JPCERT CC®

組織内 CSIRT の必要性

一般社団法人
JPCERT コーディネーションセンター

目次

- インシデントとは
- インシデント対応（活動）とは
- インシデント対応活動の必要性
  - 完全な予防策はない
  - 取り巻く環境の変化
- インシデント対応体制を設置する意義
  - インシデント対応体制について
  - 組織的なインシデント対応体制に求められる主な機能
  - インシデント対応体制を構築すべき時期
  - 事前のインシデント対応計画の策定
- 組織内 CSIRT の必要性
  - インシデント対応体制と組織内 CSIRT
  - 組織内 CSIRT の機能
  - 組織内 CSIRT のメリット
- 組織内 CSIRT 構築の推奨とその広がりについて

（参考）組織内 CSIRT の構築に役立つ資料

（参考）高度サイバー攻撃(APT) の 定義

インシデントとは

- 一般的な「インシデント」とは
  - 重大な事故に至る可能性がある出来事をいう

- 情報セキュリティの分野での「インシデント」とは
  - IT システムの正常な運用または利用を阻害するウィルス感染、不正アクセス、情報漏えい、DoS 攻撃などの事案や現象の発生をいう

インシデント対応（活動）とは

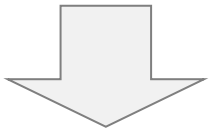
- インシデントを検知し、或いはその報告を受けることにより認知し、影響の拡大を防ぐとともに、情報を収集して分析を加え、インシデントの全体像や原因について把握し、復旧措置や再発防止のための措置を取る一連の活動

業務の多様性及び複雑性の状況や、それに伴うセキュリティコントロール（技術面、運用面、管理面）の難しさが見られるようになってきた

インシデント対応活動の必要性
完全な予防策はない

- 「コンピュータセキュリティ」で思い描くイメージ
  - 「いかにしてインシデントの発生を未然に防ぐか」を主眼に置かれることが多い

- コンピュータ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
  - 社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（インシデントの発生は避けられない）

