CSIRT人材の定義と確保(Ver.2.1)

2020年12月11日

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
CSIRT人材ワーキンググループ(CSIRT人材WG)

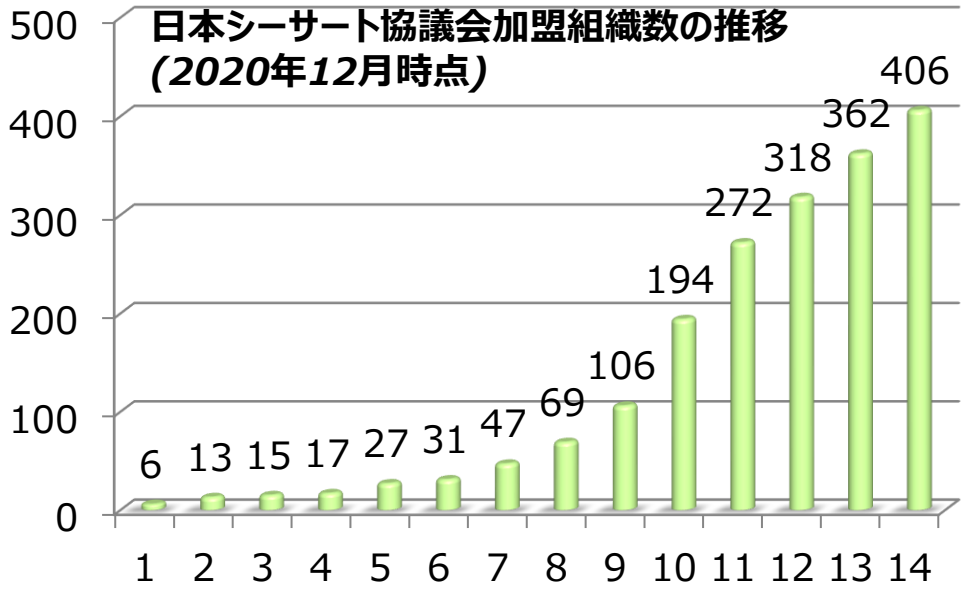
目次

1.はじめに

サイバー攻撃の増加や内部犯罪による被害も見受けられることから、日本企業では、セキュリティ管理部署の設立やセキュリティ管理者を配置するなど、人材面の投資を増やす傾向にある。その動きは、日本シーサート協議会への加盟組織数の急速な伸びにも表れている。しかしながら、CSIRT組織が何をすべきか、必要な人材はどのように確保するのか、確保した人材をどのように育成するかも明確化されないまま、セキュリティ人材の不足という言葉だけが叫ばれている。

本資料はその混沌とした課題をひも解き、CSIRTに求められる役割と実現に必要な人材のスキル、育成についてまとめた。また、参考として対象となる企業を大きく4つのモデルに分けて解説している。なお、 CSIRT人材WGでは継続的に議論を行い、またCSIRT活動に関わる多くの方々からのフィードバックを参考にしながら、改訂を行う予定である。

本資料が、日本に芽生えて間もないCSIRT組織の活動に少しでも役立つことになれば幸いである。



1.本資料の目的

- 本資料は、各企業のCSIRTにおいて必要な機能、体制、人材を明確にすることによって、CSIRTの継続的な活動を支援することを目的としている。
  特に、次の2点に着目した資料構成としている。
  - 新たにCSIRTを構築する、CSIRTの役割の一部をアウトソーシングする、あるいは、CSIRTを担う人材を定義・確保する等の参考になる情報の提供
  - 自組織向けのCSIRT人材の募集要項作成、あるいは、CSIRTの機能や人材を自組織外に求める場合の提案依頼書(RFP)や人材の募集要項作成のための参考になる情報の提供

2.CSIRTにおける課題と解決の方向性

企業のCSIRTを構築する上で、どのような人材を確保し、どのように育成すればよいのか、また、構築したCSIRTは有効に機能しているのかなど課題も多い。
本資料では、下記に沿って、課題解決の方向性を示すとともに、4つのCSIRTモデルとその実装内容を例示する。

