JPCERT CC®

CSIRTマテリアル 構築フェーズ 「組織内CSIRTの理解」

一般社団法人
JPCERTコーディネーションセンター

本資料について

- 本資料は、CSIRTのコンセプトと構造、活動内容について簡潔に説明する資料として作成したものです。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方が、それまでのインシデント対応経験をもとに、既存の体制を整理したり、見直したりしてCSIRTの構築に繋げる際の参考として頂くことを意図しています。
  本資料を含む一連のCSIRTマテリアルでは組織内CSIRTが一般的に備えるべき機能や能力について説明していますが、すべての組織内CSIRTがそれらを達成しなければならないというものではありません。それぞれの組織の状況に応じた適切なCSIRTの形があり、本資料がそれを見つける際の助けとなれば幸いです。

- 「CSIRTマテリアル」内の他の文書とあわせてご利用ください。
  - 構想フェーズ：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 ～
  - 構築フェーズ：「組織内CSIRT構築の実践」
  - 運用フェーズ：「CSIRTガイド」「インシデントハンドリングマニュアル」

CSIRTマテリアル 構築フェーズ「組織内CSIRTの理解」
目次

1．インシデント対応と組織内CSIRT

インシデントとは

- コンピューターセキュリティインシデントとは
  - 情報システムおよび制御システムの運用におけるセキュリティ上の問題として捉えられる事象。組織のセキュリティポリシーに違反し、情報システムやネットワークの健全な利用・運用および情報管理に関して脅威となる行為や事象を指す
    - 例：情報流出、フィッシングサイト、不正侵入、マルウェア感染、Webサイト改ざん、DoS(DDoS) 攻撃などのさまざまな事象
  - 本スライドおよび一連のCSIRTマテリアル関連資料においてはコンピューターセキュリティインシデントを指して「インシデント」という

- 安全管理の分野では、「重大な事故になり得る、または事故を引き起こす可能性がある状況」をインシデントと呼んで、事故（アクシデント）と区別しているので注意されたい

1-1. インシデント対応活動の必要性

予防策を尽くしても防げないインシデントがある

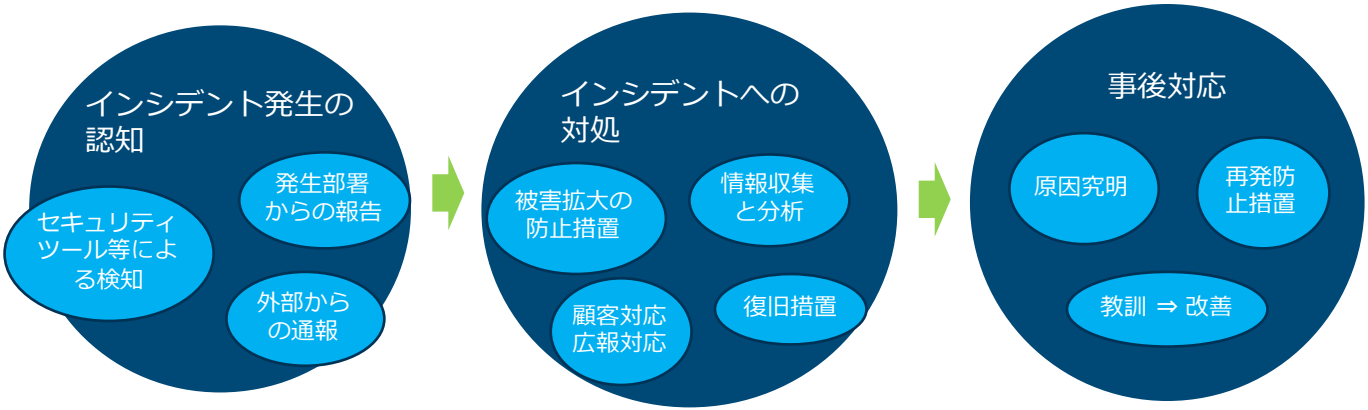
- コンピューターセキュリティを取り巻く状況を見ると．．．
  - 人為的ミス（パッチの適用忘れ、設定ミスなど）
  - 未知（公知になっていない）の脆弱性の悪用
  - 技術的な対応の限界
  - 従業員の意識に頼るところが必ず存在

インシデントの発生を完全に回避するための予防策はない

（発生確率を低下させ、発生時の影響や被害を低減するための予防策はある）

インシデント対応（活動）とは

- インシデントが発生した時に、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
  - インシデントを検知する、あるいは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、情報収集と分析によってインシデントの全体像や原因について把握し、復旧措置や再発防止措置を取る一連の活動



1-1. インシデント対応活動の必要性
対処の難しいインシデントが増えつつある

- IT 依存度の高まり
  - IT システムの複雑化
  - IT システムの汎用化

- 脅威の変化
  - 攻撃活動の潜在化
  - 攻撃手法の高度化
  - ソフトウェアの脆弱性を利用したゼロデイ攻撃
  - APTのような組織化され資金と技術力を備えた高度な脅威アクターの存在

インシデントの発見、原因特定、復旧に時間がかかる、あるいは困難になる

一つのインシデントによる被害が拡大しやすく、その伝播が速い

高い専門性が必要になり、単独の部署では対応が難しいことがある

インシデント対応のための体制づくりが必要に！

効果的なインシデント対応のための体制づくり

- 効果的なインシデント対応活動を実現するには
  - インシデント対応活動に関する機能要素を特定する
    - インシデントを発見する機能、インシデントを報告する機能、インシデントの報告を受ける機能、・・・・

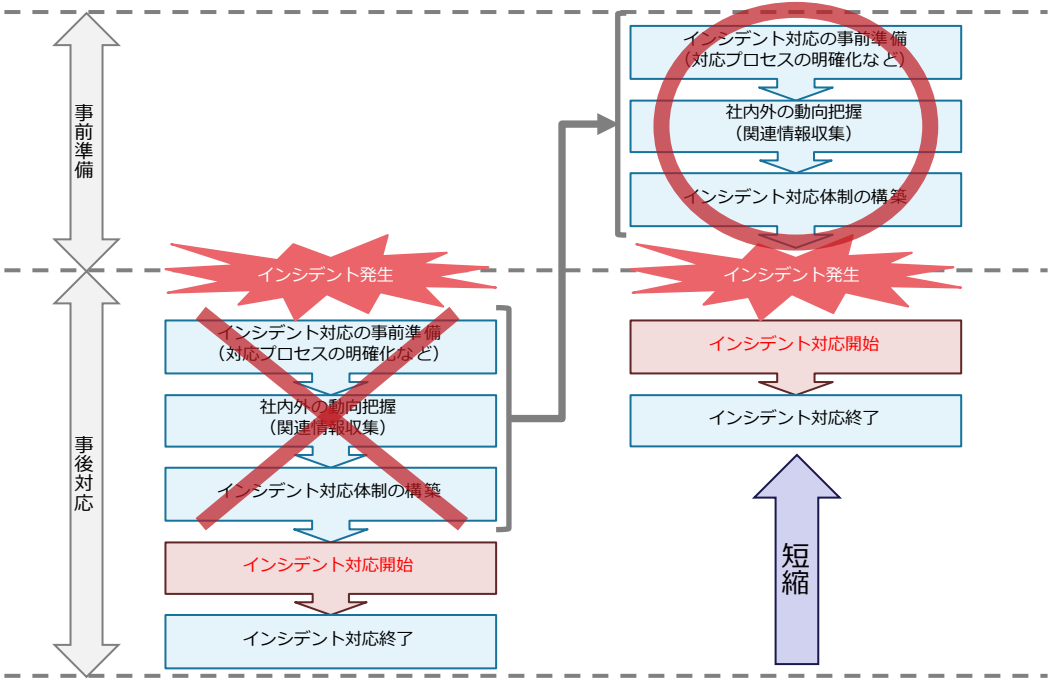
  - それらの機能要素を有機的に結びつける
    - 各要素の役割の設定、各要素間のインタフェースおよびコミュニケーションの確立、・・・・

  - 全体として、統一性と一貫性のある状態にする

インシデント対応体制の構築へ

円滑なインシデント対応には事前の準備が必要

- インシデントが発生してから対応方法を検討し体制を用意するのでは被害の拡大を止めることはできないため、**事前に対応体制を整えておく**必要がある



インシデント対応体制に求められる主な機能

- 組織内の情報共有と連携
  - インシデント報告を集める窓口の一本化
  - 組織内のインシデントの一元管理と部署間調整

- 外部組織との調整
  - 外部からのインシデント関連情報を受け取る窓口の一本化
  - 組織間での連携が必要となる状況に備え、事前の外部組織との信頼関係の構築
    - 外部に起因するインシデント（DDoS、不正アクセス、フィッシングメールなど）を解決するための当事者や関係者との折衝を含む