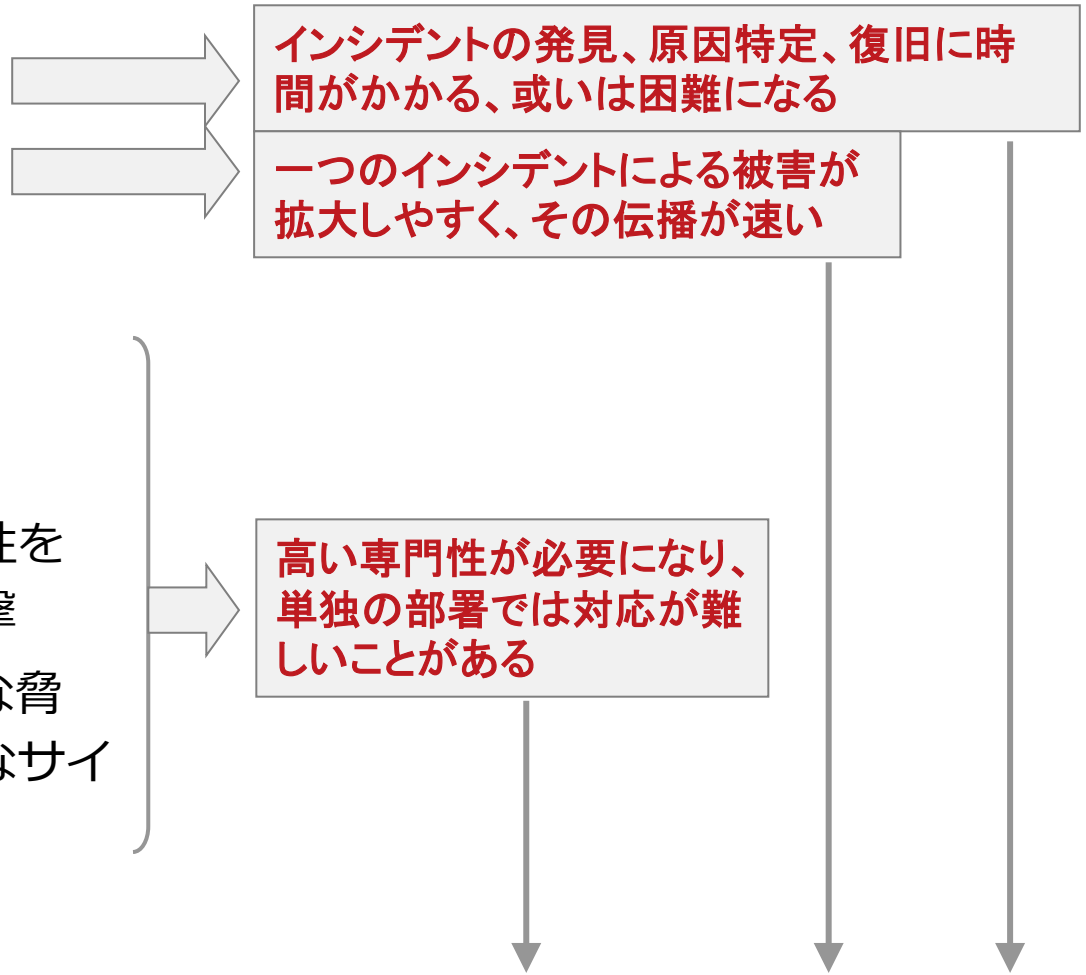
（発生確率を低下させ、発生時の影響や被害を低減するための予防策はある）

インシデント対応活動の必要性

取り巻く環境の変化

- 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

- 攻撃の変化
  - 攻撃の潜在化
  - 攻撃手法の高度化
  - ソフトウェアの脆弱性を使用したゼロデイ攻撃
  - APT（先進的で執拗な脅威）と呼ばれる高度なサイバー攻撃の増加



組織的なインシデント対応活動が必要に！

インシデント対応体制について

- 組織的なインシデント対応活動を実現するためには
  - 組織内におけるインシデント対応活動に関する機能要素を見出す
    - インシデントを発見する要素、インシデントを報告する要素、インシデントの報告を受ける要素、・・・・