課題	解決の方向性
CSIRTで必要な人材がわからない	✓ 役割毎の必要な前提スキルの定義
CSIRTで確保した要員をどのように育成したらいいかわからない	✓ 役割毎の追加教育スキルの定義 ✓ 参考とすべき資格 ✓ 教育方法
自組織のCSIRTで実施すべきことがわからない	✓ CSIRTを組織する役割の定義 ✓ 役割毎の実施内容の定義 ✓ 役割間の関連
セキュリティベンダーと同じ要求をされても、一般企業には要求が高すぎる	✓ CSIRTのモデル分け ✓ アウトソーシングの考え方 ✓ 兼任できる役割の考え方 ✓ CSIRTで必要な人数

3.対象とするCSIRTの役割と業務内容

■ 本資料で想定する組織が保有すべきCSIRTの役割とその業務内容

機能分類	業務内容	役割名称
情報共有	社内、社外との連絡窓口。経営者に対してはCSIRT全体統括者とともに連絡を行う。 社外の例：NCA、JPCERT/CC、CSIRT、警察、監督官庁、等々 社内の例：法務、渉外、広報、各事業部、等々	社外PoC：自組織外連絡担当
		社内PoC：自組織内連絡担当
	コンプライアンス、法的要求内容や法令の解釈において、法務部門とCSIRTの橋渡しを行う。	リーガルアドバイザー：リーガルアドバイス担当
	脅威情報、脆弱性情報などを自組織内へ情報発信したり、対応調整などを行う。	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、IT部門調整担当
情報収集・分析	セキュリティ機器から発せられるアラートの調査や予兆を分析し、情報分析担当とともに状況を調査し、インシデント管理担当に報告する。また、脅威情報や自社にかかわる漏えい情報なども収集する。	リサーチャー：情報収集担当
	情報収集担当が集めたデータを分析し、自社に適応すべきかの判断やトリアージを行う際に必要な情報を整理してインシデント管理担当に報告する。	キュレーター：情報分析担当
	自社のシステムについてアプリやインフラに脆弱性があるか検査、診断を行い、評価する。	脆弱性診断士：脆弱性の診断・評価担当
	自社の資産管理の維持管理を行い、最新に保つよう、自社の部門に働きかける。 また、リスクアセスメントを行い、改善項目があれば計画立てて実施する。	セルフアセスメント担当
	自社のセキュリティ機器類の全体設計を行い、有効性評価とともに企画、導入を行う。	ソリューションアナリスト：セキュリティ戦略担当

機能分類	業務内容	役割名称
インシデント対応	平常時、インシデント対応時のCSIRT全体統括を行う。必要であれば、PoCとともに経営者に説明を行う。	コマンダー：CSIRT全体統括担当
	インシデントの情報を情報収集担当や情報分析担当から収集し、CSIRT全体統括へ情報共有する。また、インシデント処理担当へ対応指示を行い、状況を管理し、インシデントレポートを記録する。	インシデントマネージャー：インシデント管理担当
	発生しているインシデント対応を行う。また、影響しているシステムへの対応支援も行う。 セキュリティベンダーを利用している場合にはベンダーとの連携を行う。	インシデントハンドラー：インシデント処理担当
	内部犯罪やサイバークライム事案などの調査を必要であれば警察と連携して行う。	インベスティゲーター：調査・捜査担当
	平常時にはインシデントが発生した時のシステム停止、再開の対応基準を準備しておく。また、インシデント発生時には対応の優先順位をCSIRT全体統括を支援しながら決定する。	トリアージ担当：優先順位選定担当
	機器類の証拠保全やシステム的な鑑識を行い、内部で何が起きているのかの足跡を調査する。また、発見されたマルウェアの解析も行う。	フォレンジック担当
自組織内教育	自組織の一般の役職員に対してセキュリティ教育を行う。CSIRT要員に対する教育は専門家が行う。	教育担当：教育・啓発担当
経営者	セキュリティにかかわる人的、システム的なリソースの手配、インシデント対応も含めたセキュリティ施策の最終判断と責任を持つ。	CISO、CSO、社長など
組織運営 ※CSIRTが特定の部署に属さない場合	CSIRTの予算申請・管理、要員調整、労務管理、工数管理に係わる関係部署との調整を行う。	CSIRT運営管理担当
システム運用 ※CSIRT内でもシステム運用部門でもよい。	CSIRTで利用するセキュリティ機器やネットワーク機器のシステム的な維持管理を行う。	システム運用担当

