JPCERT CC®

CSIRT ガイド

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

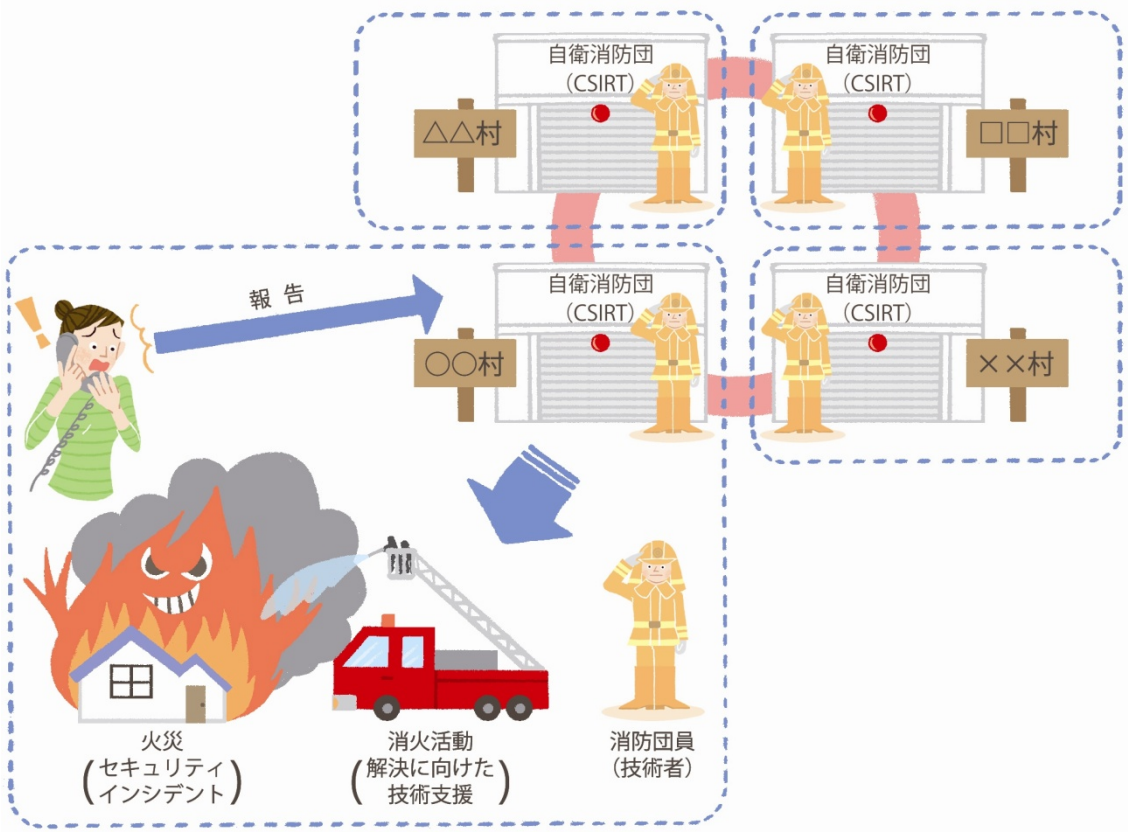
JPCERT CC®

はじめに

近年、著名な企業や官公庁等におけるサイバーセキュリティ侵害に関する報道が、国内外を問わず数多く目にされます。企業や組織の活動において IT への依存度が高まるとともに、IT システムを狙うサイバー攻撃はより高度化しその脅威を増しています。さらに IT システムが複雑化するにつれて、侵害の発見や原因の特定は困難となり、復旧に時間がかかるようになってきています。情報セキュリティ問題が企業や組織にもたらすリスクへの対応は、もはやシステム管理者だけの問題ではなく、経営層が積極的に関与しなければならない問題ですが、情報セキュリティインシデントへの対応には技術的に高い専門性だけではなく、業務に対する幅広い知識が求められます。

このような中で、多くの企業や組織では情報セキュリティ問題への対処を行う機能として、CSIRT（シーサート:Computer Security Incident Response Team）が設置、運用されてきています。

CSIRT はウイルス検知ソフトやファイアウォールといったセキュリティ管理策の導入に限らず、情報セキュリティインシデントやサイバー攻撃に関する情報収集、分析、リスク評価、インシデント対応ポリシーや手順の策定、外部組織との連携、リスクコミュニケーションなど、情報セキュリティに関する多くの事柄に関わり、それらの活動において中心的な役割を果たします。平時の対応はもちろん、情報セキュリティインシデントが発生した際にその被害を最小限に食い止めるといった有事の対応、更にインシデントからの復旧、原因究明および再発防止策の検討・実施などの事後の対応までを行ないます。このような一連の活動は、消防署の活動に似ています。組織を 1 つの村と考えれば、CSIRT は次の図のように「自衛消防団」にたとえることができます。



JPCERT CC®

今日では、日本国内の多くの企業や組織が CSIRT を備え、国内の代表的な CSIRT コミュニティーである日本シーサート協議会や、各業界の ISAC（Information Sharing and Analysis Center）を中心とした CSIRT 間の連携の枠組みが生まれ、活動を拡大しています。CSIRT は今日の企業や組織が直面するサイバーリスクに対応するために備えるべき基本的機能といえるでしょう。経済産業省が 2016 年に公表した「サイバーセキュリティ経営ガイドライン」では「CSIRT の整備」を経営層が指示すべき事項として取り上げており、また一部の省庁では所管する業界の構成企業に対して CSIRT を中心としたサイバーセキュリティへの対応体制を整備することを求めています。そうしたことを背景に、現在 CSIRT を持たない企業や組織において CSIRT を構築しようとする動きは今後も増えていくものと思われます。
本書の初版は 2008 年に、これから自組織内に CSIRT を構築しようと考えている組織の経営層や、CSIRT のメンバーとなる社員の方向けの入門書として公表しました。その後 2015 年に、高度サイバー攻撃（APT）に関連する記述を追記した改訂版を公表しています。今回の改訂では、国内外の組織において CSIRT が普及し多くの組織で広く運用されるようになった現状を踏まえた記述の修正を行い、それでも基本的なメッセージは変えず、CSIRT のコンセプトと組織構造、活動内容について簡潔に説明する資料として作成しました。

> 米国 CERT/CC が作成し、JPCERT/CC が翻訳した「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」が CSIRT 構築前だけでなく、構築後も「辞書」として使えるものであるのに対し、本書は CSIRT 構築前に読む「読み物」という位置づけになります。

なお本書では、さまざまな種類の CSIRT がある中で、自組織の情報セキュリティ問題に対応するための CSIRT「組織内 CSIRT」に対象を絞って解説します。
また本書の記述内容は、一般的な企業や組織における CSIRT についての推奨事項であり、ISMS のような標準規格を示すものではありません。セキュリティ上守るべき対象やポリシーは組織によって異なり、CSIRT の実装も組織によって異なります。CSIRT に「規格」はないのです。
本書が、読者の皆さまの組織にとってふさわしい CSIRT を構築するにあたっての第一歩としてお役に立てば幸いです。

一般社団法人 JPCERT コーディネーションセンター

JPCERT CC®

目次

1. CSIRT とは？

CSIRT（シーサート）とは、「Computer Security Incident Response Team ＝ コンピューターセキュリティインシデントに対応するチーム」の略です。そこで、まず「コンピューターセキュリティインシデント（以下「インシデント」）とは何かを説明します。

1.1 インシデントと CSIRT

「インシデント（incident）」とは、一般的に「重大な事故に至る可能性がある出来事」を意味し、「アクシデント（accident: 偶発事故）」や「ハプニング（happening: 出来事）」とは区別されます。情報セキュリティにおけるインシデントとは、情報の機密性、完全性、可用性を脅かす事象であり、その結果として事業運営を危うくする可能性のあるものです。コンピューターウイルスへの感染やサービス運用妨害攻撃、その結果生じる情報漏えいやシステム停止など、IT システムの正常な運用または利用を阻害する（実害のある）一連の事象だけでなく、そのような事象に繋がる可能性のある（まだ実害のない）弱点探索（スキャン）なども広義のインシデントとして含む場合もあります。

なお、インシデントの分類の一つとして「不正アクセス」という言葉が用いられることがありますが、これは厳密には正確ではありません。国や文化によって法的あるいは倫理的に不正とされるものが異なる（日本国内の例でいえば、「不正アクセス行為の禁止等に関する法律」によって「不正アクセス」が主に実害のあるものに限定された内容で定義されている）ことや、システムの仕様によって不正とするものが異なることなどから、何をもって「不正」と定義されるのかが曖昧であるため、発生したインシデントの様態をあらわす言葉として使用する場合は注意が必要です。

［表 1.1-1 インシデントの例］

- スキャンなどの不審なアクセス（Scan）
- 送信ヘッダを詐称した電子メールの配送（Forged）
- システムへの侵入（Intrusion）
- フィッシング詐欺（Phishing）
- 分散型サービス運用妨害（DDoS）
- コンピュータウィルスの感染（Virus）
- 迷惑メール（Spam）
- 先進的で執拗な脅威（APT）

このように定義されるインシデントに対して CSIRT が行うのが「インシデント対応」です。

具体的には、(1) インシデントを検知する、あるいはその報告を受けることによりその発生を認知し、影響の拡大を防ぐとともに、(2) 情報を収集して分析を加え、インシデントの全体像や原因について把握し、(3) 復旧措置や再発防止のための措置を取るまでの一連の活動を指します。

このようなインシデント対応において、まず意識すべき点は、インシデントの発生を完全に回避する予防策はないということです。
かつての情報セキュリティ対策は、ウイルス対策ソフトやファイアウォールの導入といった、インシデントの発生を未然に防ぐことに主眼が置かれていました。もちろんセキュリティ対策として、このような事前の対策が重要なのは言うまでもなく、適切な事前対策によってインシデントの発生確率を減らすことは可能です。しかし、実際に発生したインシデントの原因を分析すると、次のようなものが少なくありません。

（1）人為的ミス

パッチの適用忘れ、システムやソフトウェアの設定の誤り、システム運用やデータの取扱いにおける人為的ミスがインシデントに繋がることは珍しくありません。人間のやることである以上、このようなミスを完全になくすことはできません。

（2）対策のない脆弱性の悪用

発見された脆弱性のすべてに対してパッチが提供されるとは限りません。何らかの理由により製品開発者が速やかにパッチを提供しないケースや、発見された脆弱性情報を製品開発者が知るより前に、悪意のある者の間で秘密裏に脆弱性情報が流通するケースもあります。そのような回避策のない脆弱性が悪用された場合、防御することが難しく、深刻なインシデントの発生に繋がる可能性があります。