インシデント対応手順の策定

- インシデント対応体制の構築には、組織の情報セキュリティリスクを想定したインシデントシナリオを検討し、その対応手順を立案することが重要

- インシデント対応手順を立案するためのポイント
  - ネットワークおよびシステムを含む、情報資産の特定
  - リスク評価の実施とリスク許容度の設定
  - インシデント対応ポリシーおよび手順等の整備
  - インシデント対応の担当者／責任者の明確化
  - インシデント発生時の報告窓口の一元化
  - インシデント対応に必要な技術的支援、ノウハウ、関連情報の入手を支援する人／チーム／部署の設置
  - 連携するべき外部組織の特定と、外部組織の対応能力、連携手順の把握
  - インシデントの種別に応じた対応マニュアルの整備

インシデント対応体制と組織内CSIRT

- 組織内CSIRTとは
  - 組織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への対応と関連業務を専門に担当するチーム
    - 発生したインシデントに関する分析と対応
    - 組織のセキュリティ品質向上のための教育や監査などの活動
  - 組織内および外部組織と適切に連携し、組織のインシデント対応体制における中心的な役割を担う

「組織のインシデント対応体制」のベストプラクティス ＝ 組織内 CSIRT

組織内CSIRTの主な役割

組織内に対する主な役割

- 組織内で発生したインシデントの報告を受けるための、一本化された窓口を提供する
- 発生したインシデントに対応する、または、対応に必要な技術的支援やノウハウを提供する
- インシデント対応における組織の意思決定を支援する
- 組織横断的に発生するインシデントにおいて、組織内の調整役として活動する
- 情報システム管理者、ユーザー、経営層、その他の従業員に対し、セキュリティ教育と意識啓発を行う

組織の外部に対する主な役割

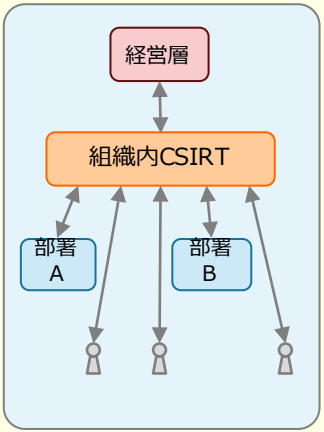
- 外部のインシデント対応組織との連絡調整を行う
- セキュリティインシデントの事例や動向、インシデント対応手法や技術に関する情報を収集し、組織内に展開する
- 従業員・メディア・顧客を含む組織内外のステークホルダーへの適切な情報提供を行う、またはそれを支援する

組織内CSIRTによる効果

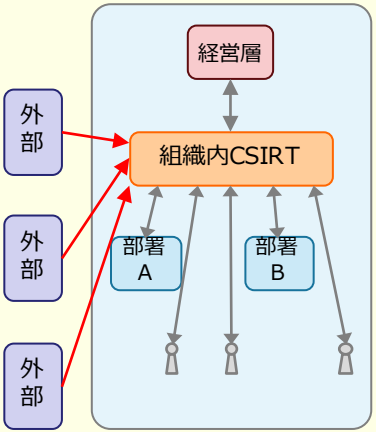
■ 組織内CSIRTを整備することで、一般的に以下のような効果が期待できる

①インシデントに関する情報を一元的に管理することにより
- **組織内のセキュリティ情報の共有と集中管理**
- **セキュリティ対応に係る指示系統の迅速化**

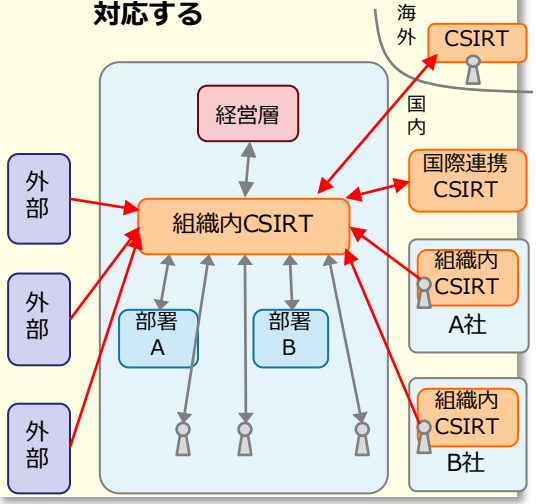
を実現する



②組織のインシデント対応に関する統一された窓口となることにより
- **外部に対して信頼性のある窓口を提供する**
- **外部からの情報を一元管理する**



③外部組織との窓口として認知され、インシデント関連情報の共有やインシデント対応における連携を可能にすることにより
- **インシデント対応に利用可能な情報量を向上する**
- **想定外のインシデントにも柔軟に対応する**



組織内CSIRTの構築を推奨する

- 組織内CSIRTの整備は今日の標準的なセキュリティプラクティスの一つ
  - インシデントによる被害の局限化と迅速な復旧を図る「組織的なインシデント対応体制」の一般的なプラクティス
  - 外部組織と連携したインシデント対応を実現するための有効な手段

- 組織内CSIRTの広がり
  - 多くの組織において組織内CSIRTが整備・運用されている
    - FIRST（インシデント対応チームの世界的なフォーラム）
      https://www.first.org/
    - TF-CSIRT（ヨーロッパにおけるCSIRTのフォーラム）
      https://tf-csirt.org/
    - 日本シーサート協議会
      https://www.nca.gr.jp/

（参考）組織内CSIRTの構築に役立つ資料

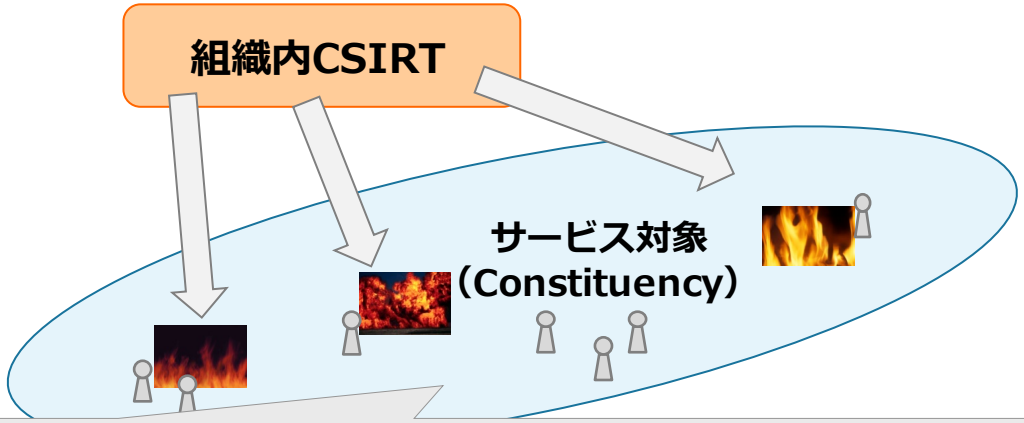
- JPCERT/CC
  - CSIRTマテリアル
    - https://www.jpcert.or.jp/csirt_material/
  - コンピュータセキュリティインシデント対応チーム（CSIRT）のためのハンドブック
    - https://www.jpcert.or.jp/research/2007/CSIRT_Handbook.pdf

- その他
  - 日本シーサート協議会
    - CSIRT構築に役立つ参考ドキュメント類
      https://www.nca.gr.jp/activity/build-wg-document.html
    - CSIRT 人材の定義と確保
      https://www.nca.gr.jp/activity/training-hr.html
  - CERT（カーネギーメロン大学）– “CREATE A CSIRT”
    - https://resources.sei.cmu.edu/asset_files/WhitePaper/2017_019_001_485695.pdf
  - AusCERT – “Forming an Incident Response Team”
    - https://www.auscert.org.au/publications/forming-incident-response-team
  - RFC 2350 – “Expectations for Computer Security Incident Response”
    - https://www.ietf.org/rfc/rfc2350.txt