4.役割別任用前提スキルと追加教育スキル
4.1「PoC（Point of Contact）」

自組織外・自組織内連絡担当

社内、社外との連絡窓口。経営者に対してはCSIRT全体統括者とともに連絡を行う。
社外の例：NCA、JPCERT/CC、CSIRT、警察、監督官庁、等々
社内の例：法務、渉外、広報、各事業部、等々

任用前提スキル

- ✓ 情報を正しく伝えるコミュニケーション能力
- ✓ ITSSレベル２程度の基礎的なITリテラシー
- ✓ 情報を適切に判断する能力

追加教育スキル

- ✓ 情報を収集し、インテリジェンスを生成・報告できる能力
- ✓ サイバーセキュリティ問題に関する外部組織と学術機関に関する知識
- ✓ 既知の脆弱性に関する知識

役割別任用前提スキルと追加教育スキル
4.2「リーガルアドバイザー」

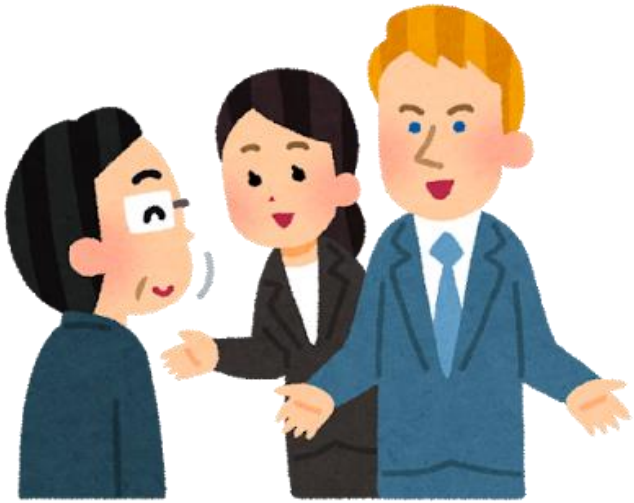
リーガルアドバイス担当
コンプライアンス、法的要求内容や法令の解釈において、法務部門とCSIRTの橋渡しを行う。

任用前提スキル
- ✓ セキュリティに関わる関連法の知識、もしくはITSSレベル２程度の基礎的なITリテラシー
- ✓ サイバーセキュリティに関連する技術的動向、法的なトレンドの追跡、解析ができる能力。
- ✓ 情報を正しく伝えるコミュニケーション能力

追加教育スキル
- ✓ セキュリティに関わる関連法、ITリテラシーのさらに深い知識
- ✓ インシデントレスポンスとハンドリングの知識
- ✓ 調達、サプライチェーン、業務委託をセキュアに行うための知識

役割別任用前提スキルと追加教育スキル
4.3「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、IT部門調整担当
脅威情報、脆弱性情報などを自組織内へ情報発信したり、対応調整などを行う。



任用前提スキル
- ✓ 情報を正しく伝えるコミュニケーション能力
- ✓ ITSSレベル２程度の基礎的なITリテラシー
- ✓ 情報を適切に判断し、説明する能力
- ✓ 自組織システムに関する知識
- ✓ 折衝能力

追加教育スキル
- ✓ ITセキュリティ、セキュリティマネジメントの基礎
- ✓ インシデントレスポンスとハンドリングの知識
- ✓ 自組織セキュリティガイドライン、遵守事項の知識
- ✓ 既知の脆弱性に関する知識
- ✓ 事象に対するリスク把握と優先順位を説明出来る能力

役割別任用前提スキルと追加教育スキル
4.4「リサーチャー」

情報収集担当

セキュリティ機器から発せられるアラートの調査や予兆を分析し、情報分析担当とともに状況を調査し、インシデント管理担当に報告する。また、脅威情報や自社にかかわる漏えい情報なども収集する。

