JPCERT CC®

組織内 CSIRT の役割とその範囲

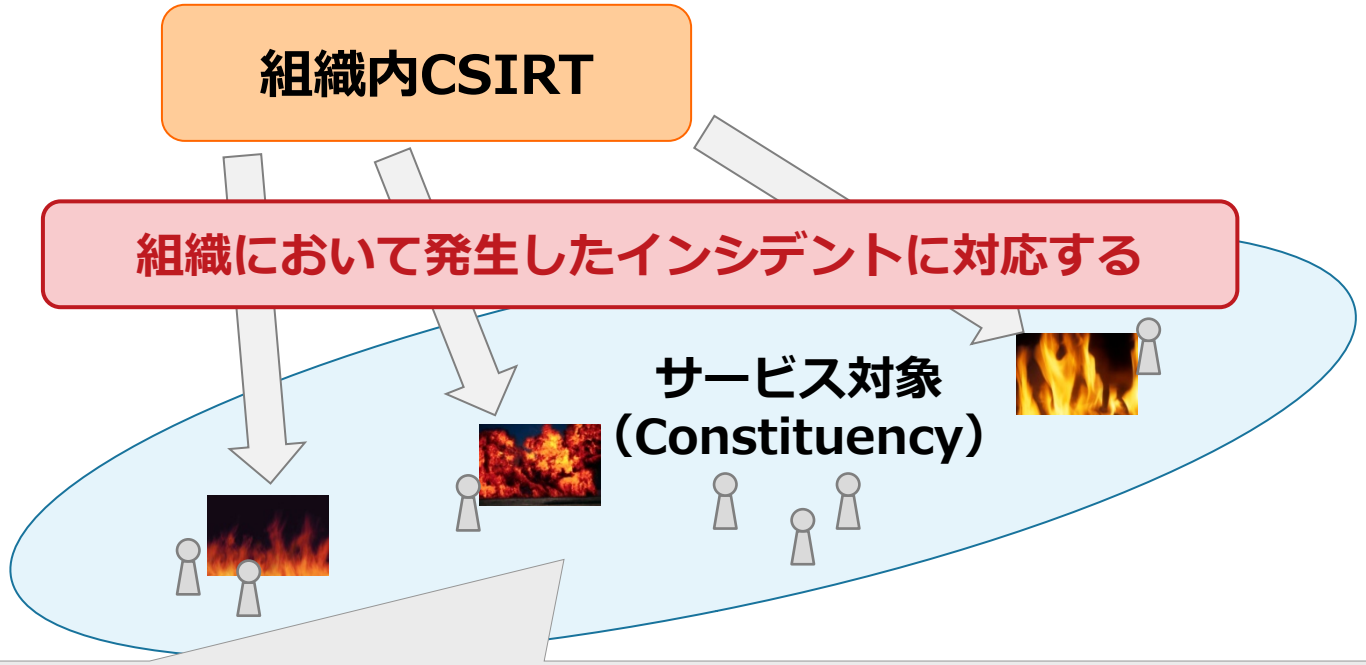
一般社団法人
JPCERT コーディネーションセンター

目 次

- 組織内 CSIRT の基本的な役割
- 組織内 CSIRT の役割範囲には違いがある
- インシデント対応の重要ポイントから見る役割
  - 「ユーザからのインシデント報告」
  - 「外部のインシデント対応チームとの連携」
  - 「インシデント関連情報の伝達経路の保全」
  - 「他組織のCSIRTとの情報共有」
- 組織内 CSIRT の役割の定義
- 組織内 CSIRT の役割
- 組織内 CSIRT の役割の例
  - インシデントへの「直接」対応
  - インシデントへの「支援的」対応
  - インシデントへの「調整役としての」対応
- 組織内 CSIRT の役割の重要性
- CSIRT の役割の説明に役立つ資料
  - CSIRT と消防署の類似例の活用
  - CSIRT の概念が作られたきっかけ

組織内 CSIRT の基本的な役割

- 組織内 CSIRT の基本的な役割



サービス対象（Constituency）とは：

組織内CSIRTのサービス（インシデント対応、インシデント対応に必要な技術的支援など）を提供する対象のこと。サービス対象者の例としては、以下の全部あるいは一部を定義することが多い。

