学術機関におけるCSIRT活動

大阪府立大学
大学院 人間社会システム科学研究科 教授
学長特別補佐（情報システム，情報セキュリティ担当）

宮本 貴朗

組織におけるCSIRTの役割（１）

大阪府立大学
OSAKA PREFECTURE UNIVERSITY

- CSIRTの活動
  - 平常時の活動
    - 脆弱性情報，攻撃予兆情報などのインシデント関連情報の収集・分析
    - インシデント対応方針や対応手順の策定
    - 教育・啓発活動
  - インシデント発生時の活動
    - インシデントマネジメント
  - 事後対応を含めた包括的な対応全般

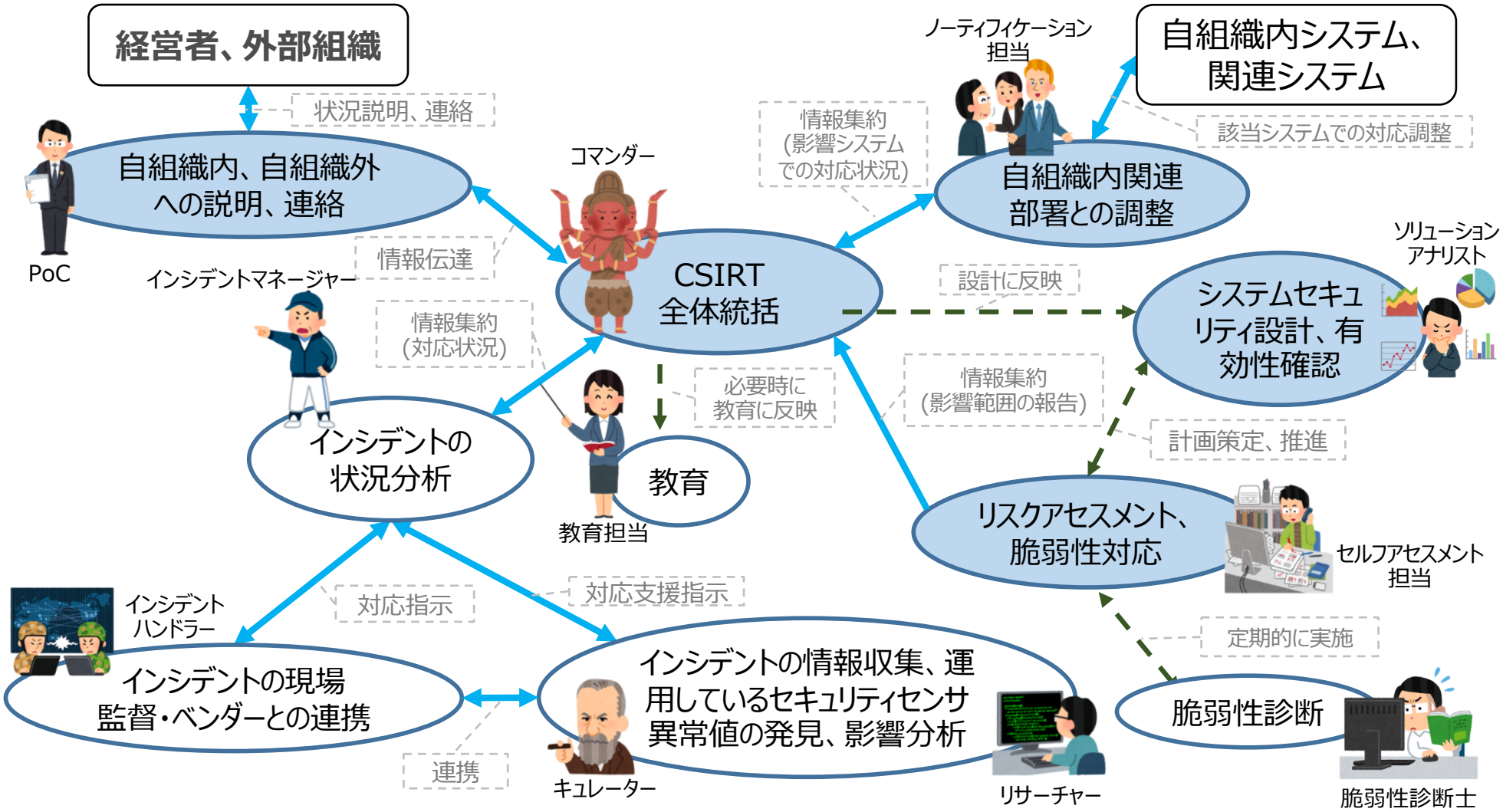
  - CSIRT活動はインシデントマネジメントの中核を担う
    - 事前対応はあくまでCSIRT活動の一部