任用前提スキル

- ✓ 基礎的なセキュリティに関する知識
- ✓ 情報を鵜呑みにしないメディアリテラシー
- ✓ 英語を正しく読む能力

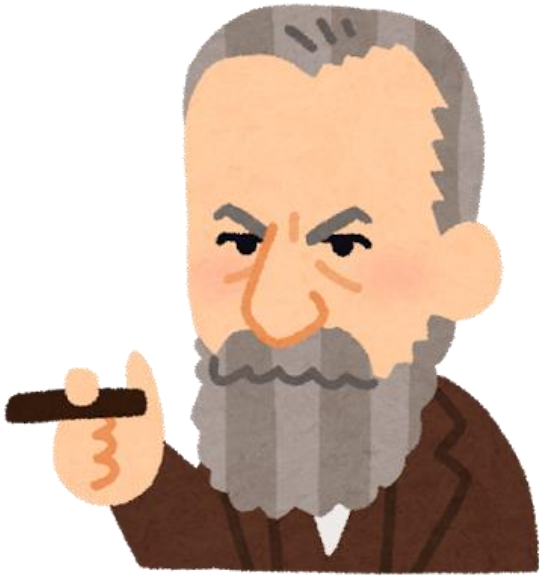
追加教育スキル

- ✓ 国家間の関係、ハクティビスト*に関する知識
- ✓ メディアの特性を知り、活用できる能力
- ✓ セキュリティ機器で検出される情報を正しく読む能力
- ✓ 攻撃戦術、ステージ、技術、手順に関する知識

*ハクティビストとは、ハッキング行為と政治的な活動を行うアクティビストから作られた造語で、政治的なハッキング活動を行う人物や組織のことを言う。

役割別任用前提スキルと追加教育スキル
4.5「キュレーター」

情報分析担当
情報収集担当が集めたデータを分析し、自社に適応すべきかの判断やトリアージを行う際に必要な情報を整理してインシデント管理担当に報告する。



任用前提スキル
- ✓ 自組織のセキュリティアーキテクチャ、ビジネスに関する知識
- ✓ 情報を鵜呑みにしないメディアリテラシー
- ✓ 英語を正しく読む能力

追加教育スキル
- ✓ 情報を収集し、インテリジェンスを活用できる能力
- ✓ 国家間の関係、ハクティビストに関する分析能力
- ✓ メディアの特性を知り、活用できる能力
- ✓ セキュリティ機器で検出される情報を相関分析できる能力
- ✓ 攻撃戦術、ステージ、技術、手順に関する知識
- ✓ 自組織のセキュリティ対策に適用すべきか判断できる能力

役割別任用前提スキルと追加教育スキル
4.6「脆弱性診断士」

脆弱性の診断・評価担当
自社のシステムについてアプリやインフラに脆弱性があるか、検査、診断を行い、評価する。

任用前提スキル
- ✓ OS、ネットワーク、アプリ、DBの脆弱性に対する知識
- ✓ パケットレベルの解析ができる能力
- ✓ ペネトレーションテストやツールに関する知識
- ✓ 一般的な攻撃手法に関する知識

追加教育スキル
- ✓ 自組織のセキュリティアーキテクチャに関する知識
- ✓ 新興の情報セキュリティ技術に関する知識
- ✓ 脅威情報に関する知識
- ✓ コンピュータ、ネットワーク防衛と脆弱性の評価ツールを活用できる能力

役割別任用前提スキルと追加教育スキル
4.7「セルフアセスメント担当」

セルフアセスメント担当

自社の資産管理の維持管理を行い、最新に保つよう、自社の部門に働きかける。
また、リスクアセスメントを行い、改善項目があれば計画立てて実施する

任用前提スキル

- ✓ ITSS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、文書化能力

追加教育スキル

- ✓ 個人情報保護法、PCIDSS、ISMSの公的規約の知識
- ✓ 自組織セキュリティポリシーやシステム構築に関するガイドライン、遵守事項の知識
- ✓ リスクマネジメントプロセスに関する知識
- ✓ インテリジェンスや最新の技術を読み取る能力

役割別任用前提スキルと追加教育スキル
4.8「ソリューションアナリスト」

セキュリティ戦略担当
自社のセキュリティ機器類の全体設計を行い、有効性評価とともに企画、導入を行う。

任用前提スキル
- ✓ 自組織ビジネスビジョンに合わせて計画化する能力
- ✓ 自組織セキュリティガイドライン、遵守事項の知識
- ✓ リスクマネジメントプロセスを活用できる能力
- ✓ 自組織システムに関する知識

追加教育スキル
- ✓ 個人情報保護法、PCIDSS等の公的規約の知識
- ✓ インテリジェンスや最新の技術を読み取る能力
- ✓ セキュリティ要求事項と製品・運用を組合わせる能力

