 Computer Security Incident Handling Guide, 2012,
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

3: 情報処理推進機構,中核人材育成プログラム,
https://www.ipa.go.jp/jinzai/ics/core_human_resource/about.html

4: 芳賀茂, レジリエンスエンジニアリングの安全マネジメントへの応用のための課題と実践セーフティⅡを目標とする安全マネジメントの実践, 日本原子力学会誌, Vol.63 , No.10, 2021,
https://www.jstage.jst.go.jp/article/jaesjb/63/10/63_708/_pdf

5: NIST, SP800-172, 2024, https://csrc.nist.gov/glossary/term/cyber_resiliency

6: 情報処理推進機構, 責任者向けプログラム業界別サイバーレジリエンス強化演習（CyberREX） 事業内容, https://www.ipa.go.jp/jinzai/ics/short-pgm/cyberrex/index.html

7: 厚生労働省　重要事例情報―分析集(指示時のコミュニケーションエラー)
https://www.mhlw.go.jp/topics/bukyoku/isei/i-anzen/1/syukei6/9b.html

8: JPCERT/CC インシデント対応マニュアル
https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20211130.pdf

9:情報処理推進機構, 制御システムのセキュリティリスク分析ガイド第 2 版,
https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

10:JPCERT/CC, 重要社会インフラのためのプロセス制御システム(PCS)のセキュリティ強化ガイド,
https://www.jpcert.or.jp/research/2009/PCSSecGuide_20091120.pdf


Industrial Cyber Security Center of Excellence
ICSCoE