2．組織内CSIRTの役割

2-1. サービス対象とCSIRT

- CSIRTはそのサービスを提供する目的の相手である「サービス対象（Constituency）」を持つ



サービス対象（Constituency）とは：

CSIRTのサービス（インシデント対応や、そのための技術的支援など）を提供する対象を指す。
一般的な組織内CSIRTのサービス対象は以下を含む。

- システム管理者、ネットワーク管理者
- 従業員
- 顧客
- 関係組織（グループ会社や保守管理業務を受託している会社など）

2-2. 組織内CSIRTの役割

- 組織によって事業内容、規模、部門構成、業務遂行形態、組織や事業に対する脅威およびリスクが異なる

↓

- 発生するインシデントの傾向が違う
  - 発生しやすいものや、発生しにくいものがある
- インシデント対応のアプローチがいろいろある
  - 現場で技術的な解決が直接される場合や、外部の対応組織に依頼しなければならない場合などがある

↓

組織内CSIRTに期待される役割（インシデント対応）の範囲が違う

2-3. インシデント対応の重要ポイントから見る役割

- 適切なインシデント対応を行うための重要なポイント
  - ユーザーからのインシデント報告
    - インシデント発生時にサービス対象（一般ユーザーなど）から組織内CSIRTへ適切に報告されるようにする
  - 外部のインシデント対応チームとの連携
    - 組織内CSIRTは、外部のインシデント対応チームの対応能力と連携の手順を理解し、適切な依頼をすることができる関係を維持する
  - インシデント関連情報の伝達経路の保全
    - 組織内CSIRTは、インシデント関連情報をやり取りするための、なりすまし、改ざん、盗聴などがされない安全な経路を確保する
  - 他組織のCSIRTとの情報共有
    - 組織内CSIRTは、他組織のCSIRTと相互補完的な関係になり、同一または類似の脅威による被害を防止する

2-3. インシデント対応の重要ポイントから見る役割
「ユーザーからのインシデント報告」

- 組織内CSIRTがユーザーからインシデント報告を受けるために必要なこと
  - サービス対象（一般ユーザーなど）は、インシデントを報告する必要性を理解している

    組織内CSIRTは、サービス対象者に対して、セキュリティに関する啓発活動をする
  - サービス対象は、組織内CSIRTがどんな目的で何をするのかを理解している

    組織内CSIRTは、サービス対象者に対して、組織内CSIRTに関するポリシーや報告手順を（Web サイト等で）周知徹底する
  - サービス対象は、組織内CSIRTに何を期待していいのか、かつ、信頼していいのかを理解している

    組織内CSIRTは、適切なインシデント対応の実績を積み重ね、サービス対象からの信頼を得る

2-3. インシデント対応の重要ポイントから見る役割
「外部のインシデントチームとの連携」

- 組織内CSIRTが外部のインシデント対応チームと適切に連携するために必要なこと
  - 組織内CSIRTは、どのインシデント対応チームに何を依頼できるかを知っている

    組織内CSIRTは、平時より外部のインシデント対応チームとコミュニケーションをとっておく

  - 組織内CSIRTは、外部のインシデント対応チームとの間に、適切に依頼をすることができる関係（依頼を受けてくれる関係）がある

    組織内CSIRTは、外部のインシデント対応チームと信頼関係を構築しておく

2-3. インシデント対応の重要ポイントから見る役割
「インシデント関連情報の伝達経路の保全」

- インシデント関連情報の伝達経路に求められること
  - サービス対象（一般ユーザーなど）や外部のインシデント対応チームが、組織内CSIRTから来る情報に関して、なりすましや改ざんが行われていないことを確認できること

組織内CSIRTは、発信する情報に関して、その情報の完全性および信頼性に関して確認する手段を提供する

  - サービス対象および外部のインシデント対応チームと組織内CSIRTとの間のやり取りが第三者に盗聴されないこと

組織内CSIRTは、盗聴されてはいけない情報伝達には、暗号技術を活用する

2-3. インシデント対応の重要ポイントから見る役割
「他組織のCSIRTとの情報共有」

- 他組織のCSIRTとの情報共有を行うために必要なこと

  — 攻撃者のプロファイルやインディケータといった、攻撃活動の予防・発見に役立つ情報が共有できる状態にある

  組織内CSIRTは、攻撃者のプロファイルを構築し、インディケータの管理をする

  — 他組織のCSIRTとの間で、安全なコミュニケーション方法を使い、タイムリーな情報共有が実施できる

  組織内CSIRTは、安全な情報共有方法を用意し、他組織のCSIRTとの技術情報の交換やワーキンググループの実施を検討する

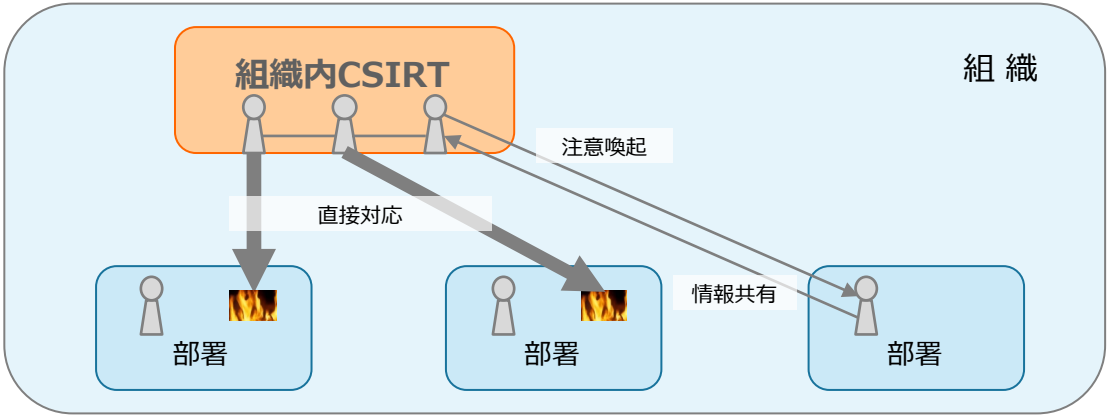
2-4. 経営層やサービス対象からの期待から見る役割

- 組織内CSIRTの役割（インシデント対応）の範囲は、**経営層やサービス対象から期待されること**によって定義される

- 組織内CSIRTに対する一般的な期待
  - インシデントへの「直接」対応
    - 組織内においてインシデントに**「直接」対応**するチームを設けたいという期待
  - インシデントへの「支援的」対応
    - 特定の部門ではインシデント対応を行う機能があるが、組織全体のインシデント対応に結びついていないため、部門によるインシデント**対応を「支援」**しながら、組織全体の統制をとるチームを設けたいという期待
  - インシデントへの「調整役としての」対応
    - DoS攻撃、不正アクセス、フィッシングのような外的要因のインシデントに対応するために、組織内外の部門と**「調整して」対応**するチームを設けたいという期待

インシデントへの「直接」対応

- 組織内CSIRTにインシデントに**直接**対応することを期待する

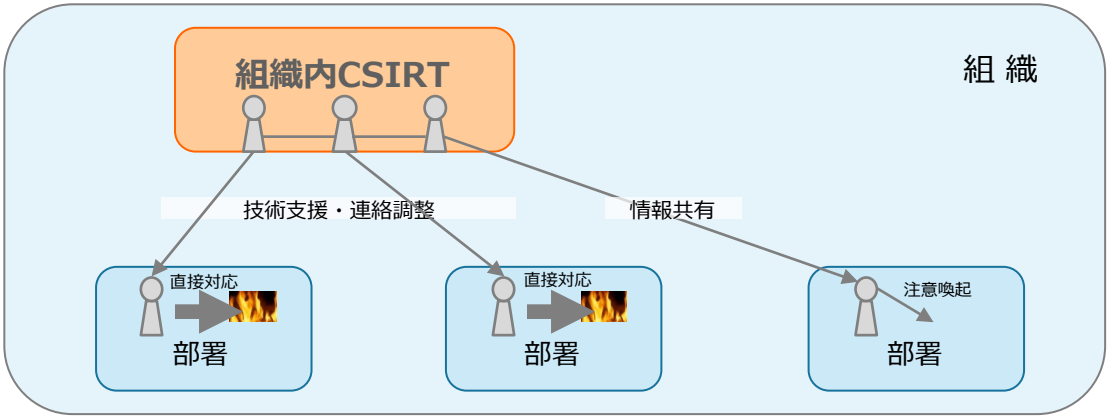


- 責務と使命の例：
  - 組織内CSIRTは、組織内で発生したコンピューターシステムおよびネットワークなどで発生するインシデントの被害を局限化し、迅速な復旧を実施する
  - 組織内CSIRTは、インシデントが早期に発見され、迅速に対応できる仕組み（各部署等との情報共有および連携など）を整備し維持する