（3）技術的な対応の限界

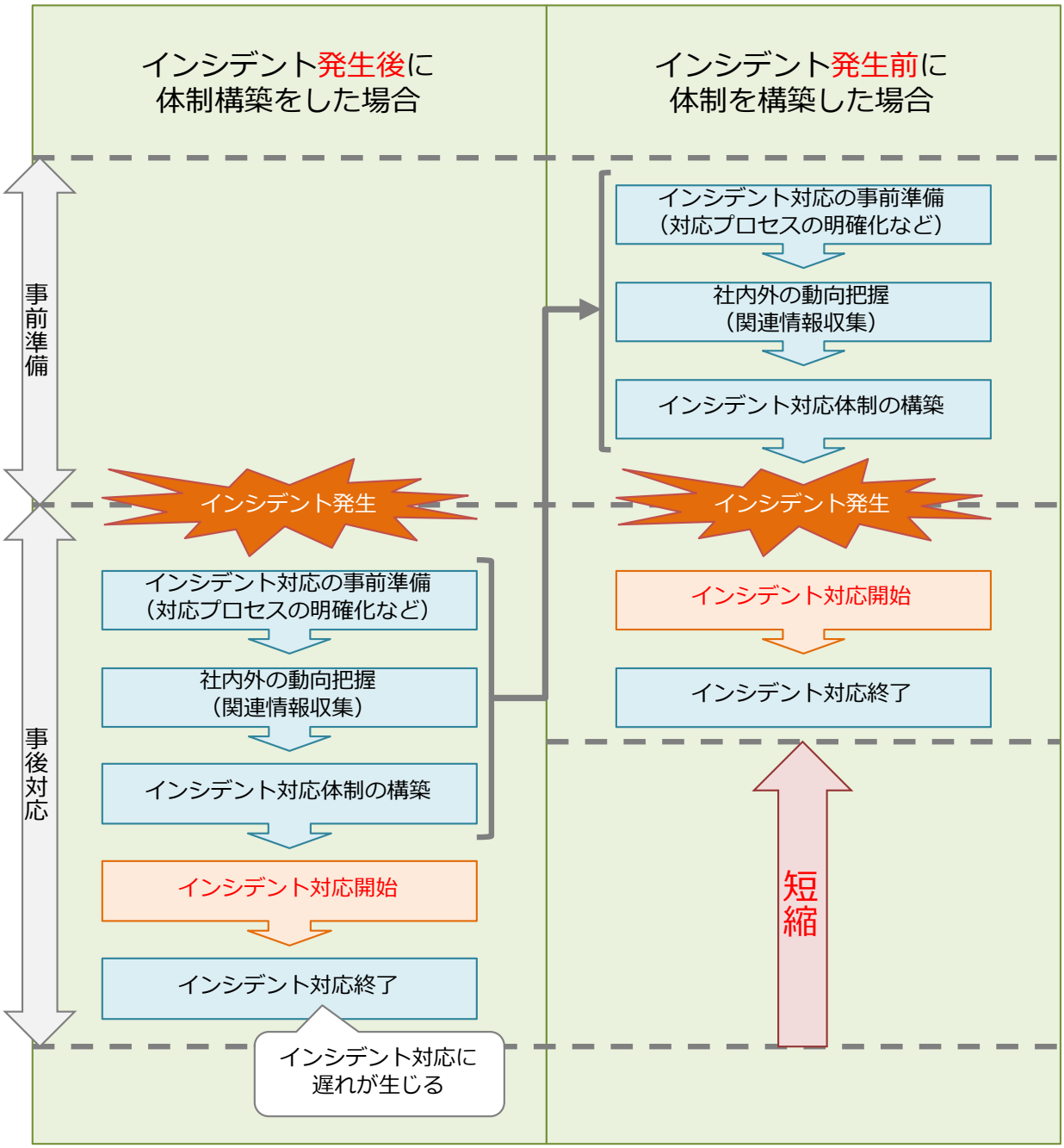
システムの仕様上、特定のインシデントの発生を防ぐ機能がない、すなわち根本的にシステムを入れ替えない限り、対応が不可能な場合もあります。例えば、危殆化した暗号アルゴリズムを使用する製品や、サポートが終了しアップデートが提供されない製品などを入れ替えずそのまま使用し続けることは、インシデント発生のリスクを高めることになります。

（4）セキュリティポリシーに定義されず個人の解釈に依存する事項の存在

セキュリティに関わる事項は複雑多岐に渡るため、すべてをセキュリティポリシーに定めることは事実上不可能であり、個人の解釈や理解によって左右される曖昧な事項がどうしても残ってしまいます。そのような曖昧さのために適切な対応がとられず、その結果期待されるセキュリティレベルを維持できない可能性があります。

これらの原因からわかるように、どんなにインシデントの未然防止策を講じたとしても、インシデントを発生させる余地を残してしまいます。

そこで、適切なインシデント対応として求められるのは、まずインシデントの発生を完全に防ぐことは不可能であるという「事故前提」の意識の下、インシデント発生時に「いかにして被害を最小限に食い止めるか」、そして発生後「いかにして速やかに復旧するか」といった点です。そのためには、インシデントが発生する前にあらかじめインシデント対応のための体制を構築しておくことが推奨されます。

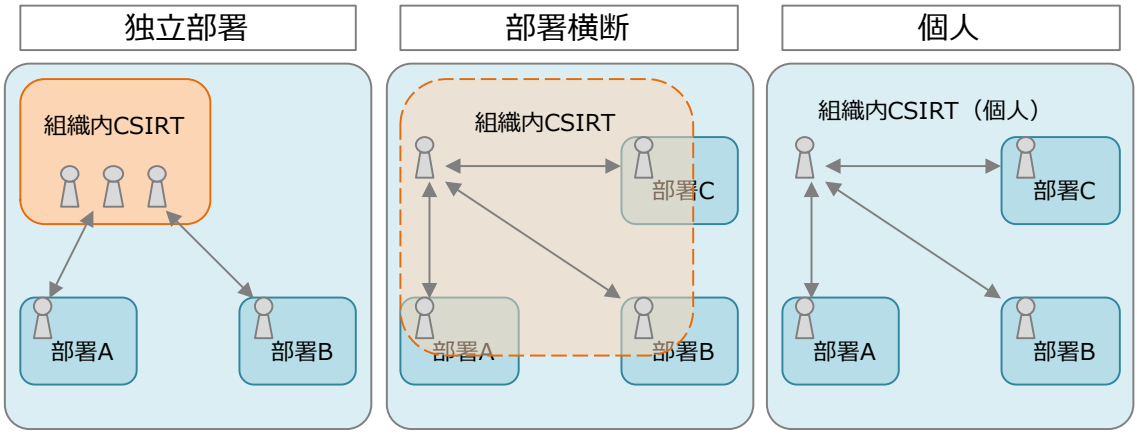


［図 1.1-1 あらかじめインシデント対応体制を構築しておけば対応が速やか］

また、組織をとりまく環境の変化にも注目しなければなりません。そもそもインシデントは災害や犯罪に比べて原因が分かりづらいものですが、組織の活動の IT への依存度が高まるにつれて IT システムが複雑化することで、インシデントの発見や原因の特定が一層困難になり、復旧に時間がかかるようになってきています。さらに、攻撃の潜在化や攻撃手法の高度化、またソフトウェアの未知の（＝回避策が困難な）脆弱性を悪用したゼロデイ攻撃、標的とした組織に対し執拗かつ長期的に活動を行う高度サイバー攻撃（APT）の増加によって、インシデント対応には、技術的に高い専門性が求められるだけでなく、業務に対する幅広い知識も必要になり、そのため情報システム部などのシステム管理を行う部署だけでは対応が難しい場合が増えてきています。

このような背景から「組織的なインシデント対応」が必要となってきており、それを実現するための実装が CSIRT です。

CSIRT は Computer Security Incident Response Team の略であることから、どうしても「チーム = 専門部署」のイメージを持たれがちですが、CSIRT は必ずしも「インシデント対応を専門に行う部署」である必要はありません。必要なのは「インシデント対応を専門に行う機能」としての CSIRT であり、組織によっては他の関連業務と兼務したメンバーによる、部署を横断した形態で CSIRT の機能を実装している例は少なくありません。そこで CSIRT ではなく、CSIRC （シーサーク: Computer Security Incident Response Capability = コンピューターセキュリティインシデントに対応する機能、能力） という表現が使われることもあります。



［図 1.1-2 CSIRT の実装はさまざま（独立部署、部署横断、個人）］

1.2 サービス対象 と CSIRT

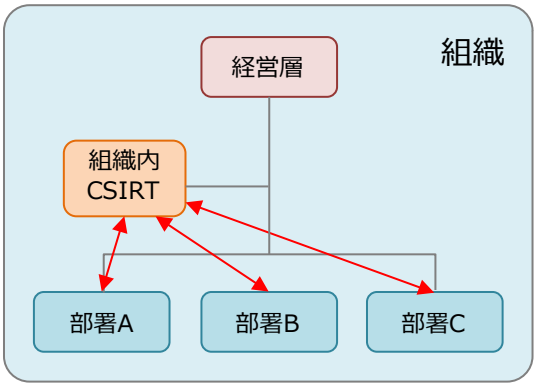
CSIRT にとって重要なのは、まず「どこで発生したインシデント」に対応するのか、つまり CSIRT のサービスが提供される対象（活動範囲）がどこであるかを明確に定義することです。英語ではそれを「Constituency」といいますが、本文書では「サービス対象」と呼びます。
CSIRT の機能は、サービス対象によって次のように分類されます。