  - その機能要素を有機的に結びつける
    - 各要素の役割や機能の設定、各要素間のインタフェース及びコミュニケーションの確立、・・・・

  - 全体として、統一性及び一貫性のある状態にする

組織的なインシデント対応体制の構築へ

インシデント対応体制を設置する意義

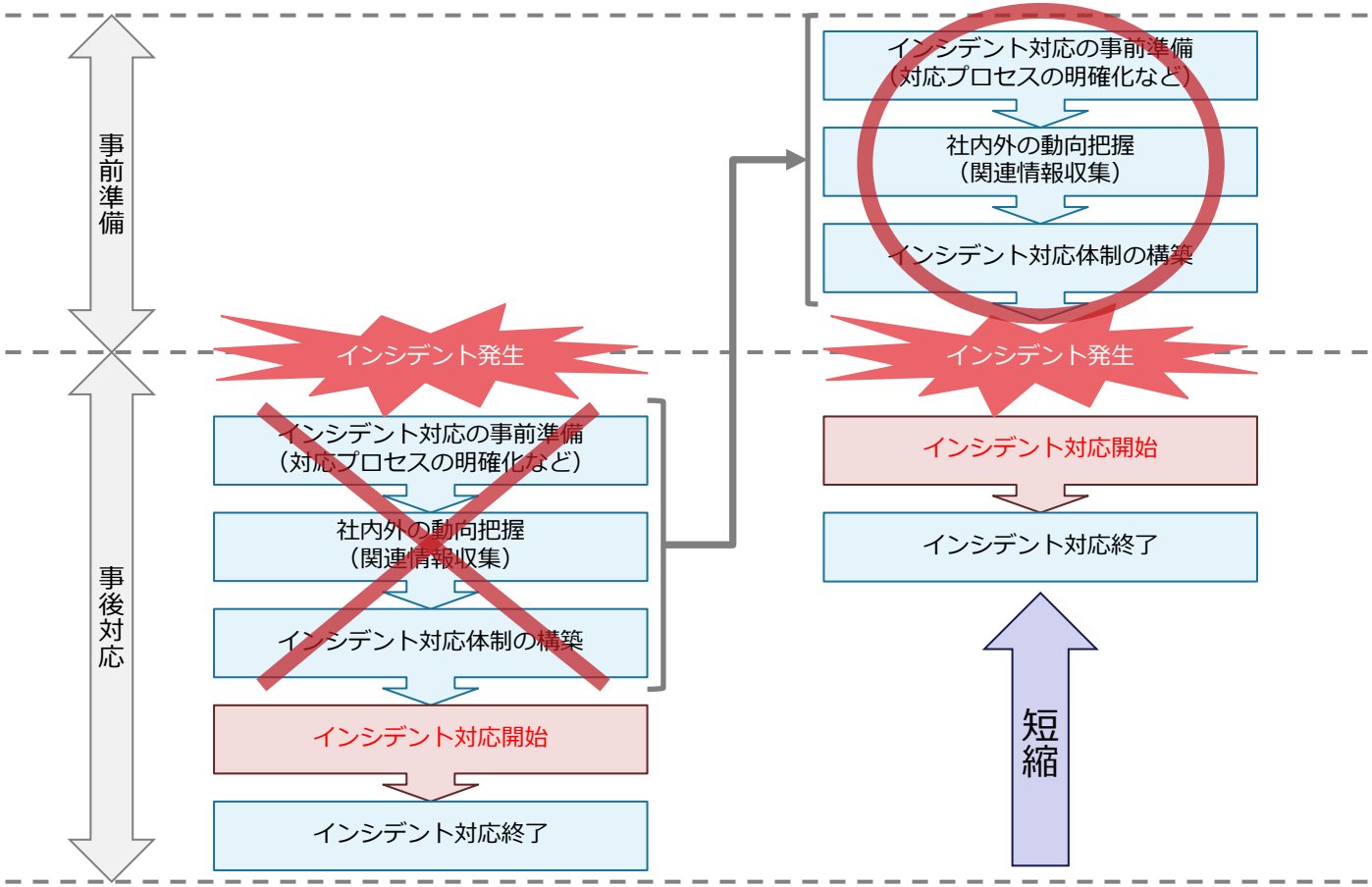
組織的なインシデント対応体制に求められる主な機能

- 組織内の情報共有及び連携
  - 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
  - 外部に起因するインシデント（DDoS、高度サイバー攻撃(APT)による攻撃など）を解決するため、他組織に対する適切な依頼
  - 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
  - 組織間で連携しなければならないインシデント対応のため、外部組織との強い信頼関係の構築

インシデント対応体制を設置する意義

インシデント対応体制を構築すべき時期

- インシデント発生後に、その対応方法を考え始め対応体制をとるのは、被害を拡大させる一因となるため、できるだけ**事前に対応体制等を整えておく**必要がある



インシデント対応体制を設置する意義

事前のインシデント対応計画の策定

- インシデント対応体制の構築には、事前のインシデント対応計画の策定が重要である

- 組織的なインシデント対応計画を策定するためのポイント
  - 複雑化するネットワーク及びシステムの把握
  - 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
  - インシデント対応に必要なポリシー及びマニュアル等の整備
  - 外部組織に依頼する場合の、外部の対応能力の把握と適切な報告
  - リスク評価の実施とリスク許容度の設定

インシデント対応体制と組織内 CSIRT

- 組織内 CSIRT について
  - Computer Security Incident Response Team の略、「シーサート」と発音される
  - 組織内でコンピュータセキュリティインシデント対応に関する業務を専門に担当するチーム
  - 組織によっては、他の関連業務と兼務することによって、組織内に CSIRT の機能を実装している場合もある

組織的な「インシデント対応体制」のベストプラクティス（最善策）

＝

組織内 CSIRT

組織内 CSIRT の機能

- 組織の内部に対する主な機能
  - 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、発生したインシデントへの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として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
  - 組織の情報システム管理者、ユーザ、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機能
  - 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外部から収集し、組織内に展開する
  - 従業員・メディア・国民へ適切な情報を提供する