2-4. 経営層やサービス対象からの期待から見る役割

インシデントへの「支援的」対応

- 部門内で発生するインシデントへの対応能力はすでにあるが、組織全体でのインシデント対応能力が十分ではないため、組織内CSIRTに**インシデント対応の支援および調整**を期待する

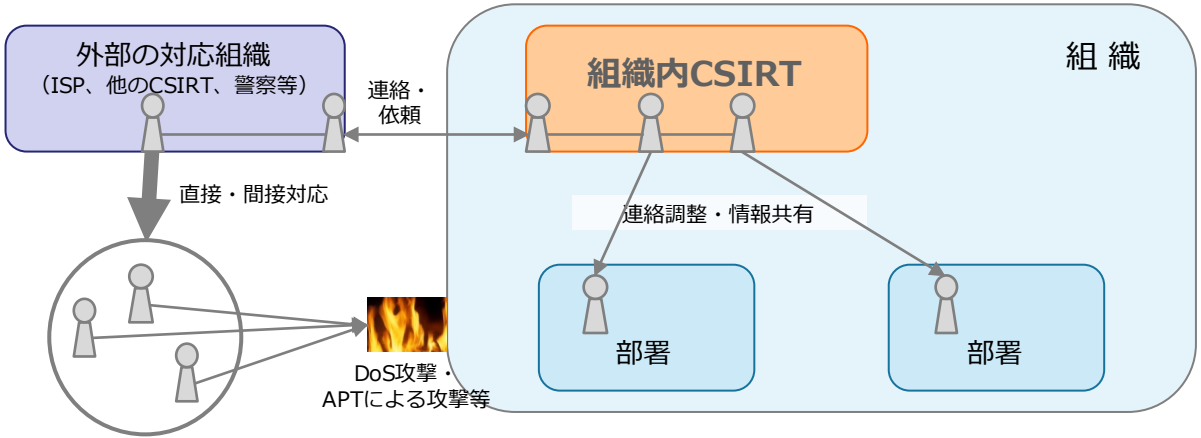


- 責務と使命の例：
  - 組織内CSIRTは、組織内で発生したインシデントに対する各部署等の対応活動に対して、技術的支援、組織内全体の調整、統制等をすることにより、迅速な被害の局限化および迅速な復旧を支援する

2-4. 経営層やサービス対象からの期待から見る役割

インシデントへの「調整役としての」対応

- 外的要因に基づくインシデント（DoS攻撃、APTによる攻撃等）に対する対応能力が十分ではないため、組織内 CSIRTに**インシデントへの対応と、それに必要な組織内外への調整**を期待する



- 責務と使命の例：
  - 組織内CSIRTは、外的要因に基づくインシデントに対応する責任を持ち、外部のインシデント対応組織との連携および組織内における必要な調整をすることにより、被害を局限化し、迅速な解決に努力する

2-5. 組織のインシデント対応に一貫性と整合を与える

■ インシデント対応を行う既存のチームが組織内に複数存在する場合

例：
- ネットワーク運用部署・・・ネットワークのセキュリティに関する対応
- システム管理部署・・・PCやサーバ、およびサービスのセキュリティに関する対応
- 情報セキュリティ管理部署・・・組織全体のポリシーや手順の違反に関する対応

■ 考えられる課題

- それぞれのチームの対応は連携していなければならない
- インシデント対応は組織全体として整合のとれたものでなければならない
- 外部とやり取りをする場合、組織の窓口としての一貫性を保つことができなければならない
- 発生したインシデントが、正しい相手に適切に報告されなければならない

組織内CSIRTがこれらの役割を果たす

参考：CSIRTの役割の説明に役立つ資料

CSIRTと消防署の役割の比較

CSIRTの場合（例）

- 発生したインシデントへの対応
  - 連絡先の提供：Email アドレス／電話
  - 連絡目的：対応や技術支援などの要請
  - CSIRTでの活動：
    - インシデントの分類、優先度の判断と対応方法の決定
    - 適切な（技術的）対応を取る人への連絡調整
    - 被害の局限化策の実施（ネットワークからの切り離し、システムの設定変更等）
    - インシデント原因の排除（脆弱性箇所へのパッチ適用、ウイルス除去、Phishing サイト停止等）
- インシデントの発生予防
  - ユーザーへのセキュリティ啓発活動
  - インシデント脅威情報の提供

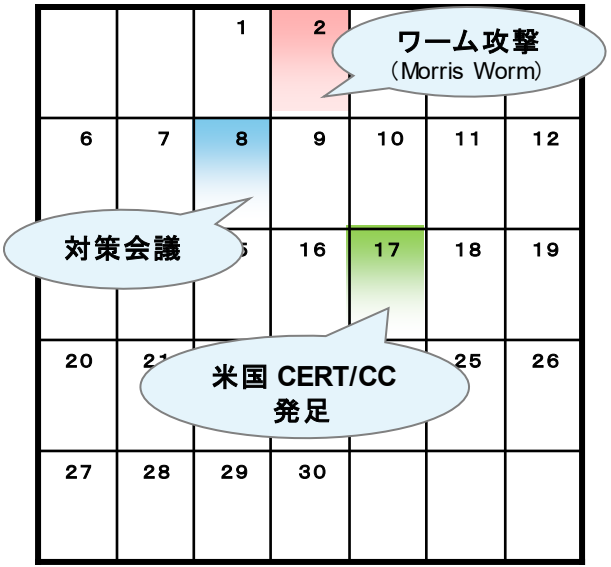
消防署の場合（例）

- 発生した火事や事故への対応
  - 連絡先の提供：　電話（１１９番）
  - 連絡目的：　消火依頼、救出要請など
  - 消防署での活動：
    - 火災規模、症状等の判断と対応方法の決定
    - 最寄の消防車や救難器材の手配に関する連絡
    - 火事の拡散防止や救出等の緊急避難等のための一部破壊
    - 消火活動および救出活動
- 火事や事故の発生予防
  - 防火訓練や救出講習等の啓発活動
  - 火災／乾燥注意報による注意喚起

参考：CSIRTの役割の説明に役立つ資料

CSIRTの概念が作られたきっかけ

1988年11月

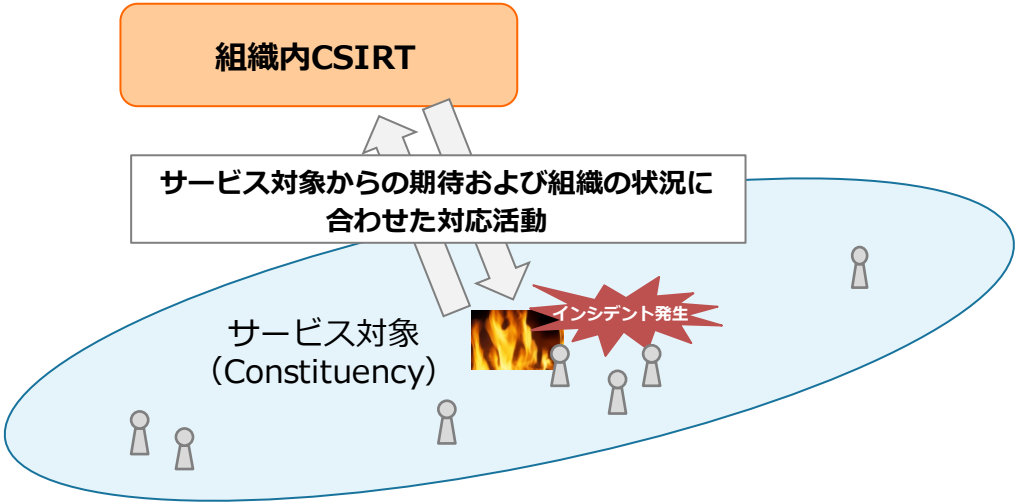


- 1988年米国において発生したMorris Wormの蔓延が、当時のネットワーク全体に多大な被害を与えた
- その後、このようなインシデントに対して相互協力（情報共有、連携対応等）できる体制の必要性が高まる
- 1988年11月、利害関係者間の連絡調整におけるセンターとして、CERT/CCが発足
  - 主要なセキュリティインシデントの対応およびプロダクト製品の脆弱性分析を主として、その役割は拡大している
  - 世界で初めての CSIRT