組織内 CSIRT
国際連携 CSIRT
コーディネーションセンター
分析センター
ベンダーチーム
インシデントレスポンスプロバイダー

この分類方法は一例に過ぎず、他にもさまざまな視点で分類されることがあります。

（1）組織内 CSIRT

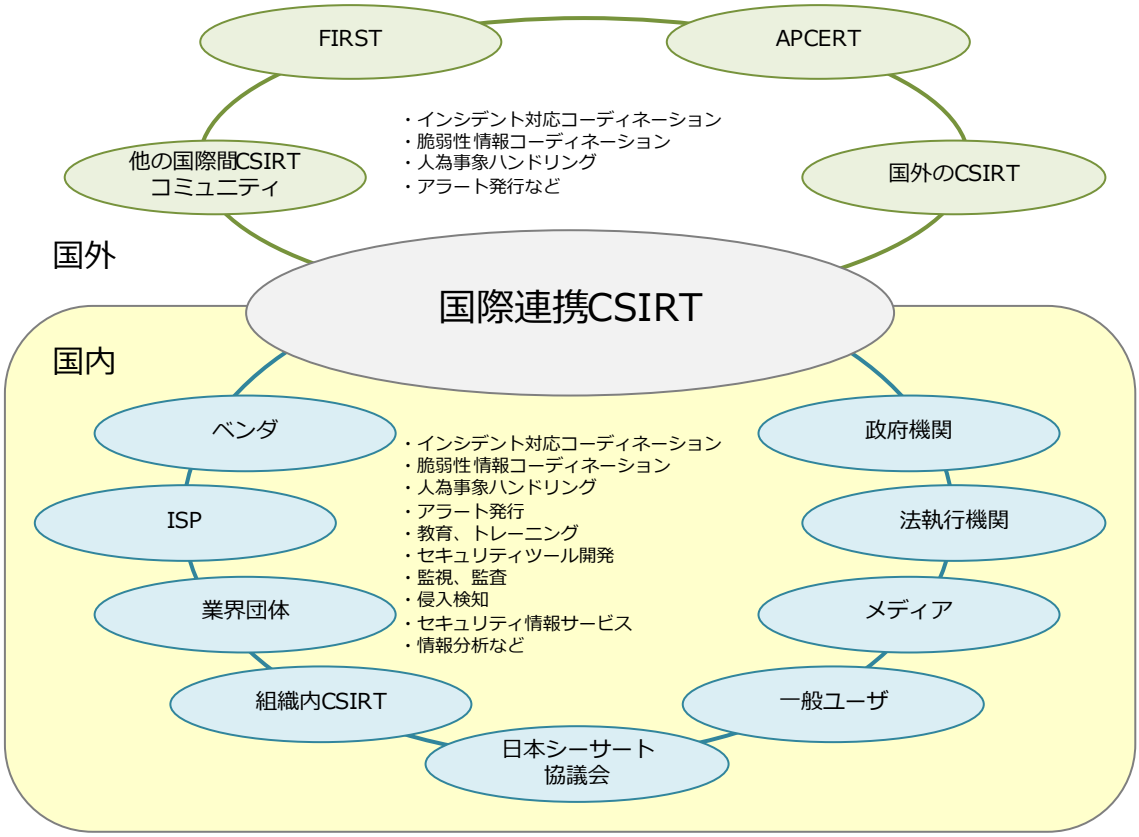
サービス対象は、CSIRT が属する組織の従業員、システム、ネットワークなど。組織にかかわるインシデントに対応する。企業内 CSIRT。



［図 1.2-1 組織内 CSIRT のサービスモデル］

（2）国際連携 CSIRT

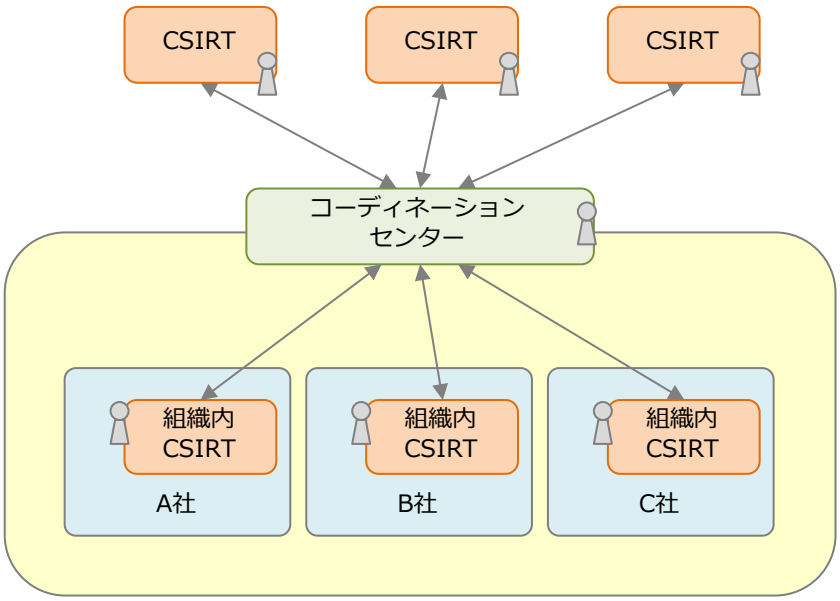
サービス対象は、その CSIRT が置かれる国や地域。このようなサービス対象をもつ CSIRT は、国や地域を代表して、他の国や地域とのインシデント対応のための連絡窓口として活動する。



［図 1.2-2 国際連携 CSIRT のサービスモデル］

（3）コーディネーションセンター

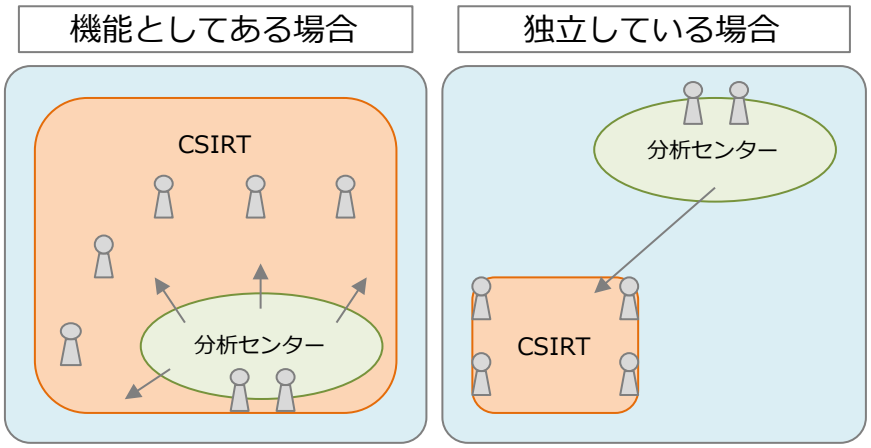
サービス対象は、協力関係にある他の CSIRT。インシデント対応において CSIRT 間の情報連携、調整を行う。企業グループを統括する CSIRT では、企業グループ間のコーディネーションセンターとして各グループ企業の CSIRT との連携や調整機能を担うことも多い。



［図 1.2-3 コーディネーションセンターのサービスモデル］

（4）分析センター

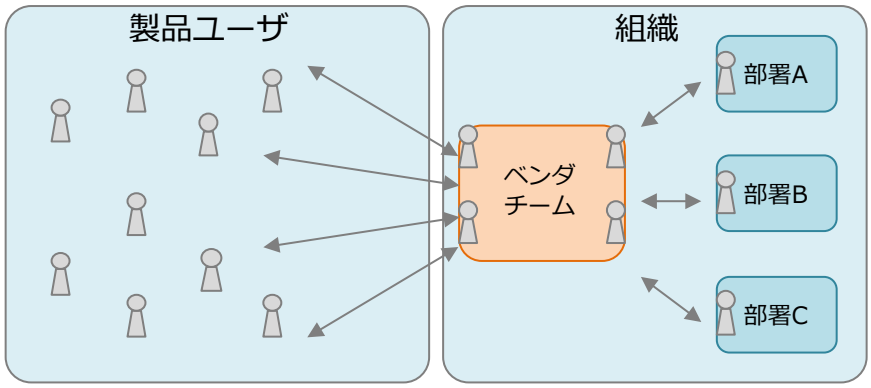
サービス対象は、その CSIRT が属する組織または国や地域。インシデントの傾向分析やマルウェアの解析、侵入等の攻撃活動の痕跡の分析を行い、必要に応じて注意喚起を行う。独立した組織の場合もあるが、CSIRT の中の機能として設けられる場合も多い。



［図 1.2-4 分析センターのサービスモデル］

（5）ベンダーチーム

サービス対象は自組織および自社製品の利用者。自社が開発・提供する製品の脆弱性に対応し、社内の関係部門と連携してパッチの作成やアップデートの提供を行い、製品利用者への情報提供と注意喚起を行う。PSIRT（Product Security Incident Response Team）とも呼ばれる。ベンダー企業によっては、組織内 CSIRT の中にこの機能を持たせるケースもあれば、組織内 CSIRT から独立して PSIRT を設置するケースもある。



［図 1.2-5 ベンダーチームのサービスモデル］

コラム：PSIRT について

PSIRT（Product Security Incident Response Team）は、自組織が開発・提供する製品やサービス等のセキュリティ問題に対処するチームです。
自組織が提供する製品やサービスに内在する脆弱性や欠陥により生じるセキュリティリスクに対処することを目的としています。組織内 CSIRT との明確な違いは、PSIRT はその活動を、自組織が提供する製品やサービスにフォーカスするという点です。すなわち、組織内 CSIRT が主として組織内の従業員や情報システムにおけるセキュリティリスクに対処するのに対し、PSIRT は自組織が提供する製品やサービスを利用するユーザーや顧客のセキュリティリスクを低減することを活動のスコープに含みます。組織内 CSIRT の中の機能の一つとして PSIRT 機能を実装する場合もありますが、活動の性質が異なるため CSIRT とは独立して PSIRT を設ける組織も多く見られます。

PSIRT の活動の全体像について、CSIRT の国際的な団体である FIRST（Forum of Incident Response and Security Teams）は、PSIRT の設置と運用、必要な能力に関するガイド「PSIRT Services Framework」を作成し公開しています。

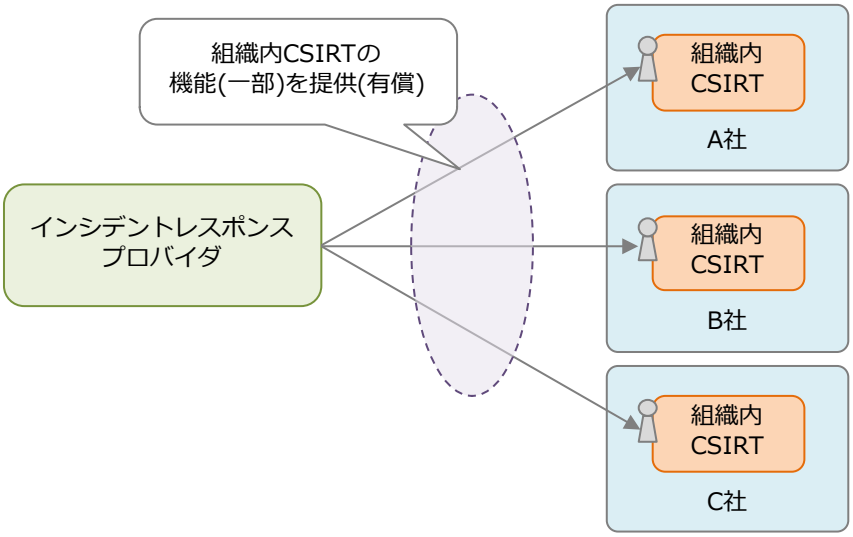
FIRST：「Education Program: Services Framework」
https://www.first.org/education/service-framework

またわが国においては、経済産業省告示にもとづく脆弱性情報流通の枠組み「情報セキュリティ早期警戒パートナーシップ」が運用されており、製品開発者や Web サイト運営者を対象とした脆弱性関連情報の提供と対応支援の枠組みとして利用されています。PSIRT は自組織の製品やサービスに関する脆弱性情報を入手し対処するために、これらの取り組みに参加し活用することが推奨されます。