  - 例えば，
    - 適切にトリアージできるか？
    - 適切に経営層が判断可能な情報を提供できるか？

CSIRTの役割と業務内容の関連図(平常時)

大阪府立大学 OSAKA PREFECTURE UNIVERSITY

実線は活動時の情報の流れ。
点線は必要時に実施する活動の流れ。



＊法的確認や対応方法としてアドバイスが必要な場合には
各役割からリーガルアドバイザーに支援を要請する。

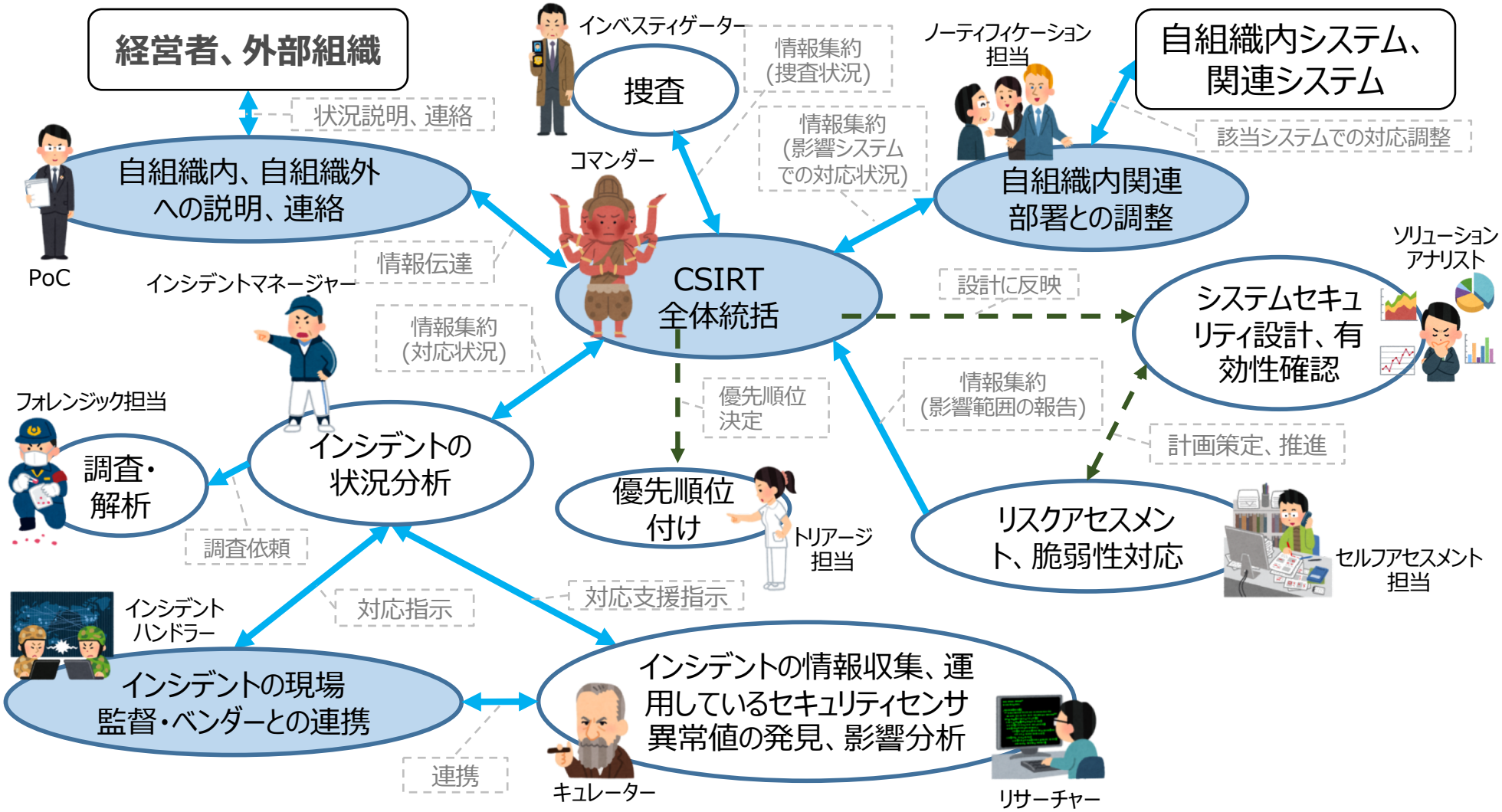
出典：日本シーサート協議会
CSIRT人材の定義と確保 Ver.1.5

CSIRTの役割と業務内容の関連図(インシデント対応時)

大阪府立大学 OSAKA PREFECTURE UNIVERSITY

※インシデントが発生し、CSIRTが対応している状態を「インシデント対応時」と定義

実線は活動時の情報の流れ。
点線は必要時に実施する活動の流れ。



＊法的確認や対応方法としてアドバイスが必要な場合には
各役割からリーガルアドバイザーに支援を要請する。

出典：日本シーサート協議会
CSIRT人材の定義と確保 Ver.1.5

大阪府立大学 OSAKA PREFECTURE UNIVERSITY

- 組織が保有すべきCSIRTの役割とその業務内容

機能分類	役割名称	業務内容
情報共有	社外PoC：自組織外連絡担当	NCA、 JPCERT/CC、CSIRT、警察、監督官庁、等々との情報連携
	社内PoC：自組織内連絡担当、IT部門調整担当	法務、渉外、IT部門、広報、各事業部、等々との情報連携