・システム管理者およびネットワーク管理者
・全社員
・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）

組織内CSIRTの役割範囲には違いがある

- 組織の事業内容、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

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」を行なうための重要なポイントは、以下のとおり
  - 「ユーザからのインシデント報告」
    - サービス対象（一般ユーザなど）から、発生したインシデントが組織内CSIRTに報告されること
  - 「外部のインシデント対応チームとの連携」
    - 外部のインシデント対応チームが、どのように対応するかを理解した上で、適切な依頼をすることができる関係になっていること
  - 「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やり取りは、通常のインターネット回線を使用することが多いため、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こと
  - 「他組織のCSIRTとの情報共有」
    - 他組織のCSIRTと相互補完的な関係になり、同一攻撃者からの攻撃をブロックできること

インシデント対応の重要ポイントから見る役割

「ユーザからのインシデント報告」

- 「ユーザからインシデント報告」を受けるためには、以下のことが必要である
  - サービス対象（一般ユーザなど）が、インシデントを報告する必要を知っていること

    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

  - サービス対象が、組織内 CSIRT がどんな目的で、何をするところなのかを知っており、理解していること

    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

  - サービス対象が、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こと

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

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」

- 適切に「外部のインシデント対応チームとの連携」を図るには、以下のことが必要である
  - 外部のどこのインシデント対応チームに対して、何が依頼できるかを知っていること

組織内 CSIRT は、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

  - 外部のインシデント対応チームに対して、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）があること

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

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の保全」を確保するには、以下のことが必要である
  - サービス対象（一般ユーザなど）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、なりすまし及び改ざんさ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、その情報の完全性及び信頼性に関して確認する手段を提供する

  - サービス対象及び外部のインシデント対応チームとのやり取りが第三者に盗聴されていないこと

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こと

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」をするには、以下のことが必要である
  - 攻撃者のプロファイルやインディケータといったAPT攻撃の予防・発見に役立つ情報が共有できる状態にあること

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と情報共有する際には、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ようにすること