JPCERT/CC：「脆弱性情報ハンドリングとは」
https://www.jpcert.or.jp/vh/

（6）インシデントレスポンスプロバイダー

サービス対象は、サービス提供契約を結んでいる顧客。組織内 CSIRT の機能またはその一部を有償で請け負うサービスプロバイダー。セキュリティベンダー、SOC 事業者など。



［図 1.2-6 インシデントレスポンスプロバイダーのサービスモデル］

なお、本書はこれらの分類のうち「組織内 CSIRT」に対象を絞っています。

CSIRT の中には、1 つの CSIRT がこれらの分類された機能を複数有することもあります。以下の表 1-2-1 は、JPCERT/CC および国内のいくつかの CSIRT で見られる機能の例です。

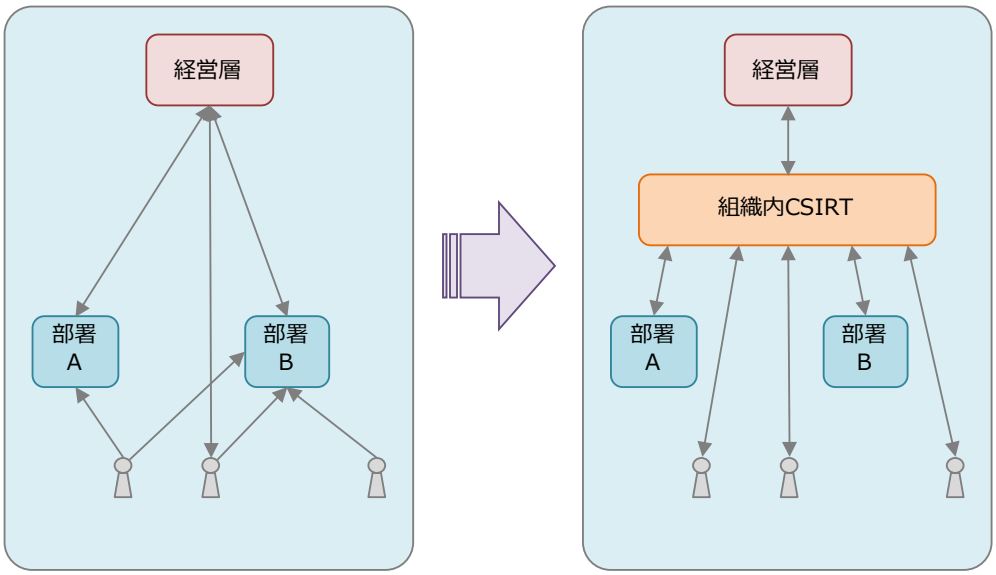
［表 1.2-1 既存 CSIRT の例］

	JPCERT/CC	A 社 CSIRT	B 社 CSIRT	C 社 CSIRT	D 社 CSIRT
組織内 CSIRT		○	○	○	○
国際連携 CSIRT	○				
コーディネーション センター	○	○			○
分析センター	○	○		○	
ベンダーチーム					○
インシデントレスポンス プロバイダー				○	

2. CSIRT の必要性

CSIRT を構築することで得られる「メリット」には次のようなものがあります。

（1）情報セキュリティインシデントに関する情報の一元管理

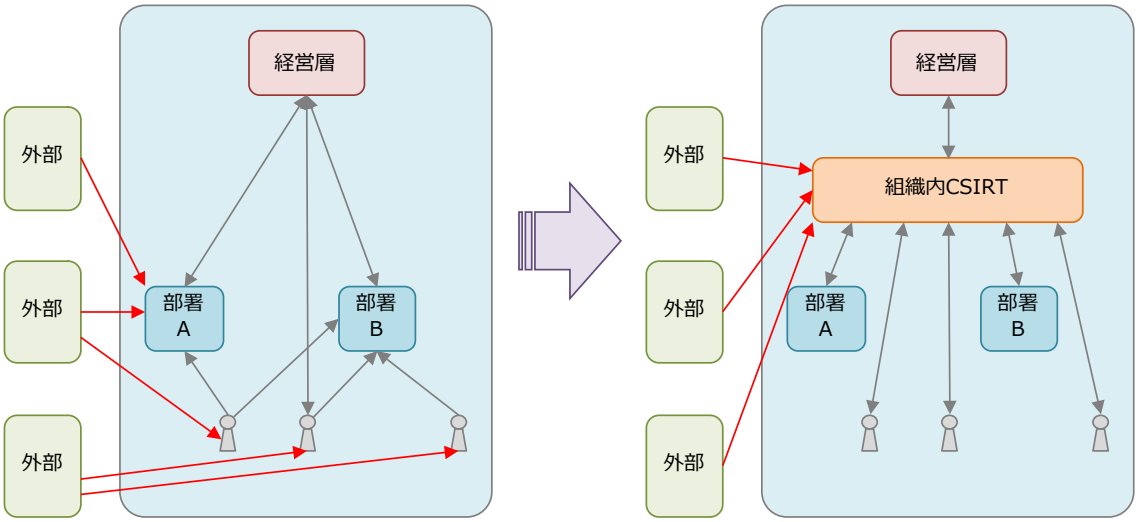


［図 2-1 組織内 CSIRT のメリットのイメージ 1］

CSIRT が存在しない場合、組織内で発生したインシデントなどの情報セキュリティに関する情報が各部署からばらばらとまとまりのない形で経営層に伝達されるため、（一般的に専門的知識のない）経営層が状況を整理しなければならなくなります。また、対応に関する指示は経営層から各部署に個別に行わなくてはならなくなります。

CSIRT はそういった組織内のギャップを吸収し、インシデントや情報セキュリティに関する情報の集約と、組織内の関係者に適切に伝達する機能を担い、効果的な対応と対策がなされることを支援するとともに、組織内における情報の不適切な流通を防ぎます。

（2）情報セキュリティインシデントに関する組織内外との統一された窓口

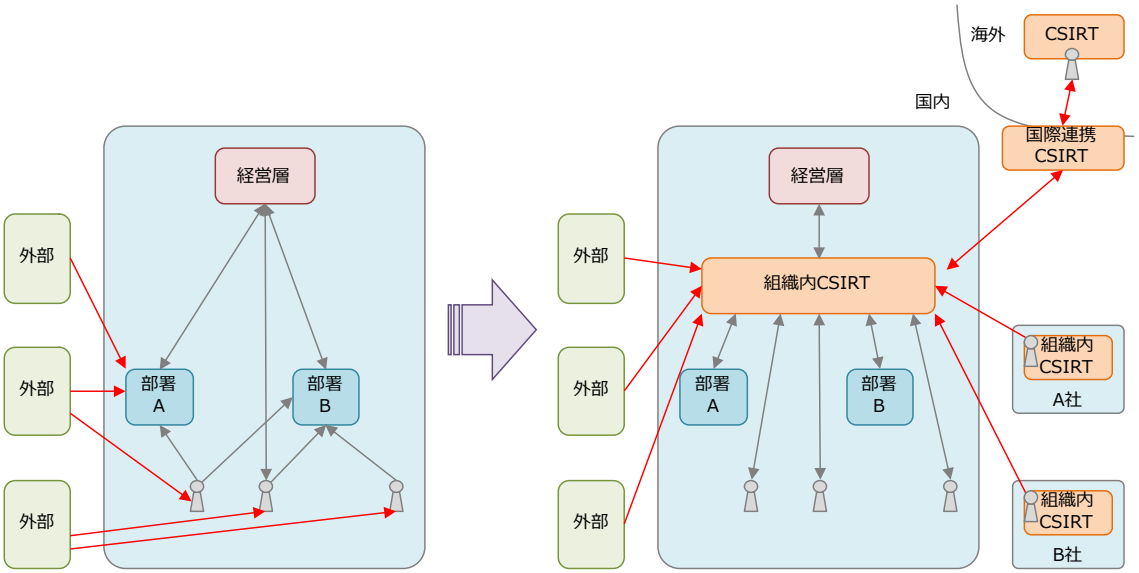


［図 2-2 組織内 CSIRT のメリットのイメージ 2］

CSIRT が存在しない場合、自組織で発生したインシデントに関して外部から問い合わせを受ける窓口が一元化されず、複数の窓口に届けられた個々の情報間の連携、関連付けが難しくなり、結果としてインシデントへの対応が混乱し、遅れる可能性があります。

CSIRT はインシデントの報告や関連する問い合わせについての社内外に向けた窓口として機能することで、情報を集約し、関連付けを行い、効果的な対応に繋げるとともに、社内外に発するメッセージを統一化します。

（3）インシデント対応に関係する外部組織との信頼関係の構築



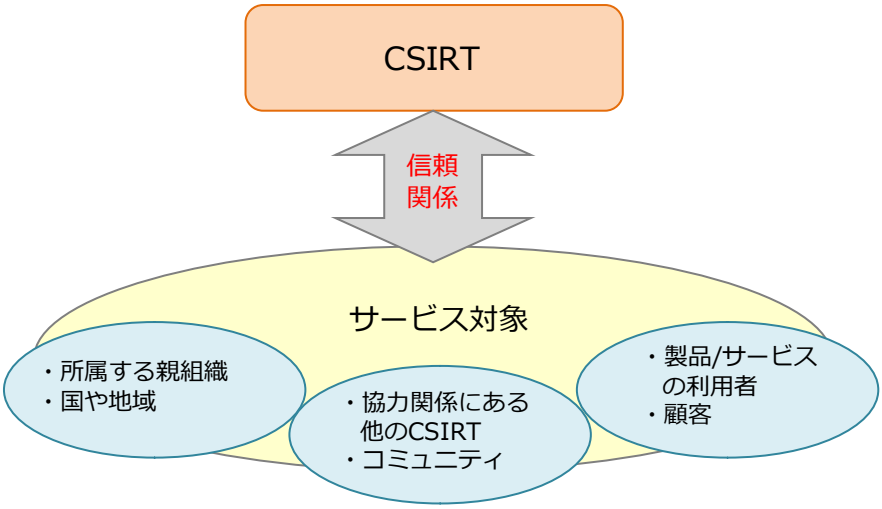
［図 2-3 組織内 CSIRT のメリットのイメージ 3］

インシデントに関する情報を他組織と共有することで自組織のインシデント対応に役立てることができます。しかし組織にとって機微な情報を含む可能性のあるインシデント関連情報を外部に出すことは一般的には難しいことです。したがって、そのような情報を共有する上で最も必要なことは、お互いに関係者以外に情報を漏らさないという「信頼」です。しかし CSIRT が存在しなければ、他組織にとっての情報交換の相手は各部署の担当者となり、さらに案件ごとに異なる部署と情報交換するようなことになれば、提供した情報が果たして相手の組織内で適切に扱われるかどうか確信を持つことができないかもしれません。そのような状況では、一般的に信頼関係の構築は難しくなります。逆に CSIRT があれば、CSIRT が外部に対する「信頼の窓口」として機能することで組織間の信頼関係の構築が容易になります。