	リーガルアドバイザー：法務部CSIRT担当	コンプライアンス、法的内容とシステム間の翻訳
	ノーティフィケーション担当：自組織内調整・情報発信担当	各関連部署との連絡ハブ、情報発信
情報収集・分析	リサーチャー：情報収集担当、キュレーター：情報分析担当	定例業務、インシデントの情報収集、各種情報に対する分析、国際情勢の把握
	脆弱性診断士：脆弱性の診断担当	OS、ネットワーク、セキュアプログラミングの検査、診断
	脆弱性診断士：脆弱性の評価担当	OS、ネットワーク、セキュアプログラミング診断結果の評価
	セルフアセスメント担当	平時のリスクアセスメント、有事の際の脆弱性の分析、影響の調査
	ソリューションアナリスト：セキュリティ戦略担当	ソリューションマップ作成、Fit&Gap分析、リスク評価、有事の際の有効性評価
インシデント対応	コマンダー：CSIRT全体統括	CSIRT全体統括、意思決定、社内PoC、役員、CISO、または経営層との情報連携
	インシデントマネージャー：インシデント管理担当	インシデントの対応状況の把握、コマンダーへの報告、対応履歴把握
	インシデントハンドラー：インシデント処理担当	インシデント現場監督、セキュリティベンダーとの連携
	インベスティゲーター：調査・捜査担当	捜査に必要な論理的思考、分析力、自組織内システム理解力を使った内偵
	トリアージ担当：優先順位選定担当	事象に対する優先順位の決定
	フォレンジック担当	証拠保全、システム的な鑑識、足跡追跡、マルウェア解析
自組織内教育	教育担当：教育・啓発担当	自組織のリテラシー向上、底上げ