組織内 CSIRT のメリット

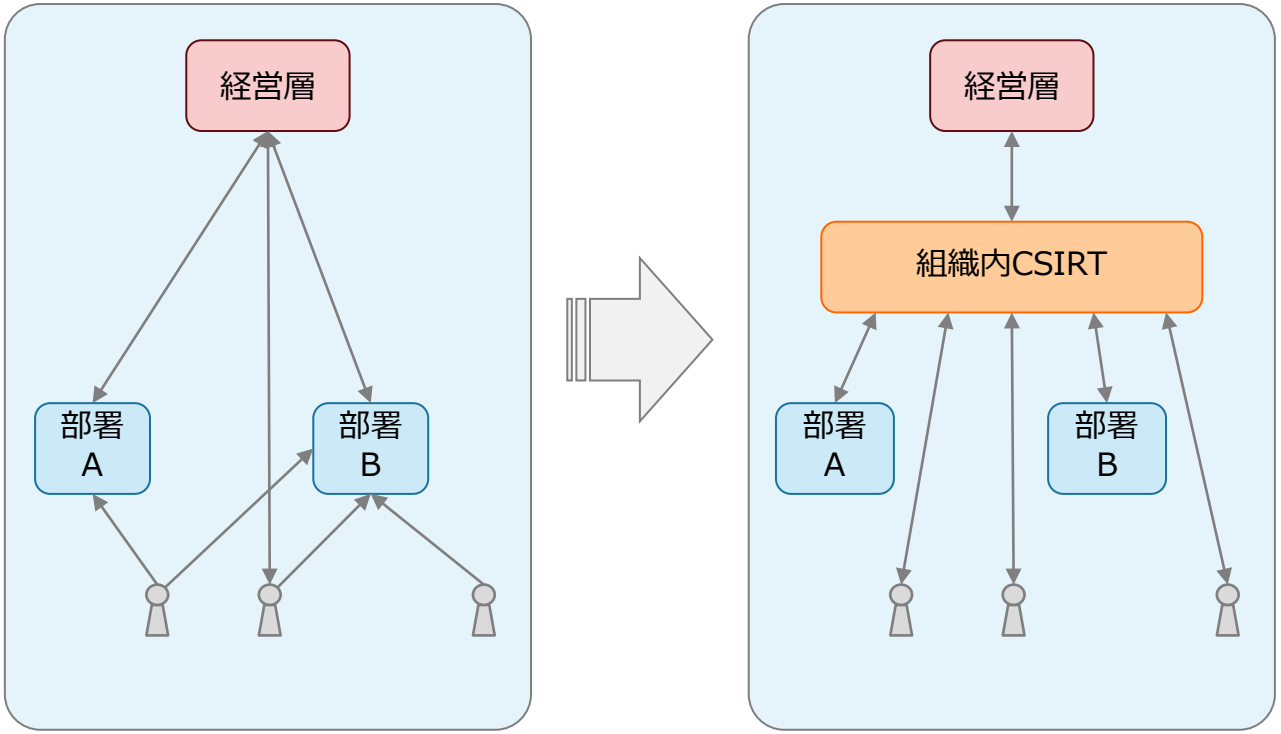
- 組織内 CSIRT を構築するメリットは、組織によって大きく異なるが、多く見られるメリットの例は以下のとおり

  - 情報セキュリティ（インシデント）に関する情報を一元的に管理する
  - 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
  - 外部組織との信頼関係を構築することにより、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