※参照元：*Handbook for Computer Security Incident Response Teams (CSIRTs)*
https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf

３．組織内CSIRTの活動を定義する

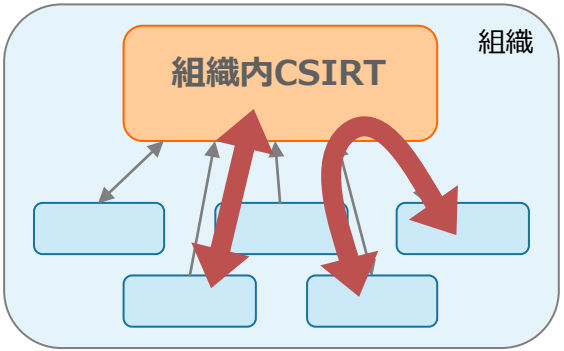
3-1. 組織内CSIRTによるインシデント対応活動



- インシデント発生時に、サービス対象からの期待および組織の状況にあわせたインシデント対応活動を提供する
  - 報告窓口の提供と告知、問題の切り分け、技術的支援、解決策の情報提供、被害の抑制策の実施、復旧の支援など

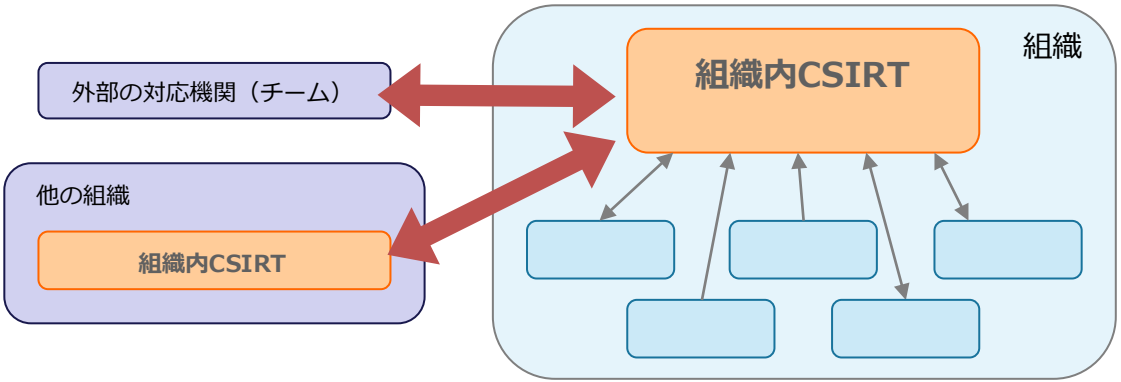
3-2. インシデント対応に備える（1）

- 組織内に対する活動：
  - サービス対象との良好な関係を維持する
    - 適切にインシデント報告を行うよう啓発するとともに、インシデントの報告先、報告内容、手順などを周知する
    - 強制力に頼るのではなく、サービス対象の理解と協力が得られるよう啓発する
    - 組織内CSIRTが誰とどのように連携・調整してインシデント対応を行うのかを周知する
  - サービス対象の状況を把握する
    - 組織内のネットワークやシステム、PC等に関する最新の利用状況を把握する



3-2. インシデント対応に備える（2）

- 外部との連携・調整を含む活動：
  - 外部に対するPOC（Point of Contact：連絡窓口）を設ける
    - 外部に対して、連絡先（メールアドレスや電話番号など）をメールやWeb等で周知する
  - 外部との良好な関係を構築・維持する
    - 平時より外部の連携先組織とコミュニケーションをとり、それぞれの体制、能力、連携手順等について相互理解する



3-3. インシデント対応活動を定義する

■ 組織がCSIRTに対し次のような役割を期待する場合

> 組織内で発生したインシデントに対して、
> 適切な対応活動を実施し、速やかな復旧の支援をする

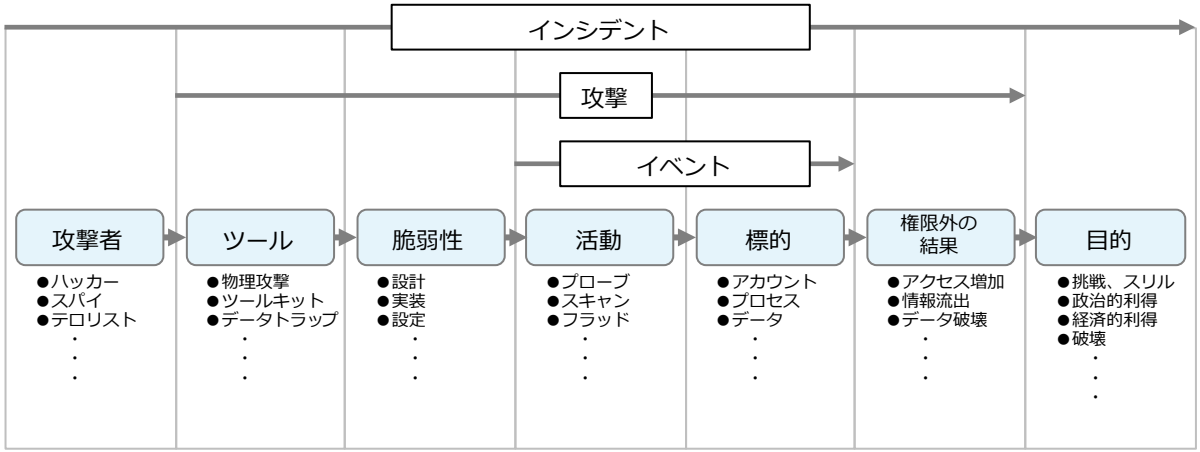
■ 組織における「インシデント」を定義する

- これまで発生したインシデントの傾向を分析する
- 同業他社で発生しているインシデントを把握し発生可能性を検討する
- 経営層や従業員が認識しているインシデントを把握する
- 予測されるインシデント発生箇所を把握し分析する
- 可能であれば、インシデントの分類を検討する

インシデントの定義は、組織内CSIRTの活動の基本方針を決めるための基礎となる重要な定義である

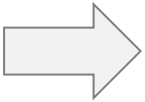
（参考）「インシデント」「攻撃」「事象（イベント）」の定義

- 用語としての「インシデント」、「攻撃」、「事象（イベント）」の使い分けの例については、以下の報告書で記述されている
  - 米国 Sandia National Laboratories の報告書
    “A Common Language for Computer Security Incidents”
    https://prod-ng.sandia.gov/techlib-noauth/access-control.cgi/1998/988667.pdf



3-3. インシデント対応活動を定義する

- 組織における「適切な対応」を定義する
  - 組織におけるCSIRTの位置づけやサービス対象との関係を考慮し、何ができるのか／何ができないのかを特定する
  - 組織内だけでは対応できないものを特定する
    - それらを解決するための外部との連携について事前に検討する
  - 経営層やサービス対象が期待する「適切な対応」を理解する
  - インシデントが発生した際、「直ちに排除する」か「範囲を特定する」かの判断ができるように、組織のリスク許容度を評価する



「適切な対応」の活動リストと、それらを実現するため事前に準備しておかなければならない活動のリストが得られる

（参考） 組織内CSIRTの活動の分類

- 組織内CSIRTの活動は、以下のように分類できる
  - 事後対応型の活動（Reactive Service）
    - インシデント報告や検知システムなどからの情報による活動
  - 事前対応型の活動（Proactive Service）
    - 脆弱性情報、脅威情報、攻撃予測情報などを提供する活動
    - インシデントの未然防止と発生時の被害抑制に直接的に寄与する
  - セキュリティ品質マネージメントに関する活動
    - セキュリティコンサルティング、教育・訓練など
    - CSIRTとしての視点や専門知識に基づいて組織のセキュリティの底上げを図る
    - インシデントの未然防止と発生時の被害抑制に間接的に寄与する

（参考）CERT/CC における分類の例

事後対応型の活動

・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

事前対応型の活動

・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

セキュリティ品質マネージメントに関する活動

・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

3-4. 組織内CSIRTの活動のフレームワーク

- 組織内CSIRTの活動の基本骨子を定義する
  - ミッションステートメント
    - 大局的な目標と目的 – 何を果たすべきなのか
  - サービス対象
    - 誰のために活動するのか
    - サービス対象はCSIRTとどのような関係にあるのか
    - サービス対象はCSIRTをどの程度認識しているか
    - サービス対象はCSIRTを信頼しているか
  - 組織内の位置づけ
    - 組織内におけるCSIRTの位置
    - 組織内におけるCSIRTの役割
    - 組織内の各部門・部署との関係
  - 他のチームとの関係
    - 他組織のCSIRTとの協力と連携