3. CSIRT に求められること

3.1 信頼の輪の重要性

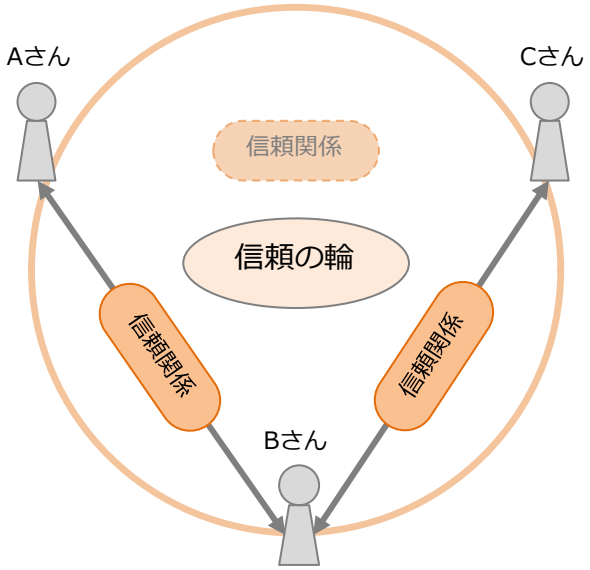
CSIRT にとって最も重要なものはサービス対象との間の「信頼関係」です。これは CSIRT が扱う情報がインシデントそのものに関する情報をはじめ、社内の機密にあたるものが多いからです。機密情報を適切に扱わない「信頼」できない CSIRT にインシデント対応を依頼するサービス対象はいないでしょう。CSIRT が CSIRT たりうる最も重要な要素はサービス対象との信頼関係なのです。



［図 3.1-1 CSIRT は「信頼関係」が命］

また、CSIRT にとって必要とされる信頼関係はサービス対象との信頼関係だけに留まりません。円滑なインシデント対応においては、他の CSIRT など、関連組織との情報連携・情報共有が欠かせません。他の組織との情報共有によって、今どのようなインシデントが世の中で起きているか、その原因や対策、攻撃活動を検知・防御するための手掛り（インディケータ）といったインシデント対応に必要な情報を、常に平常時から把握しておけば、自社で同様のインシデントが発生した際に速やかに対応することができます。また、自社で発生したインシデントに対応するために、他の CSIRT や関連組織と連携し支援を得ることによって、効率的な対応を行い復旧までのコストを軽減することができるのです。

しかしインシデントに関する情報は多くの場合、機密にあたります。そのため、インシデント関連情報を他者と共有するためには、関係者以外に情報を漏らさないという信頼がお互いに必要です。そして、このような信頼関係に基づくコミュニティー＝「信頼の輪」を形成することによって共有できる情報の幅が広がり、結果として CSIRT の活動に大きな効果を生むのです。



［図 3.1-2 信頼の輪］

A と B の間に信頼関係があり、かつB と C の間に信頼関係がある場合、A と C の間に直接の面識がなくても、A と C の間に信頼関係を成り立たせることができる。

また、「信頼の輪」は CSIRT 同士のコミュニティーにとどまりません。

インシデント対応においては、必要に応じて事実を公表しなければならないことがあります。例えば、情報漏えい事故により顧客の個人情報が漏えいした場合、その事実を Web や電子メールを通じて当該顧客に告知するだけでなく、被害の程度や社会的な影響が大きい場合は、プレスリリースや記者会見などを通じた公表が必要となる場合があります。
このようなインシデントに絡む公表に際しては、もし対応を誤れば、組織の大幅なイメージダウンに繋がりかねないだけに、慎重に行う必要があります。そのために、事実が歪曲されて伝えられることがないよう普段からメディアとの信頼関係を構築しておくことが推奨されます。一般に、CSIRT の活動にはメディアに対する適切な対応を支援する広報部門の関与が欠かせません。

3.2 信頼の輪の作り方

サービス対象からの信頼を得るためには、まず CSIRT の存在をサービス対象に認知してもらうことが重要です。
具体的には、サービス対象が閲覧できる（社内）Web サイトを設置して、CSIRT の活動内容や問い合せ先といった情報を掲載します。

また普段からサービス対象との情報共有を密に行います。
CSIRT は常に、特にサービス対象で発生する可能性があるインシデントおよび関連する技術情報を収集し、それが社内システムにかかわる場合は担当部署に対して情報を提供します。また一般社員にも必要

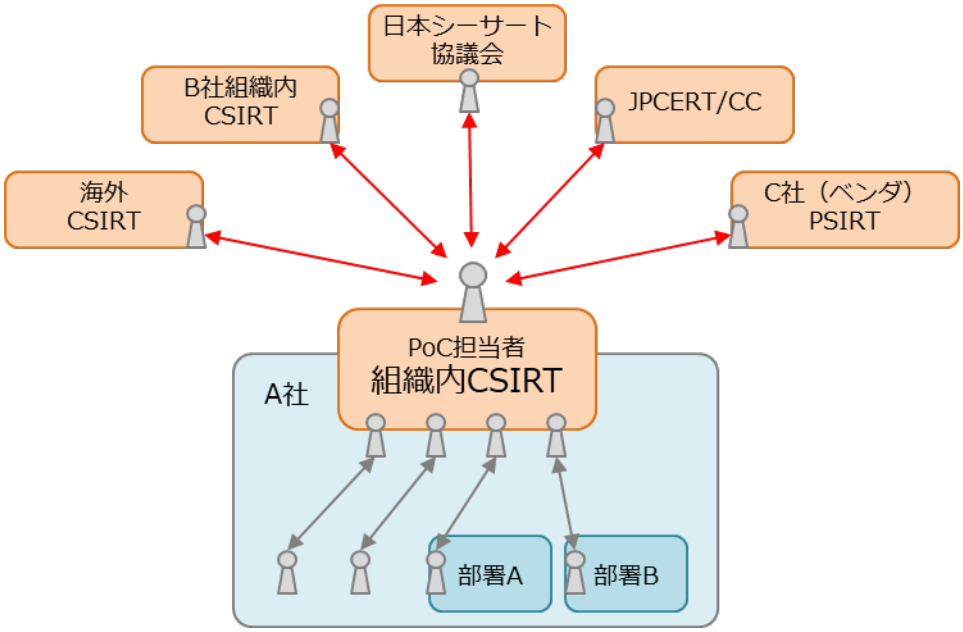
とされる情報であれば、社員向けに注意喚起を行います。さらに社員向けのセミナーやミーティング、インシデント対応演習などを定期的に実施し、CSIRT の活動を普段から社員に示すことで信頼を得ることができます。

他にも、サービス対象からのものに限らず CSIRT に何らかの問い合わせや要求が来た場合には、たとえそれが CSIRT の対応すべきインシデントや関連事項でなくても、無視することなく必ず何らかの形で応答を返すことも、CSIRT への信頼を得るために必要なことです。問い合わせや要求の内容が CSIRT に対応できないものであれば、その旨の理由を添えて回答します。

外部の CSIRT とのコミュニティーの形成や既存の CSIRT コミュニティーへの参加にあたっては、留意すべき事項があります。
CSIRT の日常的な活動はインターネットを介した情報収集など、「顔が見えない」形でのコミュニケーションが中心になります。そのため、コミュニティーも「顔が見えない」メーリングリスト等によるコミュニケーションだけで済んでしまうのではないかと思われがちですが、それでは信頼関係は成立しません。

CSIRT の情報共有に必要なのは「信頼関係」です。この信頼関係は「顔が見えない」形でのコミュニケーションでは形成できません。直接、対面での意見交換などを通じて、どの CSIRT にどのようなメンバーがいて、どのような活動をしているのか、またどのように情報が取り扱われているのかといったことを互いに共有し理解することが求められます。日本シーサート協議会やその他の多くの CSIRT コミュニティーの会合では他組織の CSIRT と直接意見交換する機会が得られるので、相互理解を深める場として積極的に利用するのがよいでしょう。またそれぞれの組織が地理的に遠距離にある場合や、在宅勤務等の事情により、直接対面の機会を作りにくいケースが今後増えていくことを考えれば、オンライン会議ツール等の活用など必ずしも直接対面を必要としない手段でのコミュニティー形成が進んでいくものと思われます。

特に密な情報共有を望む CSIRT に対してはメンバー全員と互いに顔見知りになっておく場合もあります。しかし現実にはすべての CSIRT のメンバー全員と顔見知りになるのは難しく、メンバーの担当任務の内容によっては外部に顔を知られては困る場合もあるかもしれません。また複数のメンバーが別個に対外的な活動をすることで、CSIRT として意思統一された対外的コミュニケーションが難しくなる場合もあるかもしれません。
そこで通常は、CSIRT は PoC（Point of Contact）と呼ばれる「代表者」を用意して、その PoC が CSIRT の「顔」として他の CSIRT との信頼関係を構築したり、コミュニティーとの情報共有の窓口としての役目を果たしたりします。
また、PoC には、あらかじめ CSIRT 間で取り決めたフローでは対応できないような想定外の事態が発生した場合の「柔軟性のある」連絡窓口としての役目もあります。



［図 3.2-1 組織内の CSIRT］

PoC は、CSIRT の顔としてコミュニティーとの信頼関係を構築するために、国際会議や意見交換会などの、コミュニティーのメンバーが集う場に継続的に参加し、積極的に交流を深め、「顔の見える」信頼関係を構築および維持するよう努める必要があります。

PoC は CSIRT を代表する立場であることから、CIO や CISO が兼務する場合もありますが、必ずしも組織の上級管理職クラスを充てる必要はありません。実務レベルにおいて、責任を持って情報をコミュニティーに提供できる権限と、コミュニティーから得られた情報を CSIRT 内で展開できる権限を有する必要があります。
また PoC に求められるものとしては、高いコミュニケーション能力と、コミュニティーで得られた情報を的確に判断して処理する能力、そして CSIRT の「顔」としての役目を果たせるだけの充分な知識と、セキュリティを扱う者としての高い倫理観などが挙げられます。

注意しなければならないのは、PoC はそれぞれの組織の CSIRT を代表する立場ではあるものの、ここで述べている信頼関係は、その PoC 担当者が所属する組織の信頼によるものよりも、PoC 担当者個人の信頼に根差す割合が大きいということです。もし PoC 担当者が何らかの理由で不在となったり、交替することとなった場合、一時的にでも信頼関係が損なわれることを避ける必要があります。後任者への適切な引継ぎは勿論のこと、普段から可能な限り複数の CSIRT メンバーが他組織との関係を持ち、信頼関係を持つ者を増やしておくことで、信頼関係が断絶するリスクを下げるとともに、その CSIRT 自体の信頼度を高めることに繋がります。