役割別任用前提スキルと追加教育スキル
4.9「コマンダー」

CSIRT全体統括担当

平常時、インシデント対応時のCSIRT全体統括を行う。必要であれば、PoCとともに経営者に説明を行う。

任用前提スキル

- ✓ システム障害の全体統制を行える能力
- ✓ 自組織のセキュリティアーキテクチャ、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
- ✓ 経営陣に説明できるコミュニケーションスキル

追加教育スキル

- ✓ リスク影響とビジネス継続を考慮して優先順位を決定できる能力
- ✓ 攻撃戦術、ステージ、技術、手順に関する知識
- ✓ セキュリティに特化したインシデント統制能力

役割別任用前提スキルと追加教育スキル
4.10「インシデントマネージャー」

インシデント管理担当

インシデントの情報を情報収集担当や情報分析担当から収集し、CSIRT全体統括へ情報共有する。また、インシデント処理担当へ対応指示を行い、状況を管理し、インシデントレポートを記録する。

任用前提スキル

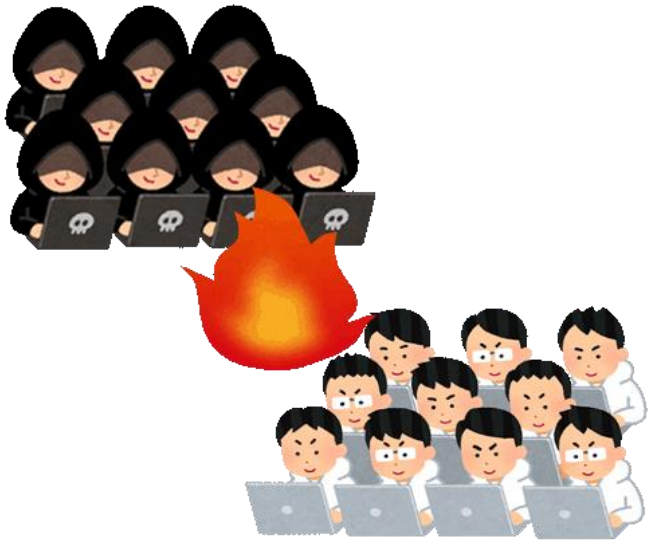
- ✓ システム運用知識
- ✓ インシデントに関する管理や報告ができる能力
- ✓ 自組織のセキュリティアーキテクチャの知識
- ✓ 自組織業務システムの知識

追加教育スキル

- ✓ セキュリティインシデント対応能力
- ✓ セキュリティインシデント後の復旧に関する知識
- ✓ 出現するセキュリティ問題、リスク、脆弱性の知識
- ✓ 脆弱性診断に関する知識
- ✓ マルウェア等各種攻撃に対する取り扱いの知識

役割別任用前提スキルと追加教育スキル
4.11「インシデントハンドラー」

インシデント処理担当
発生しているインシデントへの対応を行う。また、影響しているシステムへの対応支援も行う。
セキュリティベンダーを利用している場合にはベンダーとの連携を行う。



任用前提スキル
- ✓ システム運用知識
- ✓ インシデントに関する管理や報告ができる能力
- ✓ 自組織のセキュリティアーキテクチャの知識
- ✓ 自組織業務システムの運用経験

追加教育スキル
- ✓ セキュリティインシデント対応能力
- ✓ セキュリティインシデント後の復旧を行う能力
- ✓ 出現するセキュリティ問題、リスク、脆弱性の知識
- ✓ 脆弱性診断結果に対応する能力
- ✓ マルウェア等各種攻撃に対する対応能力

役割別任用前提スキルと追加教育スキル
4.12「インベスティゲーター」

調査・捜査担当

内部犯罪やサイバークライム事案などの調査を必要であれば警察と連携して行う。

任用前提スキル

- ✓ 情報を収集し、インテリジェンスを活用できる能力
- ✓ 国家間の関係、ハクティビストに関する分析能力
- ✓ 証拠の押収・保存の知識
- ✓ ITSSレベル２程度の基礎的なITリテラシー
- ✓ 自組織システムに関する知識

追加教育スキル

- ✓ 犯人特定のための捜査能力
- ✓ 尋問に関するコミュニケーション能力と知識
- ✓ 攻撃者の戦術・技術・手順に関する知識
- ✓ サイバー犯罪に関する法律的知識