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

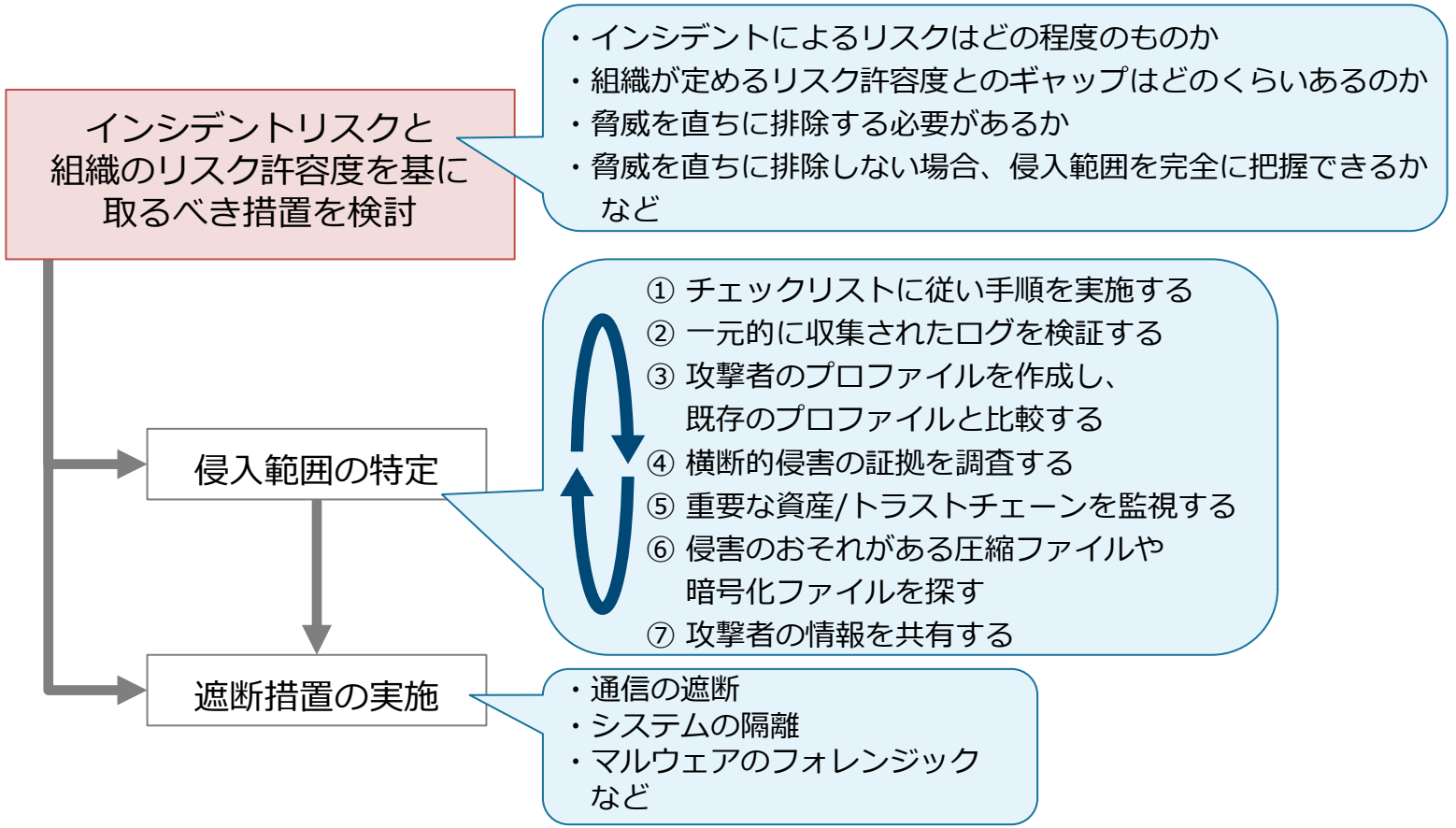
組織内 CSIRT の役割の定義

- 組織内 CSIRT の役割（インシデント対応）の範囲は、組織の状況をもとに、**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 に対する期待で多く見られるものは以下のとおり
  - 組織内に「インシデント対応能力をつける」こと
    - 組織内においてインシデントに対応する部門や人が決まっていないため、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
  - 「組織的なインシデント対応能力」を向上させること
    - 特定の部門でインシデント対応するところはあるが、必ずしも組織全体として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、組織全体としての統制をとるチーム設けたいという期待
  - 「外的要因のインシデント」への対応能力をつけること
    - DoS 攻撃やAPTによる攻撃のような外部要因のインシデントに対応する部門が決まっていないため、外部及び内部の部門と**「調整して」対応**する部門を設けたいという期待