コミュニティーとの情報共有には、さまざまな方法が使われます。日常的な情報のやり取りにはメンバーを限定したメーリングリスト等が用いられます。必要に応じて暗号化機能を持ったメーリングリストを用いることもあります。暗号化の手法としては、PGP や S/MIME が代表的ですが、国際的な CSIRT の

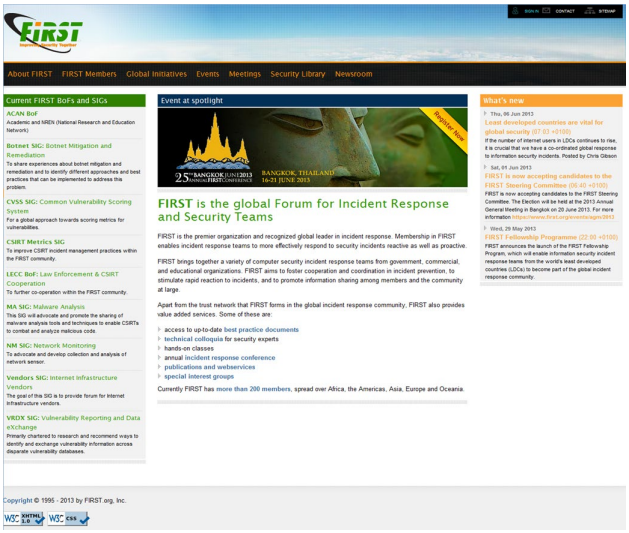
コミュニティーでは PGP が使われることが多いです。他にも Web 上に限られたメンバーのみが閲覧可能なポータルサイトを設置して CSIRT 間のコミュニケーションに使用する場合もあります。

3.3 CSIRT のコミュニティー

CSIRT によるコミュニティーには次のようなものがあります。

（1）FIRST（Forum of Incident Response and Security Teams）

https://www.first.org/



CSIRT による国際フォーラム。FIRST が定めたルールに沿う CSIRT ならどのような CSIRT でも参加可能。

（2）APCERT（Asia Pacific Computer Emergency Response Team）

https://www.apcert.org/

アジア太平洋地域の National CSIRT によるフォーラム。APCERT が定めたルールに沿う CSIRT のみ参加可能。

(3) 日本シーサート協議会（日本コンピュータセキュリティインシデント対応チーム協議会、Nippon CSIRT Association）

https://www.nca.gr.jp/

日本国内の CSIRT によるフォーラム。日本シーサート協議会の使命および活動内容に賛同し、かつ協議会から得られた情報を適切に取り扱うことができる日本国内で活動する CSIRT であれば参加可能。

上記の 3 つのコミュニティーはいずれも新規参加にあたっては既存メンバーによる推薦を必要としています。これは文字通り「信頼の輪（Web of Trust）」の考えに基づくものです。

また、FIRST では各参加 CSIRT に必ず 1 名の Rep（Representative、代表者）の存在を義務付けています。これは PoC と同義で、各 CSIRT を代表して、コミュニティーや FIRST の事務局との連絡窓口の役目を果たします。

4. CSIRT の位置づけ

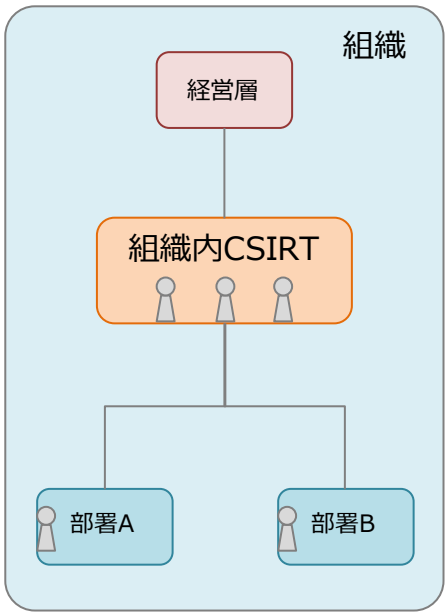
CSIRT は、組織によってサービス内容が異なるだけでなく、そのサービス内容によって実装も大きく異なります。

専任のメンバーで構成されるチーム（=部署）として実装される場合もありますが、他業務と兼務する複数部署のメンバーによる仮想的なチームとして CSIRT 機能を実装する場合もあります。チームとして複数のメンバーで構成されることもあれば、規模の小さな組織では一人の担当者がその組織の CSIRT 機能を担う場合もあります。

ここでは、CSIRT（およびその機能）を組織としてどのような位置づけにすべきか、いくつか例を挙げて紹介します。

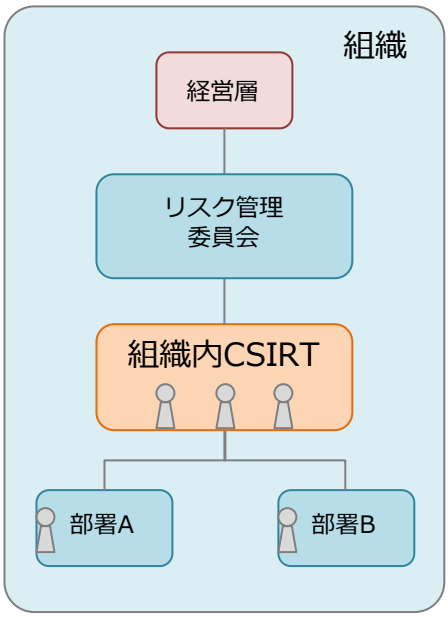
（1）経営層直下にある場合

経営層から委譲された権限の下、各部署と連携します。



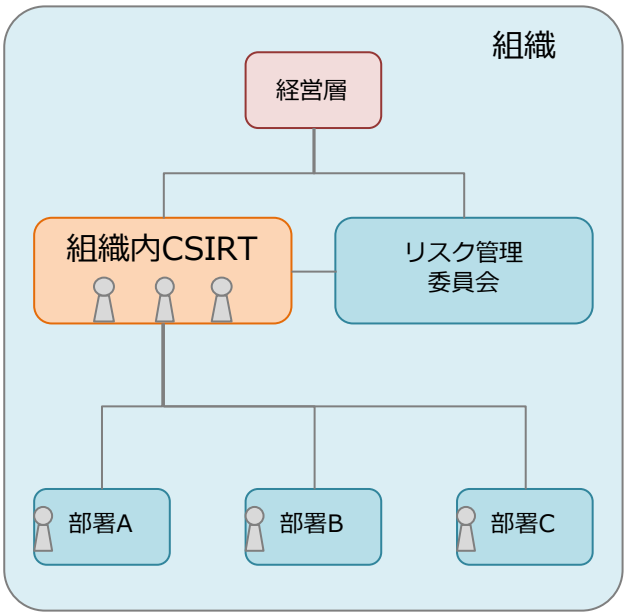
（2）経営層直下にあるリスク管理委員会の下にある場合

リスク管理委員会から委譲された権限の下、各部署と連携します。



（3）経営層直下にあり、リスク管理委員会と並立している場合

経営層から委譲された権限の下、各部署およびリスク管理委員会と連携します。



5. CSIRT にあらかじめ必要なこと

ここでは、CSIRT を構築するにあたって、あらかじめ決めておかなければならないこと、やらなければならないことを紹介します。

5.1 サービス対象の明確化

1.2 で説明したように、CSIRT にとって重要なのは、まず「誰のインシデント」に対応するのか、つまり CSIRT にとってのサービス対象者 （活動範囲） が誰であるかということを明確に定義することです。

5.2 活動目的の明確化

CSIRT の活動目的を明確にしておく必要があります。被害の局限化・最小化、被害からの迅速な復旧など、いくつかの目的が考えられますが、それらのうち、どの目的を最優先するかといった優先順位付けをしておきます。これによって、あらかじめ対応マニュアルを用意していない「予期せぬインシデント」に遭遇したときも速やかに対応できるようになります。

また CSIRT の活動目的を明確にすることで、その CSIRT が提供すべきサービス内容や CSIRT の具体的な実装も変わってきます。

CSIRT の活動目的の例：

> 会社内および子会社の従業員に対して、コンピューターセキュリティインシデントによる被害を軽減および局限化するための環境およびシステムの構築を支援する。
> 会社内および子会社の従業員に対して、コンピューターセキュリティインシデントが発生した場合の対応を支援する。
> インターネット接続サービスを契約している顧客が、そのインターネット接続サービスを起因とするコンピューターセキュリティインシデントに巻き込まれた場合、その被害を軽減し、迅速に復旧する。
> ○○グループ内で発生したコンピューターセキュリティインシデントの検知、解決、被害の軽減・局限化および発生の予防を支援することにより、○○グループのセキュリティの向上に貢献する。

5.3 サービス内容の定義

CSIRT は、サービス対象に対して提供するサービス （活動内容） を定義し、サービス対象にあらかじめ告知しておく必要があります。提供するサービスは、サービス対象のニーズに応じて変わります。

CSIRT のサービス内容を定義する際にありがちな誤解として、CSIRT は経営層による社員の監視といったガバナンス（統制）のための機能であるというものがあります。しかし、CSIRT はあくまでサービス対象に関係するインシデントに対して「中立な立場で」対応するためのものです。
CSIRT のサービスを定義する際には、サービス対象に対するヒアリングや過去に実際に発生したインシデントや今後想定されるインシデントを可能な限り詳細に分析しておく必要があります。また技術の進歩、取り巻く環境や状況の変化に応じて、適宜サービス内容を見直し、再定義することも重要です。

［表 5.3-1 サービスリストの例］

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
・アラートと警告 ・インシデントハンドリング - インシデント分析 - オンサイトでのインシデント対応 - インシデント対応支援 - インシデント対応調整 ・脆弱性ハンドリング - 脆弱性分析 - 脆弱性対応 - 脆弱性対応調整 ・アーティファクトハンドリング - アーティファクト分析 - アーティファクト対応 - アーティファクト対応調整	・告知 ・技術動向監視 ・セキュリティ監査または審査 ・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 ・セキュリティツールの開発 ・侵入検知サービス ・セキュリティ関連情報の提供	・リスク分析 ・ビジネス継続性と障害回復計画 ・セキュリティコンサルティング ・意識向上 ・教育 / トレーニング ・製品の評価または認定

実際には、CSIRT によってサービスリストの種類およびそれらの定義づけが異なります。

提供するサービスを決める際には、もう 1 つ重要な点があります。
当然のことながら CSIRT のリソースは無限ではありません。したがって、すべてのインシデントに対応できるとは限りませんので、トリアージ（優先順位付け）の基準をあらかじめ定めておく必要があります。そのためには、まず対応すべきインシデントを定義し、分類しておきます。そして、定義し分類されたそれぞれのインシデントごとの対応マニュアルを作成します。なお、対応マニュアルについては、別冊の「インシデントハンドリングマニュアル」を参照してください。