※次の３つのスライドで、それらのイメージを示す

組織内 CSIRT のメリットのイメージ 1

- 情報セキュリティ（インシデント）に関する情報を一元的に管理する



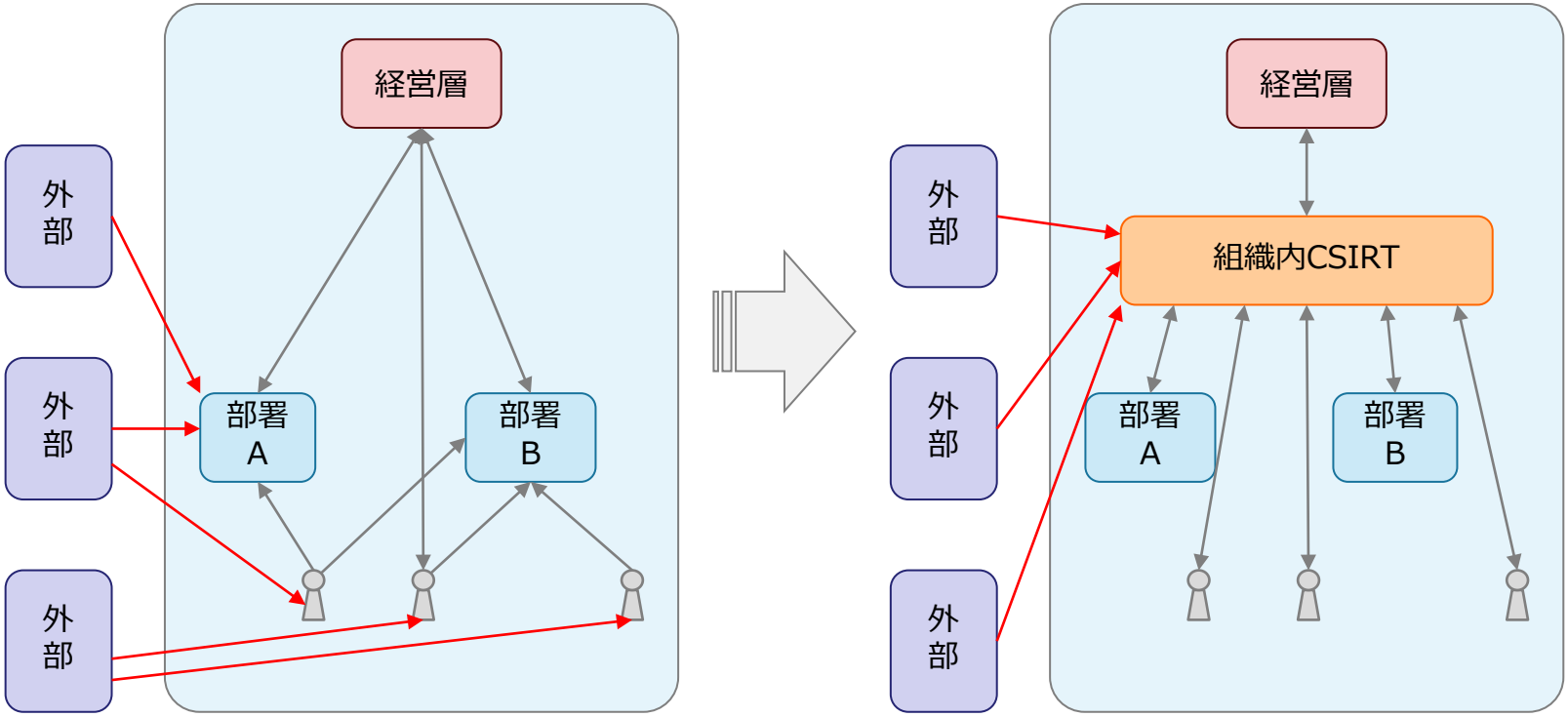
メリットの例：

①組織内のセキュリティ情報の共有、集中管理の実現

②セキュリティ対応に係る指示系統の迅速化（ダイレクトリーチ）

組織内 CSIRT のメリットのイメージ 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



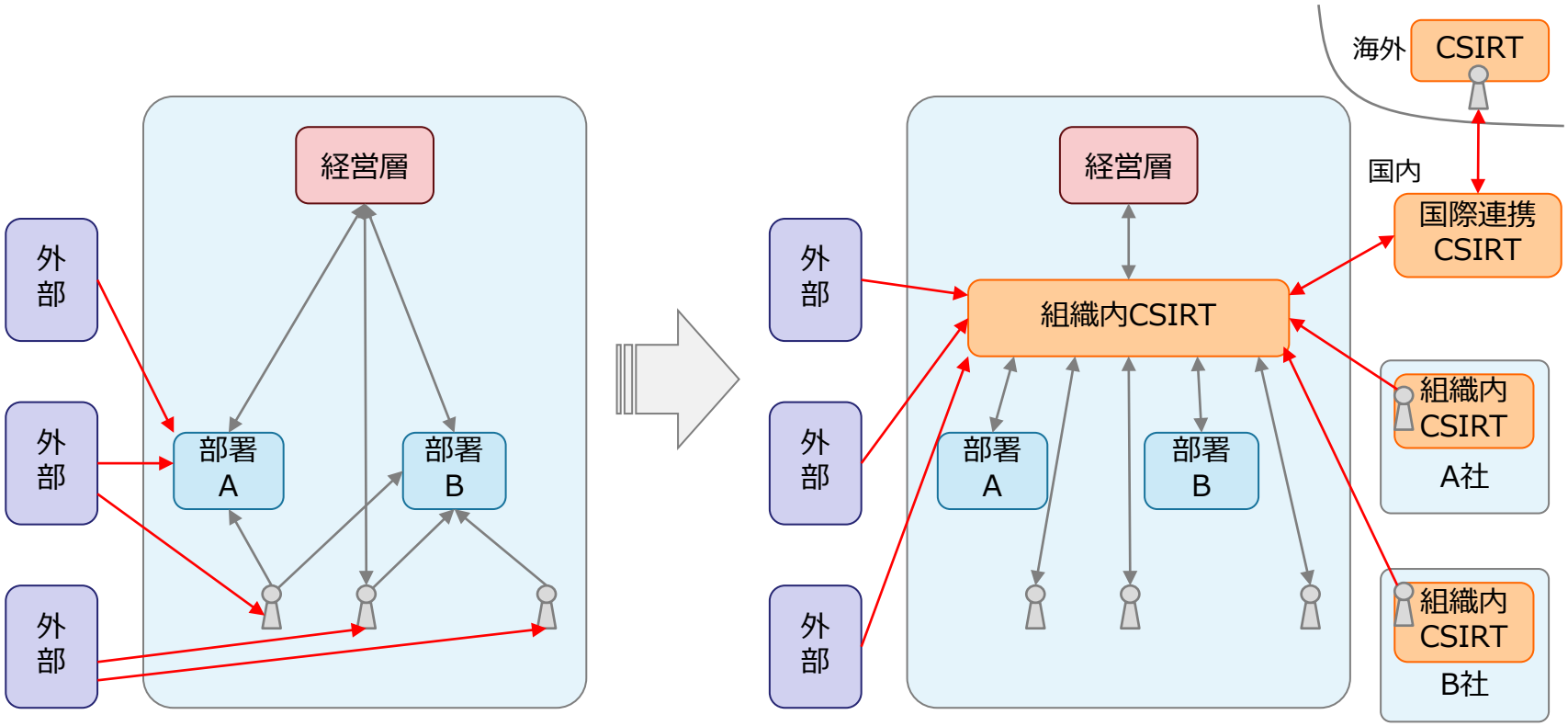
メリットの例：

①外部に対して信頼性のある窓口の提供

②外部からの情報の一元管理の実現

組織内 CSIRT のメリットのイメージ 3

- 外部組織との信頼関係を構築することにより、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



メリットの例：

①インシデントレスポンスに必要な情報量の向上

②想定外（予想外）のインシデントへの柔軟な対応

組織内 CSIRT 構築の推奨とその広がりについて

- 組織内 CSIRT を構築することを強く推奨する
  - 組織においてインシデントによる被害の局限化と迅速な復旧を図るための「組織的なインシデント対応体制」のベストプラクティス（最善策）として
  - 外部のインシデント対応チームと連携するための有効な手段として

- 組織内 CSIRT の構築の広がり
  - 組織的なインシデント対応体制の最善策として、世界各国の組織で構築が進められている
    - FIRST（インシデント対応チームの世界的なフォーラム）
      http://www.first.org/
    - APCERT（アジア太平洋地域における National CSIRT のフォーラム）
      http://www.apcert.org/
    - TF-CSIRT（ヨーロッパにおける CSIRT のフォーラム）
      https://www.terena.org/activities/tf-csirt/
    - 日本シーサート協議会
      http://www.nca.gr.jp/

（参考）組織内 CSIRT の構築に役立つ資料

- JPCERT/CCにおける関連文書
  - 組織内 CSIRT 構築支援マテリアル
    - http://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