組織内 CSIRT の役割

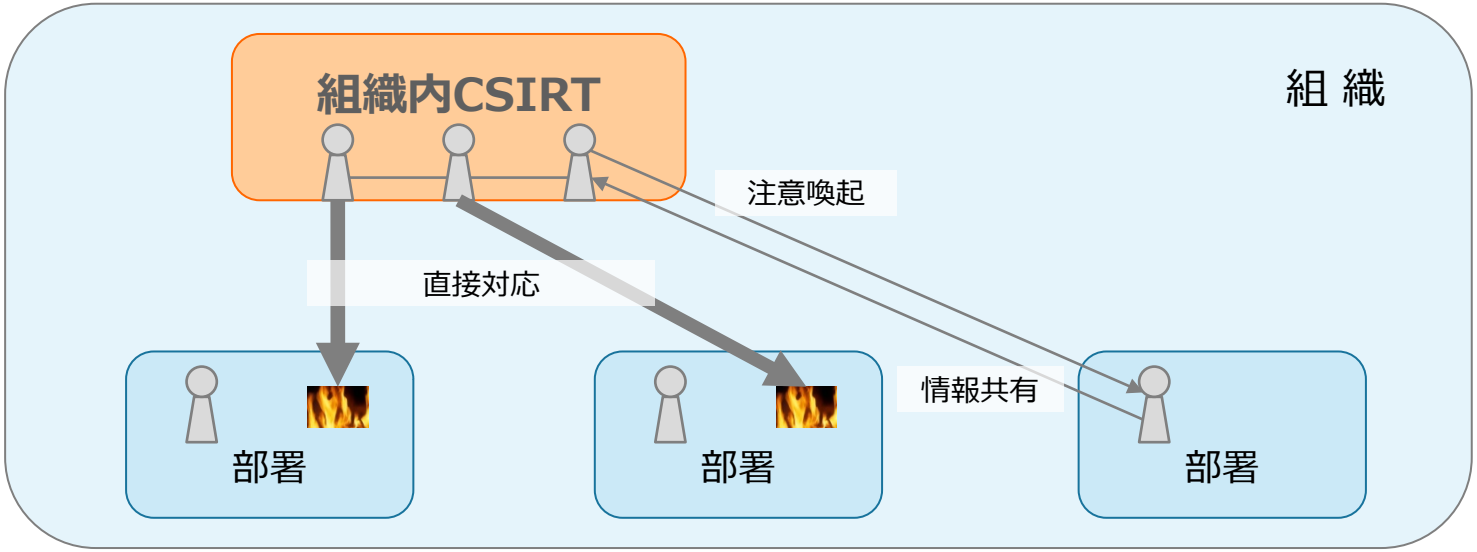
- 組織内 CSIRT の役割（インシデント対応）は、発生したインシデントリスクと組織のリスク許容度により変化する



組織内 CSIRT の役割の例

インシデントへの「直接」対応

- 組織における<u>インシデント対応能力が十分ではない</u>ので、「組織内CSIRT」に**<u>主として／直接</u>**インシデント対応をさせることを期待する場合の例：