5.4 通信チャネルの設置

対応するインシデントの内容によっては、CSIRT メンバーだけで対応し切れない場合があります。まず当事者であるサービス対象からの情報提供などの協力と連携が重要であることはもちろん、サービス対象でない当該インシデントの当事者との連携が必要なこともあります。例えば、自組織から他組織に対する攻撃、あるいは他組織から自組織に対する攻撃の可能性が指摘された場合、一方の当事者である他組織に事実確認を依頼する必要があります。

そこで、サービス対象および当該インシデント関係者との間の通信チャネルを用意し、その方法を明示しておくことが推奨されます。まず CSIRT の Web サイトの URL、連絡用メールアドレス、電話番号などの通信チャネルに関する情報をサービス対象に確実に告知します。また、サービス対象以外からの連絡 （通報、問い合わせ） が想定される場合は、組織の Web サイトなどに連絡方法を明記します。

6. インシデントハンドリング概論

6.1 インシデントマネジメント、ハンドリング、レスポンス

CSIRT がインシデントに対して行う業務（広義のインシデント対応）は大きく次の 3 つにステージに分類されます。

（1）インシデント発生前

CSIRT が平常時に行う日常業務であり、インシデント発生に備えた準備の活動でもあります。

CSIRT の日常業務としては、一般的にセキュリティ対策と呼ばれることの多い、ウイルス検知ソフトやファイアウォールの導入など、インシデントの未然防止策の実施をイメージすることが多いかもしれません。そういったセキュリティ管理策を社内に適切に導入するための技術的支援を行うことは、CSIRT に期待される業務の一つであることは間違いありません。

しかし CSIRT の日常業務として最も重要なことは、インシデントに関する情報の収集とそれが自組織のシステムに与える影響の分析、そして自組織のリスク許容度を評価することです。日々、大量に提供されるセキュリティ関連情報の中から自組織のシステムに関係するものをピックアップし、現時点で当該システムが晒されている脅威を把握し、必要な対策（パッチの適用、設定変更など）を講じることでインシデントを未然に防ぐことができる可能性が高まります。またインシデントを防ぐことができなくても、被害を最小限に抑えたり、被害から復旧したりする上で必要な情報を蓄積しておくことで、対応を速やかに行えるようになります。

さらに、システム管理者のみならず、一般社員も知っておく必要がある情報があれば、セミナーやミーティングを通じて社員への啓発を行ったり、緊急を要する情報は社内への注意喚起を行ったりします。

また、インシデント発生時に備えて、異常を速やかに検知する仕組み（装置および体制）を導入し、インシデント検知後の対応マニュアルを整備しておくことが重要です。そして、一連の対応手順が有効に機能することを確かめる目的で、演習を定期的に行うことが推奨されます。これは、防災訓練のように実際に作業を行うようなスタイルもあれば、マニュアルどおりに連絡が取れるかといったコミュニケーションチェックのみを行う場合もあります。また、CSIRT メンバーだけで行う演習や、サービス対象者も参加して組織全体の対応を確認する演習など、目的とスコープに応じたさまざまなやり方が考えられます。演習により問題が見つかった場合は、対応マニュアルなど、一連の対応手順を修正します。

（2）インシデント発生時

インシデントが発生したときに、被害を局限化、最小化し、速やかな復旧につなげることを目的とする活動です。
まず大事なのは、インシデントを速やかに検知することです。CSIRT 自らが検知するための仕組み（装置および体制など）が必要であることはもちろん、外部からの通報を受け付ける窓口を設置することも

重要です。インシデントの内容によっては自ら検知することが難しいものもあり、そのようなインシデントは多くの場合、外部からの通報がなければ知ることができません。

また、CSIRT の資源は無限ではありません。同時に複数のインシデントに対応しなければならない場合には、個々のインシデントに対して、あらかじめ決めた基準に従って、トリアージ（優先順位付け）をします。検知されたインシデントが高度サイバー攻撃（APT）である可能性がある場合（多くの場合、高度サイバー攻撃（APT）の可能性の有無は、外部情報や蓄積されたインディケータ情報を用いた専門的な知識にもとづく判断となる）、攻撃によるリスクがどの程度あるかと、自組織がどこまでリスクを許容できるかによって、直ちに脅威を排除するべきか、あるいは侵害された範囲の特定を試みるべきか等について討議し、対応方針を検討しなくてはなりません。

その後、対応マニュアルやチェックリストに従って、必要な関係者への連絡やシステム対応（ネットワークの切断、感染システムの隔離、設定変更など）を実施する、あるいはインシデント範囲の特定をしてから脅威の排除を実施します。

（3）インシデント発生後

インシデントから復旧し、再発を防止することを目的とする活動です。

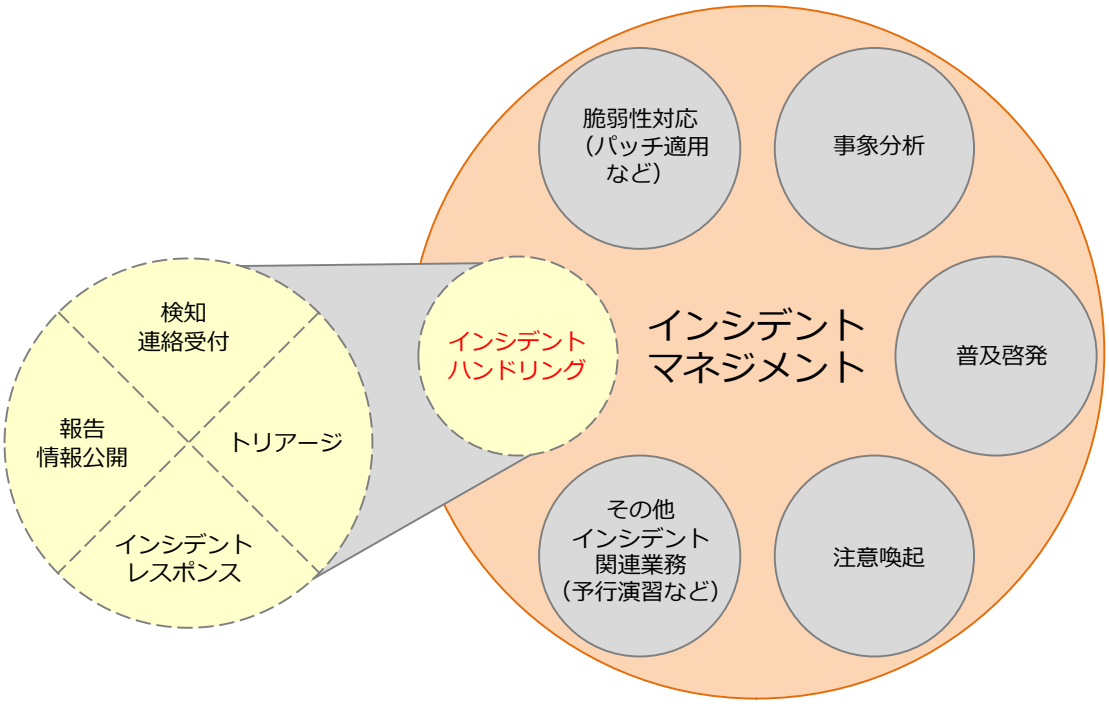
インシデントによる被害から復旧し、システムを元の状態に戻しても、インシデントの原因を取り除かなければ、同じインシデントが再発してしまいます。そこで、まず行わなくてはならないのはインシデントの直接の原因の究明です。インシデントの原因には、パッチの適用忘れや設定間違いといった初歩的なミスから、未知の脆弱性の悪用まで、さまざまなものがあり、場合によっては外部の専門機関に判断を委ねなければならないほど複雑で究明が困難なケースもあります。原因を究明し、その原因を取り除くまでは、元に戻しただけの状態のシステムを運用に移すのは大変危険です。

ここで重要になってくるのは、原因究明に必要な情報収集であり、特に外部の信頼できる組織との情報共有が有効に働く場合があります。

原因を究明し、同じインシデントが発生しない対策（パッチ適用、ファームウェアの更新、設定変更など）を講じた上で、システムを運用に戻します。その後、インシデントの原因となった事象が生じた理由を究明し、同じ事象が生じないようにします。例えばパッチの適用忘れが起こった理由を調べ、既存の運用ポリシーや手順に問題があれば、見直します。

またインシデント対応時に参照したマニュアルや手順書をレビューし、インシデント対応を進める上での問題がなかったかを確認し、必要に応じて修正、改訂します。
このような、インシデントに対して CSIRT が行う一連の業務をまとめて「インシデントマネジメント」と呼びます。また、このうち「(2) インシデント発生時」と「(3) インシデント発生後」のような実際に発生したインシデントに対して行う一連の業務を「インシデントハンドリング」と呼び、特にその中で、