出典：日本シーサート協議会
CSIRT人材の定義と確保 Ver.1.5

CSIRTに最低限必要な人材（１）

大阪府立大学 Osaka Prefecture University

- PoC（Point of Contact）
  - 自組織（IT部門，法務，渉外，広報，etc.…），他組織との連絡調整
    - 自組織の組織構成
    - 情報を正しく伝えるコミュニケーション能力
    - 情報を適切に判断する能力
    - ITリテラシー
- コマンダー
  - セキュリティインシデント対応の全体統制，CISOやCEOとの情報連携
    - インシデント対応の全体統制を行える能力
    - 自組織のセキュリティ対策，ビジネスに関する知識
    - 自組織のシステム停止，復旧時の業務影響に関する知識
    - 経営層に説明できるコミュニケーション能力
  - PoC とコマンダーは場合により兼務可能

CSIRTに必要な人材（2）

大阪府立大学 Osaka Prefecture University

- インシデントマネージャ，インシデントハンドラー
  - インシデント対応処理担当
    - 自組織のセキュリティ対策に関する知識
    - 自組織の情報システムの運用経験
    - インシデントに関する管理や報告ができる能力
- ソリューションアナリスト
  - セキュリティ戦略担当
    - 自組織のビジネスに合わせて戦略を計画できる能力
    - 自組織のセキュリティ対策に関する知識
    - 自組織の情報システムに関する知識
    - リスクマネジメント能力
- セルフアセスメント担当
  - リスクアセスメント，脆弱性対応
    - 自組織の情報システムに関する知識
    - TISSレベル2程度の基礎的なITリテラシー
    - リスクアセスメントのためのヒアリング能力，文書課能力