「ミッションステートメント」の定義

- 組織から求められる役割を明確にする
- 組織内CSIRTのミッションステートメントを作成する
  - 組織の活動目的に合致し、その実現に寄与するものでなければならない
- 経営層による承認を得る

組織内CSIRTの役割、目的、活動を理解してもらうために、サービス対象者や他のCSIRTに対して「ミッションステートメント」を周知する

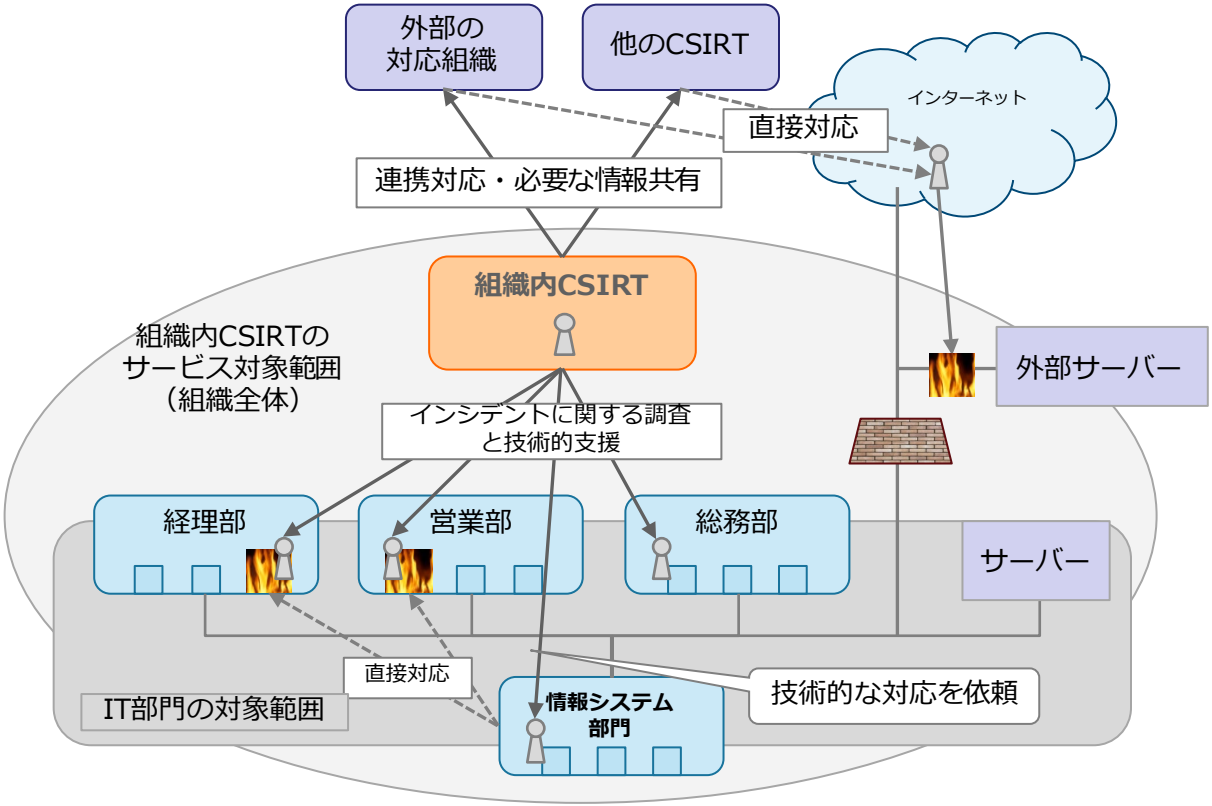
「サービス対象」の定義

- 組織内CSIRTがサービスを提供する対象を設定する
- 組織内CSIRTがサービス対象に対して行使できる権限を設定する
  - サービス対象に対する強制的な権限を持つのか、持たないのか
- 組織内CSIRTが何をするのかをサービス対象に周知する
  - インシデントの報告先として認知してもらう
- サービス対象からの信頼を得る
  - 信頼がなければインシデントは報告されない

「組織内の位置づけ」の定義

- 組織のリスク管理全体においてCSIRTに求められる役割を明確にする
- インシデント対応を行う他の部門・チーム・機能が組織内に存在する場合、それらとCSIRTの関係や、両者のミッションステートメントやサービス対象定義における区別を明確にする
- 組織におけるCSIRTの責任を明確にする

（参考）IT 部門と組織内CSIRTの活動範囲の関係の例



「他のチームとの関係」の定義

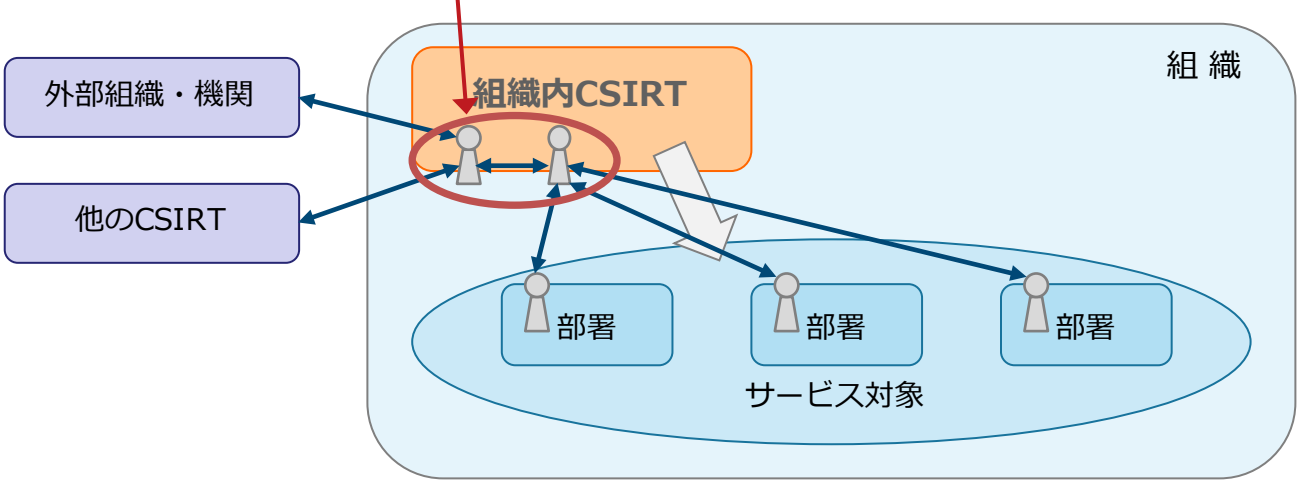
- 組織内CSIRTが外部のCSIRTとの調整・連携を行うという役割を明確にする
- 外部のCSIRTが何ができ、どんな調整・連携ができるかを理解する
  - 逆に、自らができることを外部のCSIRTに伝えることも重要
- 外部のCSIRTとの連携に必要なことを定義する
  - 有事の際には突発的で非公式な依頼を行うこともあるため、事前の信頼関係の構築が重要となる

４．組織内CSIRTの要員

4-1. 組織内CSIRT要員の重要なスキル

- CSIRT要員は、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対話を行うことが求められる

コミュニケーションスキル（対人能力とその意欲）が重要



4-2. 組織内CSIRT要員に必要なヒューマンスキル

■以下の**能力と意欲**を持っていることが求められる

- 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
- 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
- 規則や取り決めなどに従うことができること
- 強いストレスのある状況下で業務を遂行できること
- チームの評判を守る大局的な視点と行動ができること
- 勉強を続ける姿勢があること
- 問題解決能力
- 他のメンバーとの連携能力
- 時間管理能力

参考文献：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
CERT/CC 発行 （翻訳：JPCERT/CC）

4-3. 組織内CSIRT要員に必要なテクニカルスキル

- サービス対象の業務、システム、ネットワーク、関連規則等の知識のほかに、以下のテクニカルスキルや知識が必要となる
  - 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）
  - 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）
  - 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）
  - 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）
  - 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）
  - ネットワークアプリケーションとサービス
  - 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）
  - ホスト／システムのセキュリティ（システムの運用と管理）
  - 暗号技術に関する知識
  - プログラミングに関する知識