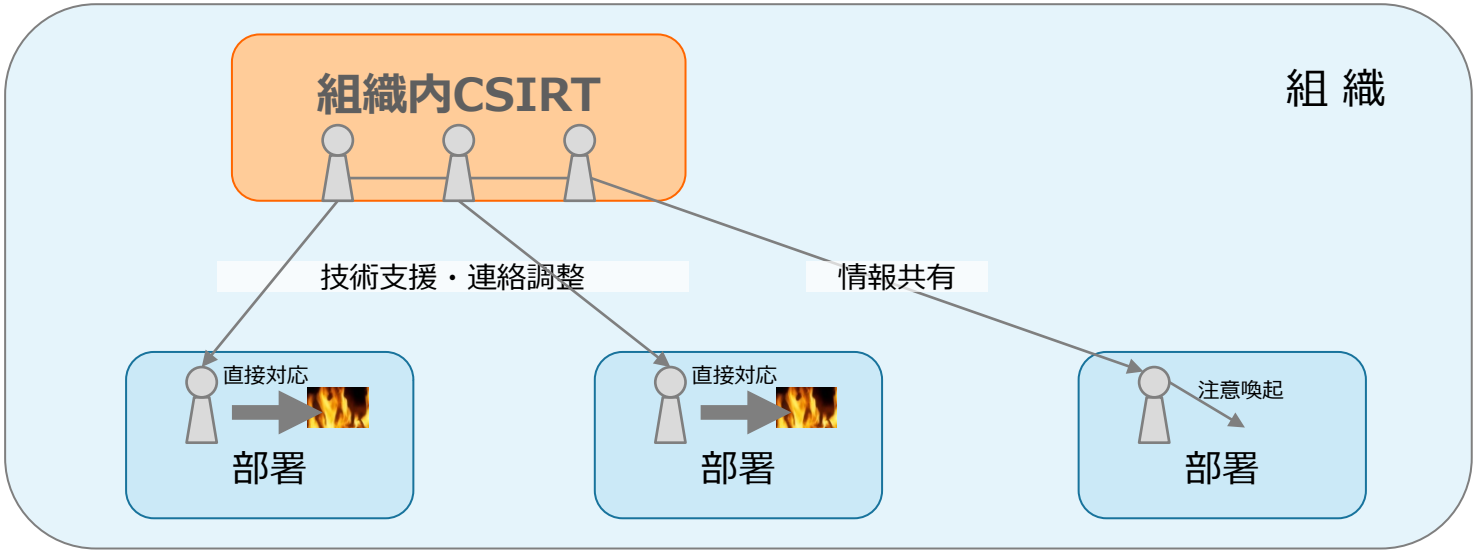


- 責務と使命の例：
  - 組織内 CSIRT は、組織内で発生したコンピュータシステム及びネットワークなどで発生するインシデントの被害を局限化し、迅速な復旧を実施する
  - 組織内 CSIRT は、インシデントが早期に発見され、迅速に対応できる仕組み（各部署等との情報共有及び連携など）を整備し維持する

組織内 CSIRT の役割の例

インシデントへの「支援的」対応

- 組織において、既に部門内で発生するインシデントへの対応能力はあるが、組織全体で（各部署を横断して）はインシデントの対応能力が十分ではないので、「組織内CSIRT」に その **発生したインシデント対応の支援及び調整** を期待する場合の例：

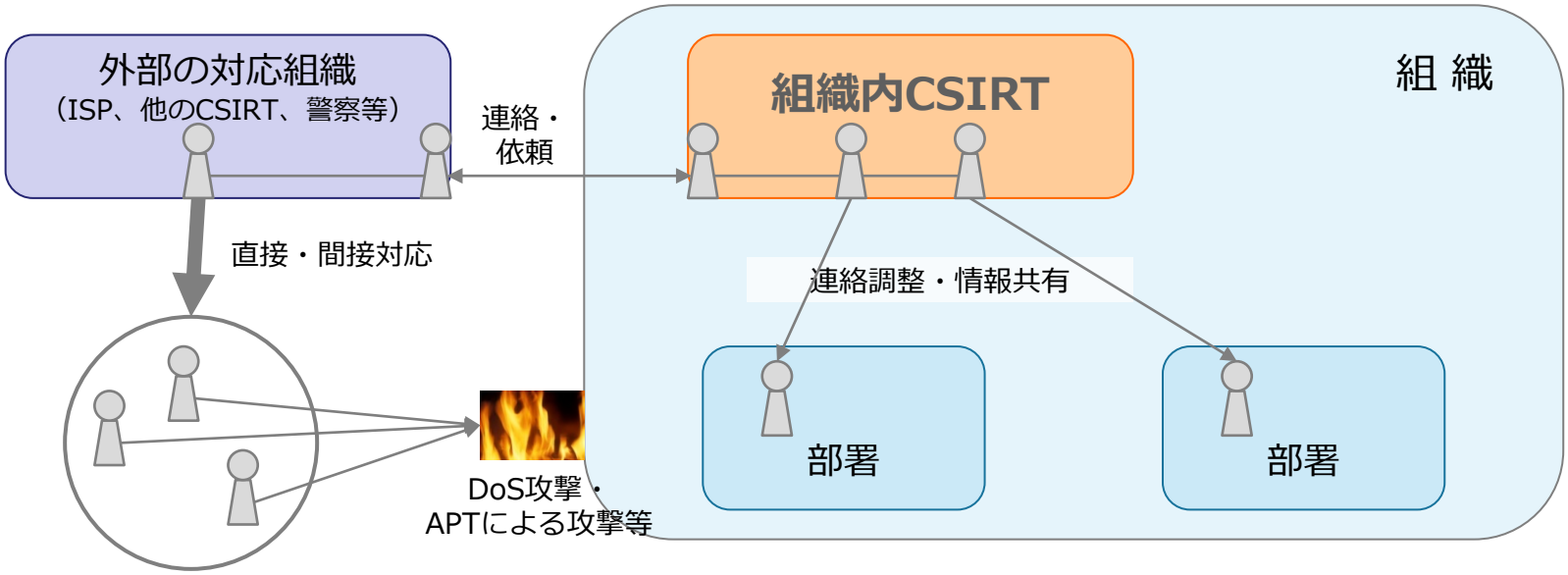


- 責務と使命の例：
  - 組織内 CSIRT は、組織内で発生したインシデントへの（各部署等による）対応活動に対して、技術的支援および組織内全体の調整、統制等をすることにより、迅速な被害の局限化及び迅速な復旧を支援する