役割別任用前提スキルと追加教育スキル
4.13「トリアージ担当」

優先順位選定担当

平常時にはインシデントが発生した時のシステム停止、再開の対応基準を準備しておく。また、インシデント発生時には対応の優先順位をCSIRT全体統括を支援しながら決定する。

任用前提スキル

- ✓ 自組織のセキュリティアーキテクチャ、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

追加教育スキル

- ✓ リスク影響とビジネス継続を考慮して優先順位を決定できる能力

役割別任用前提スキルと追加教育スキル
4.14「フォレンジック担当」

フォレンジック担当
機器類の証拠保全やシステム的な鑑識を行い、内部で何が起きているのかの足跡を調査する。また、発見されたマルウェアの解析も行う。

任用前提スキル
- ✓ OS、コマンド、システムファイル、プログラミング言語の構造とロジックに関する知識
- ✓ 脆弱性診断に関する知識

追加教育スキル
- ✓ デジタルフォレンジックに関する知識
- ✓ メモリダンプ解析能力
- ✓ マルウェア解析能力
- ✓ リバースエンジニアリングの能力
- ✓ バイナリ解析ツールを利用できる能力
- ✓ セキュリティイベントの相関分析を行える能力

役割別任用前提スキルと追加教育スキル
4.15「教育担当」

教育・啓発担当
自組織の一般の役職員に対してセキュリティ教育を行う。
CSIRT要員に対する教育は専門家が行う。

任用前提スキル
- ✓ 情報を正しく伝えるコミュニケーション能力
- ✓ ITSSレベル３程度のITリテラシー
- ✓ 情報をわかりやすく伝えるコミュニケーション能力

追加教育スキル
- ✓ 自組織セキュリティポリシーやシステム構築に関するガイドライン、遵守事項の知識
- ✓ 情報を収集し、インテリジェンスを生成・報告できる能力
- ✓ 既知の脆弱性に関する知識

役割別任用前提スキルと追加教育スキル
4.16「経営者」

CISO、CSO、社長など

セキュリティにかかわる人的、システム的なリソースの手配、インシデント対応も含めたセキュリティ施策の最終判断と責任を持つ。

役割

- ✓ 技術的な側面だけでなく、ビジネスへの影響を考慮して将来を見据えた取り組みを実施する。
- ✓ 組織全体のリスクを俯瞰し、ガバナンスの一貫としてセキュリティ対策を行う。
- ✓ セキュリティ計画の策定とともに評価や、他部門や経営陣と連携する。
- ✓ 財務会計や管理会計の指標を用いてセキュリティ対策の有効性を把握し、売上や利益に貢献する。
- ✓ 経営陣の一員として経営会議等で自社のセキュリティ状況の現状と今後の計画について把握し、実施する。