組織におけるCSIRTの役割（2）

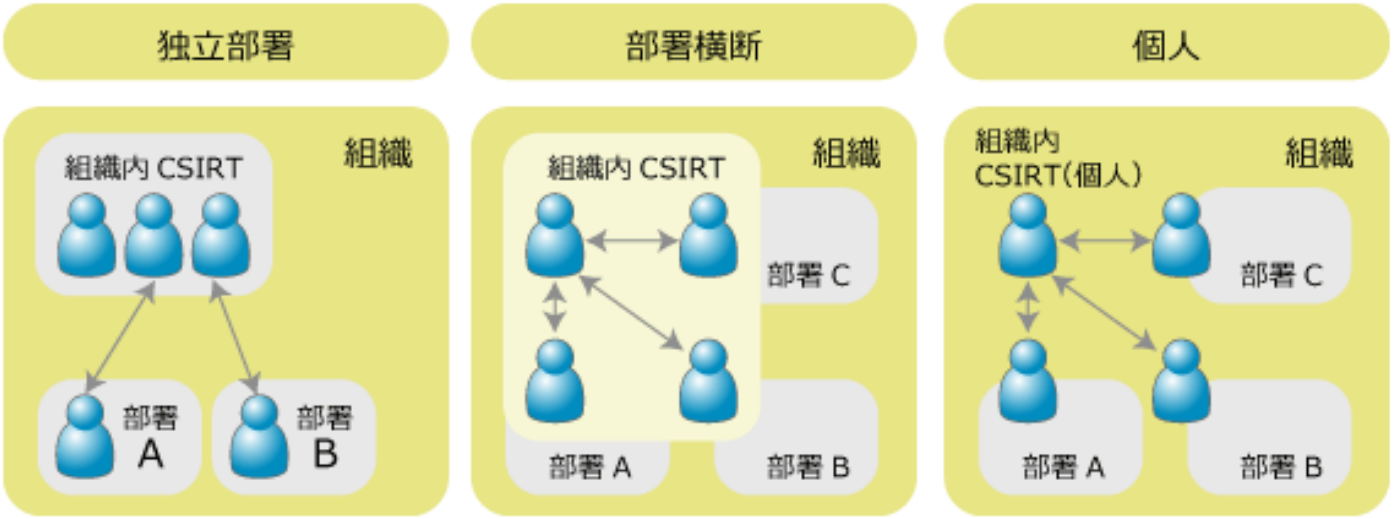
大阪府立大学 Osaka Prefecture University

- インシデント発生時の被害拡大防止，調査・分析のために情報システム（サービス）を停止するかどうかの判断
  - 時間をかけずに判断できるか？
- 経営層による経営（事業継続性）判断，意思決定のためのデータを提示
  - 自組織の情報システム，情報セキュリティ対策，ビジネスを熟知していることが必須
    - 技術的に正しいことがその組織にとって必ずしも正しいとは限らない
    - リスクアセスメントには技術以外の要素もある
    - 組織全体を見て正しい対応をとるための判断は，セキュリティベンダーにはできない
  - 世の中の情勢
    - 外部組織との情報交換も必要
  - ITスキルとコミュニケーション能力が必須
    - 報告，連絡，相談が適切な時期に，相手によって適切な内容でできるか？

CSIRT構築時の検討事項

大阪府立大学 Osaka Prefecture University

- 対象は？
  - 組織内インフラ
  - 提供サービス
  - 機密情報
- 組織体制



出典：JPCERT/CC CSIRT ガイド

- 権限
  - セキュリティポリシー等の規程類にCSIRTの存在とその権限を明記
  - 組織の文化や歴史的経緯を反映

CSIRT構築の課題（１）

大阪府立大学 Osaka Prefecture University

- 人材の確保は？
  - 理工系（情報系）の学部・研究科には技術系の研究者はいるけど…
    - それでも，教育・研究と実務は別と考える教員が多い
  - 文系の学部・研究科しかない大学はどうするの？
    - 監視や（技術的に高度な）分析は外部委託
  - 規模の小さな大学にもCSIRTは必要？
    - １人 CSIRT 問題
- では，学術研究機関はどこまでできれば/やればいいのか？
  - PoCとコマンダーは不可欠
  - 技術系（インシデントハンドラーなど）人材は居ればよし，居なければ委託可能？
  - SOCから通知が来ても重要度が判断できない…
- CIOとCISOの分離
  - 情報システム構築とともに情報セキュリティも熟知
  - 本来は，CIOとCISOはアクセルとブレーキのはず？

CSIRT構築の課題（2）

大阪府立大学
OSAKA PREFECTURE UNIVERSITY

- 組織によってCSIRTの構成は異なる
  - 組織の歴史的経緯，知識，経験
  - CSIRT組織の類型化は難しい？

- 学術研究機関におけるCSIRT構築の課題
  - 経営層の理解
    - 予算の確保，人材の確保，継続性の確保
  - 必要な人材が居るか？ or 育てられるか？
  - （教育研究目的でない）セキュリティ実務家は評価されるのか？
  - キャリアパスは？

- 学術研究機関で育成できるCSIRT人材とは？
  - 教育するためにはバックグラウンドに研究がないと…

CSIRT人材の育成

大阪府立大学 Osaka Prefecture University

- セキュリティ人材とは少し異なる？
  - 技術だけでは無い…
- 理工系（情報系）を持っている大学でも…
  - 教育・研究は技術に偏りがち
  - ITスキルを見につけ，その上にセキュリティも
    - さらに，システム管理に必要な資質や倫理観…
  - 知識，経験，資質（勘？）
    - 類型化はできないか？
- 人は失敗しないと覚えない
  - 成功体験も大事だけど…
  - 覚えるためには，実験や演習だけでなく，実運用での緊張感が必要
    - 学生は実運用しているシステム管理はさせてもらえない
  - 必要なのは失敗しないことではなく，失敗すること
  - でも，今は失敗が許されない時代
    - できれば小さな失敗で学習できる環境があると良いなぁ…