組織内 CSIRT の役割の例

インシデントへの「調整役としての」対応

- 組織において、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ので、「組織内 CSIRT」にその**インシデントへの対応及び調整と、それに必要な組織内外への調整**を期待する場合：



- 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及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

組織内 CSIRT の役割の重要性

- 組織内においてインシデント対応をとることが可能な（既存の）チームが存在している

  - ネットワーク運用・・・主に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・・・主にホストのセキュリティに関する対応
  - 情報セキュリティ管理・・・組織全体のポリシーや手順の違反に関する対応

- 必然的に組織が課題として考えること

  - 既存のチーム同士のインシデント対応は連携しているか？
  - 組織全体としてのインシデント対応となっているか？
  - 外部とやり取りをする場合、それぞれのチームは、組織の窓口としての一貫性を保つことができるか？
  - 発生したインシデントが、本当に報告されるか？

組織内 CSIRT がこれらの役割を果たす

CSIRT の役割の説明に役立つ資料

CSIRT と消防署の役割の比較例

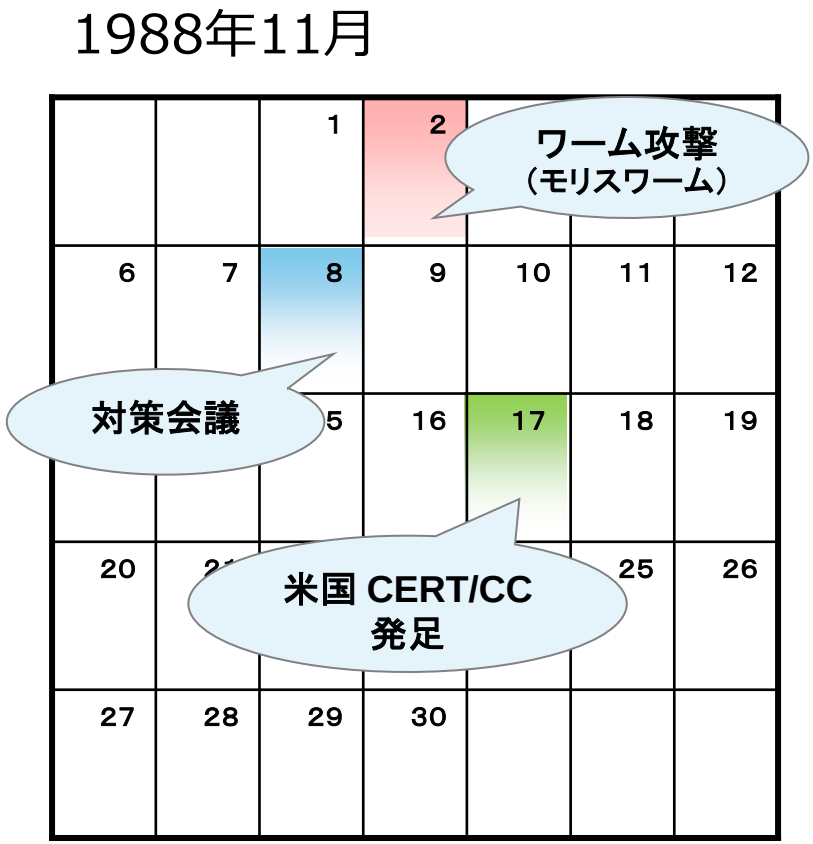
CSIRT の場合（例）

- 発生したインシデント対応
  - 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
    - 被害の極限化策の実施（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、ウィルス除去、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
    - 消火活動及び救出活動
- 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の呼びかけ

CSIRT の概念が作られたきっかけ



- 1988年、米国において、モリスワームというワームが、今で言うところのインターネットで発生し、当時のネットワーク全体に多大な被害を与えた
- その後、対策を検討した結果、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及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)
http://www.cert.org/archive/pdf/csirt-handbook.pdf