※スキルはJNSA:CISOハンドブックを参照

役割別任用前提スキルと追加教育スキル
4.17「CSIRT運営管理担当」

CSIRT運営管理担当
CSIRTの予算申請・管理、要員調整、労務管理、工数管理に係わる関係部署との調整を行う。

任用前提スキル
- ✓ 組織マネジメントの経験者

追加教育スキル
- ✓ CSIRTの対象範囲、責任範囲など、CSIRT活動を理解した上で他部署や経営陣などと交渉できる能力。

※CSIRTが特定の部署に属さない場合に必要。特定の部署内に属す場合にはその部署の組織管理職が行う。

役割別任用前提スキルと追加教育スキル
4.18「システム運用担当」

システム運用担当
CSIRTで利用するセキュリティ機器やネットワーク機器のシステム的な維持管理を行う。

任用前提スキル

✓ CSIRTが利用するインフラに対するシステム的な保守、維持管理ができる能力。

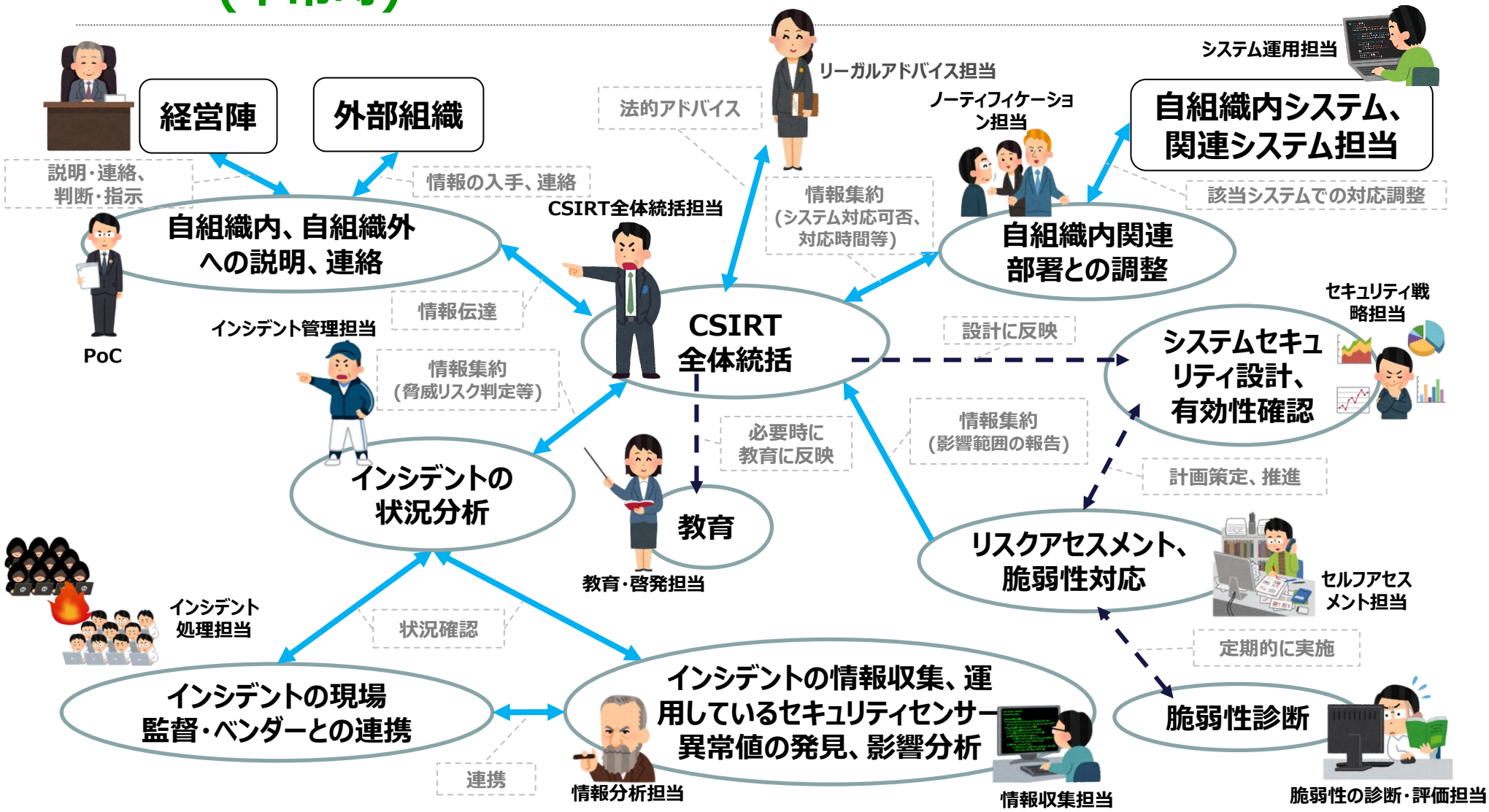
追加教育スキル

ー

※CSIRT内に設置しても、システム運用部門に設置しても良い。
※セキュリティ運用として、その機器を利用しての調査や分析はリサーチャーやキュレーターが行う。

4.19 CSIRTの役割と業務内容の関連図 (平常時)