インシデントに実際に対応する業務を「インシデントレスポンス」と呼びます。これらの関係を示したのが次の図です。

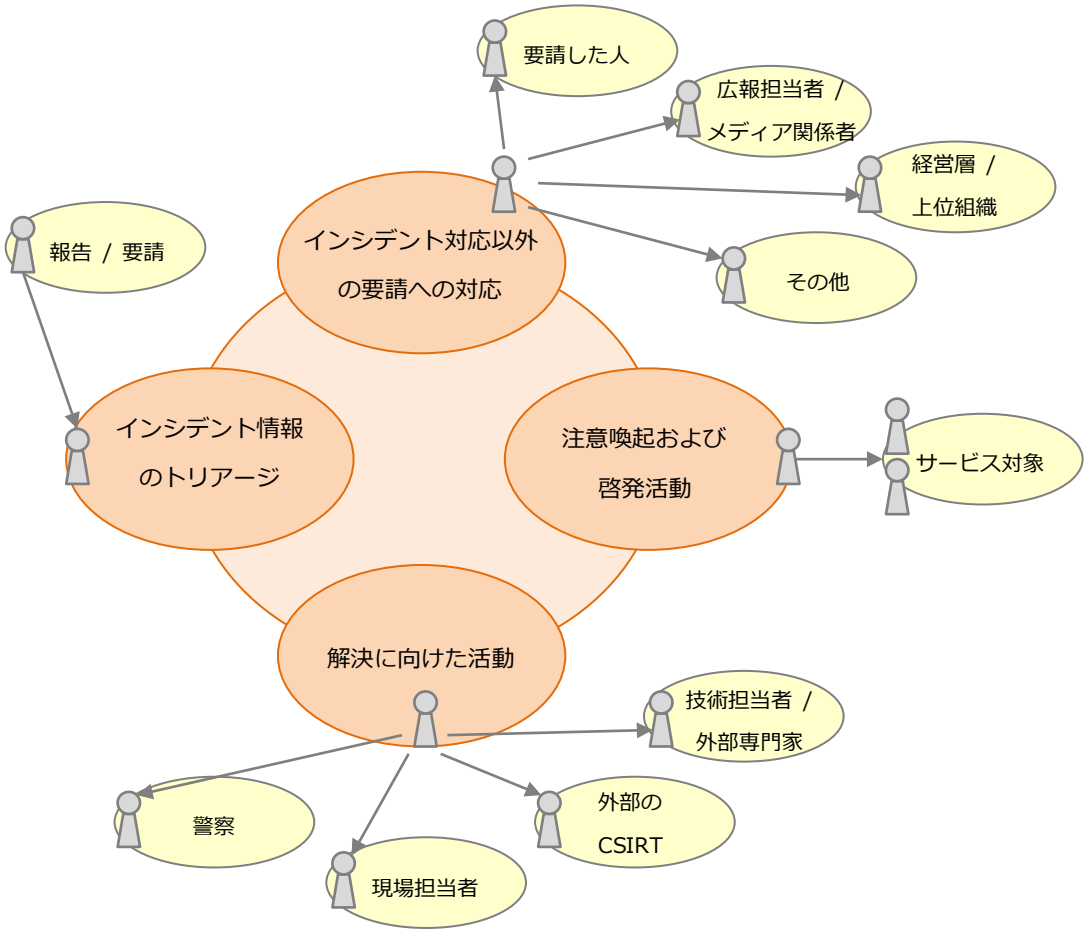


［図 6.1-1　インシデントマネジメント、ハンドリング、レスポンスの関係］

ただし、これらの区別は厳密なものではなく、CSIRT によって異なります。
以降は、これらのうち、実際に発生したインシデントに対して行う「インシデントハンドリング」について解説します。

6.2 インシデントハンドリングの機能

前節では「CSIRT の業務」の視点で説明しましたが、「CSIRT の機能」の視点で見た場合、インシデントハンドリングは「インシデント情報のトリアージ」、「解決に向けた活動」、「注意喚起および啓発活動」、「インシデント対応以外の要請への対応」の 4 つの機能から成り立っています。



［図 6.2-1　4 つの機能の関連］

（1）インシデント情報のトリアージ

CSIRT が対応すべきインシデントに対して一次分析を行い、その内容や深刻度、緊急度などから対応の優先順位付けをします。この順位付けの判断基準はあらかじめ可能な限り詳細に定めておく必要があります。

（2）解決に向けた活動

当該インシデントに関連した Web サイトの運営者や他の CSIRT、必要に応じて専門家などと情報をやり取りし、必要な対応につなげます。

（3） 注意喚起および啓発活動

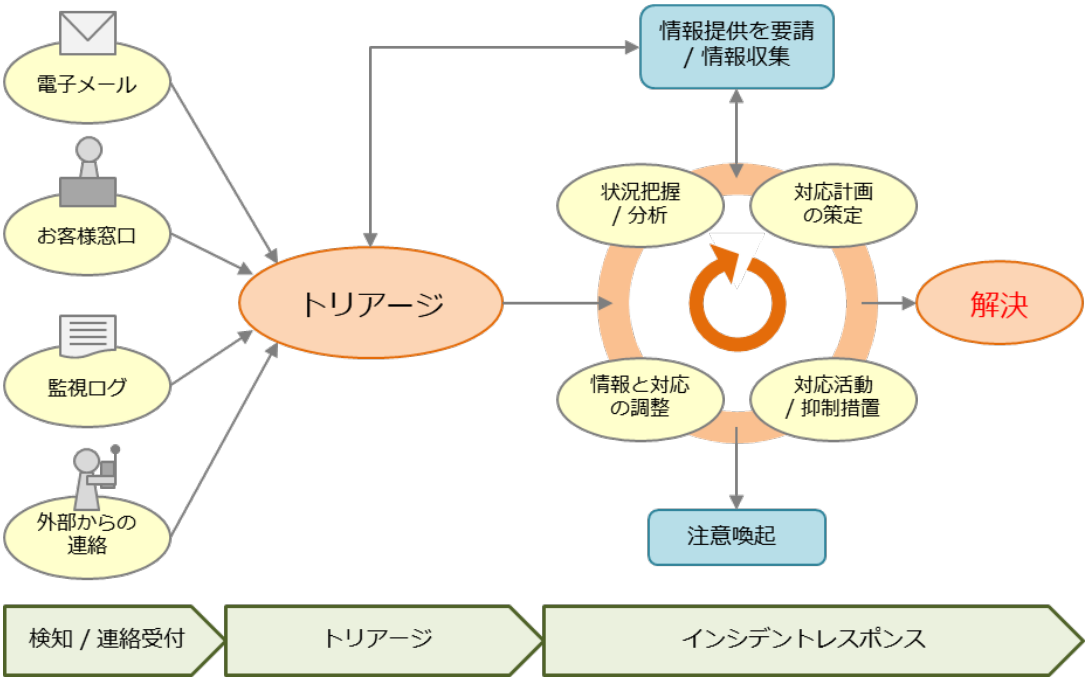
インシデントの被害の拡大防止などを目的にサービス対象に対して情報共有と注意喚起を行います。

（4） インシデント対応以外の要請への対応

インシデント対応の結果 （顛末など） を、当該インシデントについて CSIRT に対応を要請した方や関係者（上位組織や監督官庁など）に報告したり、必要に応じて広報部門を通じて情報を公表したりします。

6.3 インシデントハンドリングの流れ

代表的なインシデントハンドリングの流れを示したのが次の図です。



［図 6.3-1 代表的なインシデントハンドリングの流れ］

監視システムなどからの情報や外部からの通報などで検知または認知したインシデントを、必要に応じた外部との情報共有などに基づいてトリアージして、実際に対応すべきインシデントか否かを判断します。対応すべきインシデントに対しては、状況の把握、分析を行い、対応計画を策定します。インシデントが高度サイバー攻撃（APT）によるものだと判断される場合は、インシデントによるリスクと組織のリスク許容度に基づいて取るべき措置を検討します。脅威の排除とインシデントの範囲特定のどちらを優先とするかを判断し、対応計画に盛込みます。
次に策定した計画に基づいて対応を行い、抑制措置や範囲特定を実施します。その後、実施した対応や対策が適切であったかを確認し、必要であれば、改めて状況の把握と分析を行い、対応計画を練り直しま

す。このような「繰り返し」の結果として最終的な解決に導きます。

7. CSIRT 構築にあたって

7.1 CSIRT のメンバー

インシデントが IT に基づくものであることから、CSIRT のメンバーには IT に関する技術的専門知識が必要とされることは確かです。しかし、そのような専門知識や IT 分野における経験は、必ずしも CSIRT メンバーとなる者への必須要件とはなりません。
これまで説明してきたように、CSIRT に最も必要な「信頼」を維持し、そして速やかにかつ的確にインシデントに対応するためには、関係者とのコミュニケーションが最も重要です。
したがって、CSIRT メンバーに必ず必要とされるのは、サービス対象をはじめとする社内外の関係者とのコミュニケーションを適切に取ることができる能力、そして「個人プレイ」に走ることなく、チームメンバー間で情報を共有し、「チームプレイ」で動ける能力です。
CSIRT がサービス対象に対して提供するサービス内容によって、メンバーに求められる能力に違いはありますが、一般的に CSIRT の人材の登用にあたっては、技術的な知識や経験よりも、優れた対人スキルとコミュニケーション能力を持つことを重視し、もし CSIRT に求められる技術的知識が足りない場合はそれを後から身に付けさせるほうが、その逆より望ましいと言えます。
また、CSIRT メンバーの心得として、**サービス対象に対して情報セキュリティを担う者としての模範たる姿勢を示すこと**が求められます。これがなければ、CSIRT に対するサービス対象からの信頼を獲得し維持することはできません。

7.2 設備

CSIRT が扱う情報の多くは機密情報です。したがって、その管理には充分なセキュリティ対策が必要です。ここでは一般的なセキュリティ対策の他に、CSIRT に特徴的な設備として多くの CSIRT で用いられているものについて簡単に紹介します。ただし、これらはあくまで例であり、必ずしもここで紹介したものと同等のものが必須というわけではありません。セキュリティポリシーやサービス内容、災害時におけるサービスの継続性などに応じて必要なものを選択してください。また設計にあたっては、情報セキュリティを担う部署または機能として、サービス対象に対して模範的なものであることが強く求められます。

（1） 執務スペース 

セキュリティ上安全に保護すべきエリアを明確に定義（レベル分け）し、保護の必要のないエリアとは完全に分離します。一般的に、保護されたエリアへ入るには物理鍵以外の認証方法が使われます。例えば、多くの CSIRT では、生体認証や IC カード、暗証番号などが単一もしくは複数の組み合わせで用いられています。

（2） 通信設備  

インターネット（電子メールなど）

サービス対象や外部からの連絡を受け付けるアドレス宛に送られてきたメールは、複数の CSIRT メンバーが何らかの形で確実に見られるようにしておきます。

暗号化および電子署名付きメールが使えるようにしておきます。なお、CSIRT のコミュニティーでは PGP/GnuPG が事実上の標準となっています。

CSIRT がやり取りするメールを CSIRT メンバー以外が読むことがないように、メールサーバー、外部からの配送経路、また外部とのインターネット接続を、CSIRT 以外の業務と分離しておくとよいでしょう。

電話およびファックス

CSIRT メンバー以外がアクセスすることがないように、CSIRT 以外の業務エリアとは物理的に切り離された（アクセスに何らかの認証が必要な）場所に電話機およびファックス装置を設置します。

（主に CSIRT コミュニティーからの） 緊急時の連絡が可能な電話番号を用意します。多くの場合、CSIRT の POC 担当者の携帯電話に繋がるようにしておきます。

他の業務用の番号へ誤って繋がることがないように、似た番号を使うのを避けることも考慮すべきです。

（3） データ管理・破棄 

機密情報については、紙や CD-R などの物理的なものは耐火金庫、電子データは暗号化ファイルシステムを用いたハードディスク上に保管しておくことがあります。また物理データの破棄用に、紙や CD-R を粉砕できるシュレッダーを用意し、さらに大量の紙データの溶解処理やハードディスクの物理破壊を外部業者に委託する手順を定めておきます。

（4） インシデントトラッキングシステム（ソフトウェア） 

一般的に CSIRT ではインシデントの対応進捗状況を管理するシステムが使われています。このようなトラッキングシステムとして、オープンソースのソフトウェアである RTIR（Request Tracker for Incident Response）などが有名ですが、多くの CSIRT では独自に開発したシステムが使われているようです。

RTIR： RT for Incident Response <https://bestpractical.com/rtir/>