参考：CSIRTにおけるさまざまな役割とスキル

- インシデント対応は組織のリスク管理に関わる性質のものであるため、その中心となるCSIRTには情報セキュリティ技術に留まらない広範な知識と専門性が求められる。
  日本シーサート協議会ではCSIRTの活動において求められる役割を細分化しそれぞれに必要な人材のスキルについて纏めた文書を公開している。

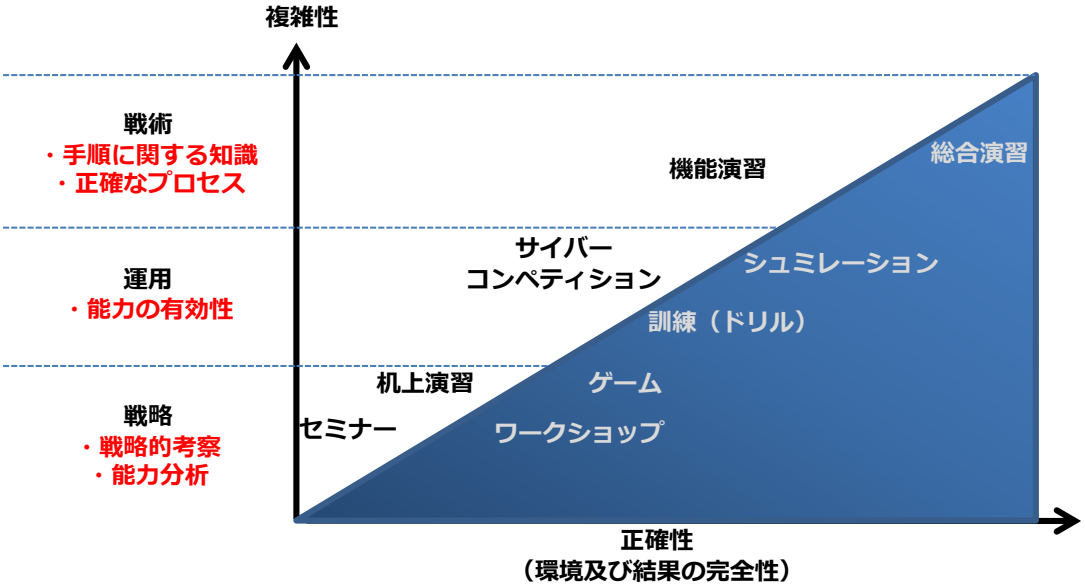
  — 日本シーサート協議会「CSIRT 人材の定義と確保」
  https://www.nca.gr.jp/activity/training-hr.html

4-4. 組織内CSIRT要員へのトレーニング

- 組織内CSIRT要員への継続的なトレーニングにより、ヒューマンスキル、テクニカルスキルと先進的な戦術への理解を維持・更新する
  - ヒューマンスキル、テクニカルスキル
    - CSIRT要員のベースライン・スキルを確保
  - 脅威、攻撃手法、戦術に関する知識
    - さまざまな攻撃手法と防御策への理解
    - 最新のセキュリティツール(SIEM、UTM等)の知識
    - 攻撃者プロファイルやインディケータ等、外部連携に必要な情報
    - インシデントの性質による対応手順の違いへの理解
    - ログの取得や保存に対する理解

4-5. 訓練・演習の実施

- 組織内CSIRTを含む、インシデント対応に関与する部門・部署を対象に、インシデント発生時を想定した訓練と演習を定期的に実施する
- 訓練と演習の実施により、トレーニングの成果を実践し、要員、プロセス、技術に求められるレベルと実際の能力とのギャップを認識することができる



5．組織内CSIRTの形態

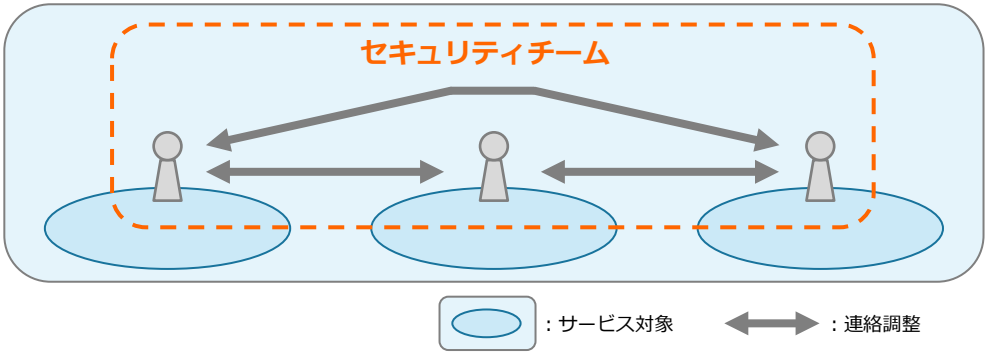
5-1. 組織内CSIRTの形態の分類

- セキュリティチーム
  - Security Team
- 分散型 CSIRT
  - Internal Distributed CSIRT
- 集中型 CSIRT
  - Internal Centralized CSIRT
- 統合（分散／集中）型 CSIRT
  - Internal Combined Distributed and Centralized CSIRT
- 調整役 CSIRT
  - Coordinating CSIRT

※参照元：Organizational Models for Computer Security Incident Response Teams (CSIRTs)
http://www.cert.org/archive/pdf/03hb001.pdf

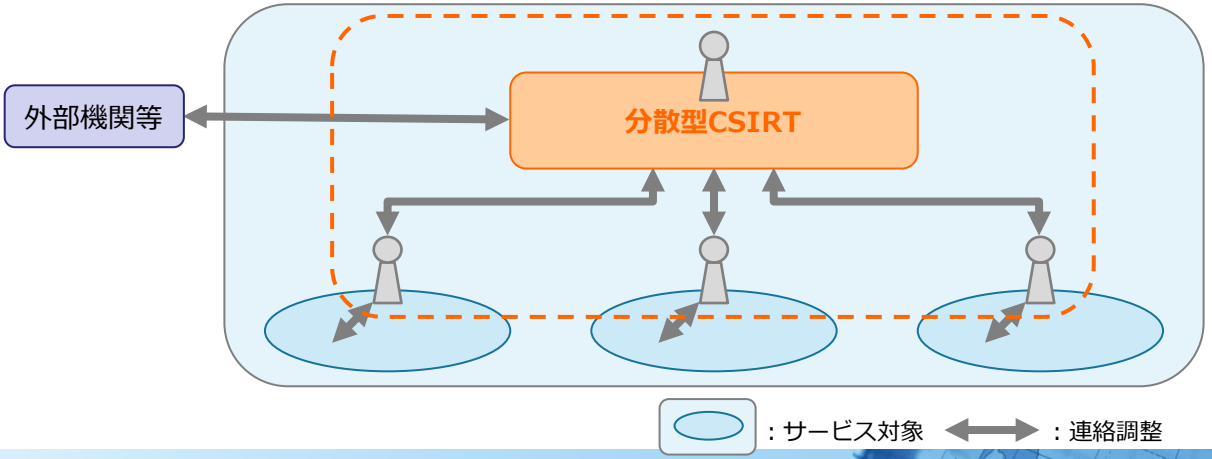
セキュリティチーム

- 正式にCSIRTとして組織化されていない（既存のＩＴエンジニア等を活用）
- システム管理者、ネットワーク管理者などの職務の一部として、セキュリティインシデントへの対応を行う
- 組織全体に及ぶインシデントへの対応が難しい
- 組織全体から情報を集めたり、平時より最新の脅威情報を収集して組織への影響度を考察し報告するような機能を持たない
- “Business as usual”（いつもどおり）のアプローチであり、インシデント対応としては極めて限定的な活動となる
- 組織内において、CSIRTとして認知されていないことが多い