    - http://www.jpcert.or.jp/research/2007/CSIRT_Handbook.pdf

- その他の参考資料
  - 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
    - http://www.nca.gr.jp/activity/build-wg-document.html
  - CERT/CC – “Creating a Computer Security Incident Response Team: A Process for Getting Started”
    - http://www.cert.org/csirts/Creating-A-CSIRT.html
  - TERENA – “CSIRT Starter Kit”
    - http://www.cert.org/csirts/Creating-A-CSIRT.html
  - AusCERT – “Forming an Incident Response Team”
    - http://www.auscert.org.au/render.html?it=2252
  - RFC 2350 – “Expectations for Computer Security Incident Response”
    - http://www.ietf.org/rfc/rfc2350.txt

（参考）高度サイバー攻撃
APT（Advanced Persistent Threat：先進的で執拗な脅威）

- 高度サイバー攻撃(APT)によるものとされる攻撃では、攻撃者は、標的とする企業や組織に対し、洗練された高度な手法を用い、戦略的かつ組織的に、また長期間にわたって攻撃活動を行い、金銭や知的財産、その他企業の競争上の強みとなる情報を窃取する。

- 高度サイバー攻撃(APT)の特徴
  - 明確で長期的な目的を持つ
  - 潤沢なリソースと整備された攻撃インフラ
  - 攻撃対象企業・組織に対するインテリジェンス能力を備える
  - 技術、ソフトウェアを臨機応変に用いる
  - 侵入検知、インシデント対応の動きに迅速に対応する

- 組織が高度サイバー攻撃(APT)によるインシデントに対応するには、他の一般的なセキュリティインシデントとは異なる対応が必要となる
  - 攻撃者の活動を追跡するための長期間に渡る各種ログの保管
  - 信頼できる外部組織との間で、攻撃関連情報（インディケータ）を共有し、侵入の検知と対応に利用する