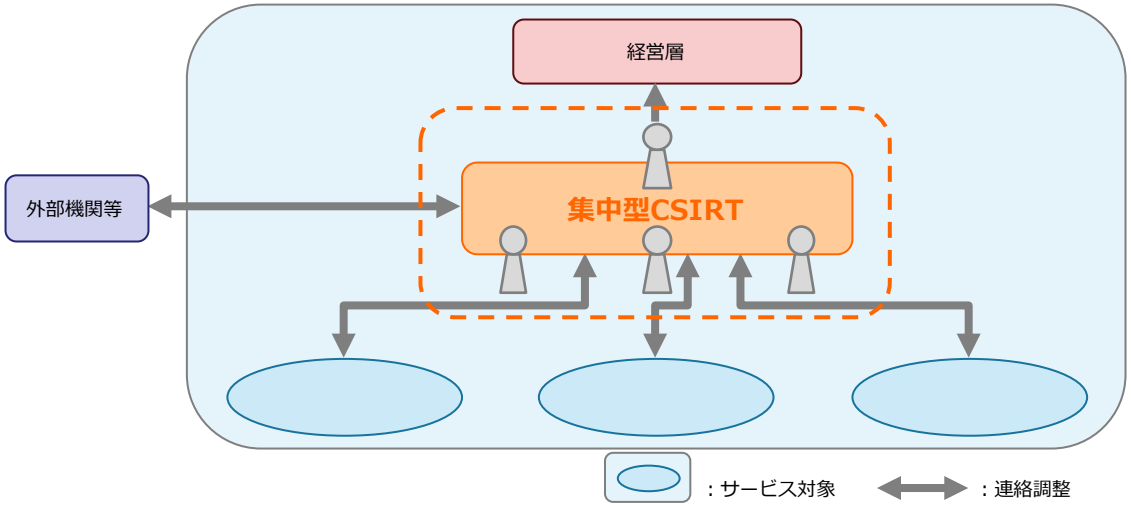
分散型 CSIRT

- 一部またはすべての下位組織の中に、仮想的に（場合によっては兼務で）CSIRTのスタッフを任命する
- 一人の責任者（マネージャー）が、監督と調整役を担う
- スタッフは、それぞれの担当エリアをベースにしながら、インシデント発生時にはCSIRTのスタッフとして活動をする。また、何人かは専任のCSIRTスタッフとして活動する
- このタイプのCSIRTは、外部から見たこの組織の SPOC（Single Point of Contact:単一窓口）としての機能を持つ



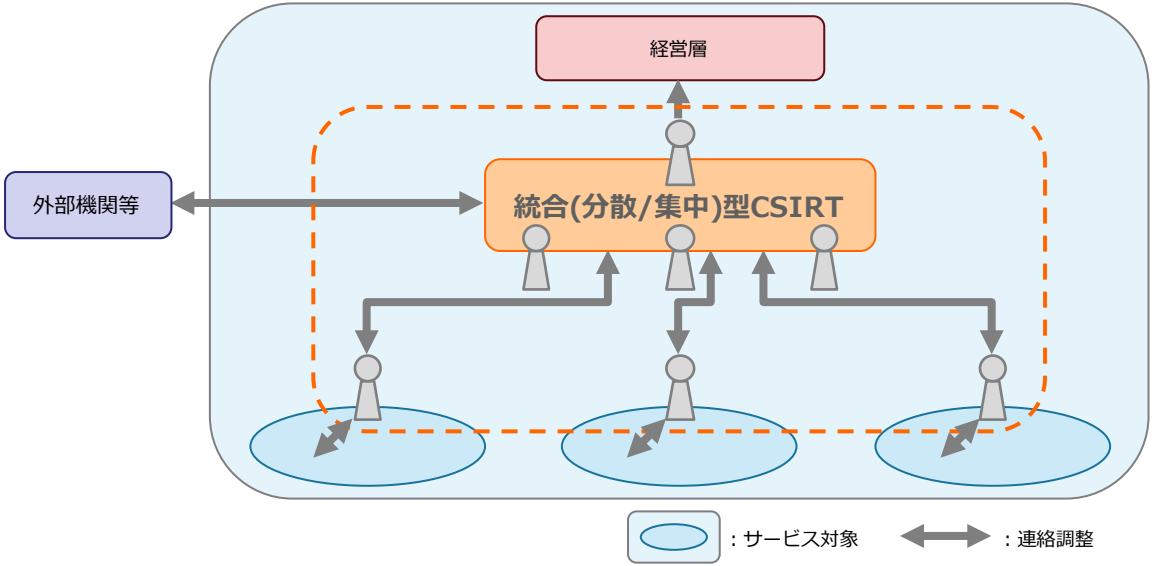
集中型 CSIRT

- 主として専任のスタッフで構成されるが、下位部署との兼務者を含む場合がある
- 責任者（マネージャー）は経営層（CIO など）に対する報告義務を伴う
- 正式に組織化され、組織内で発生するすべてのインシデントへの対応に責任を持つ
- このタイプのCSIRTは、外部から見たこの組織の POC としての機能を持つ



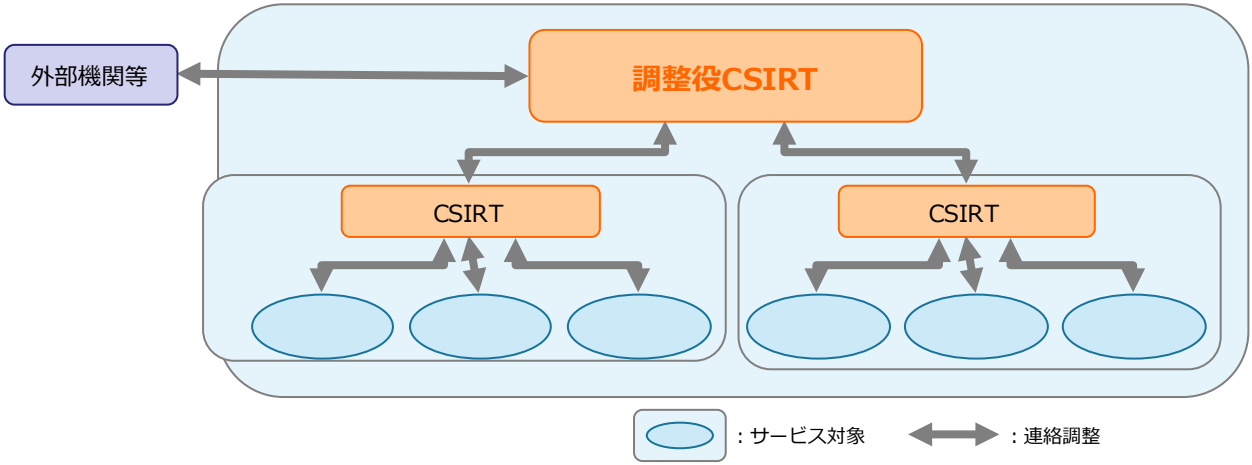
統合（分散／集中）型 CSIRT

- 分散型と集中型を合わせた CSIRT
- 組織全体に及ぶセキュリティインシデントに対応できる体制を整えるために既存の社員を最大限に活用する
- CSIRTが中心となり、下位組織を統括し調整する
- このタイプのCSIRTは、外部から見たこの組織の POC としての機能を持つ



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をしたり、その環境を構築する役割を担うCSIRT
- 広範でさまざまなサービス対象を持つ
- 他の組織のインシデントレスポンスを支援するための連絡調整も行う



5-2. 組織の実情に合わせたCSIRTの選択 1

「セキュリティチーム」を選択する組織

- インシデント対応を専門に担当する部署がない
- 既存のIT部門やセキュリティグループ等のメンバーが、通常業務の一部としてセキュリティインシデントを扱う
- インシデントが発生する都度、チームが結成され、比較的現場に近いところで対応をする

5-2. 組織の実情に合わせたCSIRTの選択 2

「統合（分散／集中）型」を選択する組織

- CSIRTがサービス対象と同じ組織内に存在する
- 最も優先すべき活動が、インシデント対応、またはインシデント対応の支援である
- インシデント対応あるいはその支援に対して、特別な権限が与えられている

5-2. 組織の実情に合わせたCSIRTの選択 3

「調整役」を選択する組織

- インシデント対応に必要な情報を取りまとめ調整することによって、実際のインシデント対応に役立つ情報の流通を図る機能がある
- インシデントに関する情報の調整やインシデント対応活動に関するノウハウの提供などを実施している
- インシデントが発生した現場で実際に対応することは少ない

（参考） さまざまなCSIRTの名称

- CSIRT
  - Computer Security Incident Response Team
- CSIRC
  - Computer Security Incident Response Capability
- CIRC
  - Computer Incident Response Capability
- CIRT
  - Computer Incident Response Team
- IHT
  - Incident Handling Team
- IRC
  - Incident Response Center
  - Incident Response Capability
- IRT
  - Incident Response Team
- SERT
  - Security Emergency Response Team
- SIRT
  - Security Incident Response Team