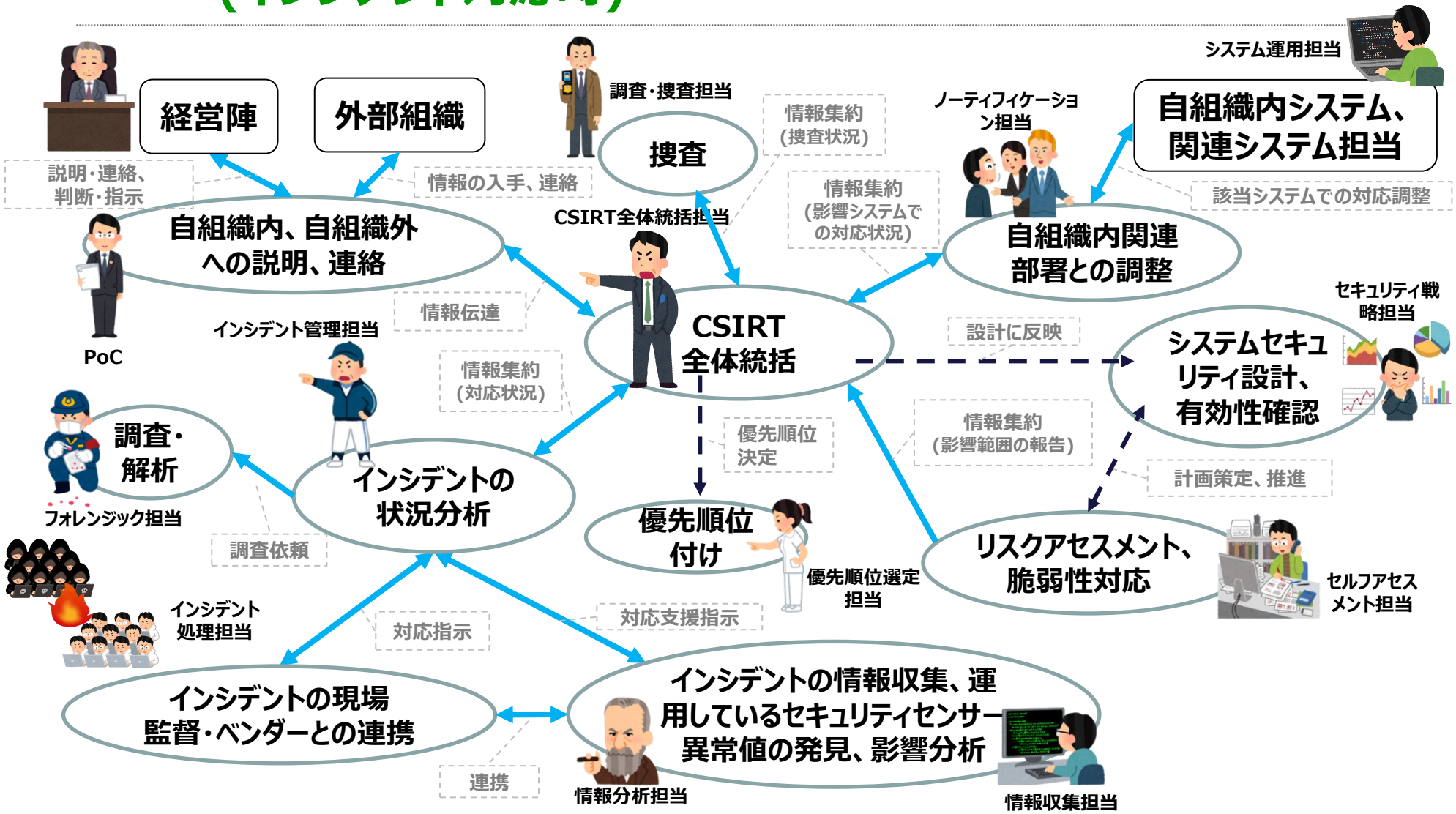
実線は活動時の情報の流れ。
点線は必要時に実施する活動の流れ。



＊CSIRT運営管理担当は上記活動のバックグラウンドとして必要である。図には記載していない。
＊システム運用担当は、「自組織内システム、関連システム担当」と同じ場合もあれば、別の場合もある。上記は同じ場合を例示した。

4.19 CSIRTの役割と業務内容の関連図 (インシデント対応時)

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。



＊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
＊法的確認が必要な場合には 各役割からリーガルアドバイザーに支援を要請する。

4.20 CSIRTの兼任可能な役割

以下に兼任可能な役割と実施内容・注意点を同一の背景色で記載する。ただし、これは一例であり、自社の事情に合わせて適宜調整すること。

機能分類	役割名称	兼任グループの実施内容・注意点
情報共有	社外PoC：自組織外連絡担当	**兼任グループ１（連絡・全体統括）** 連絡窓口となり、報告・説明を関係者、経営者に行う。 話し相手に合わせたコミュニケーションスキルが必要。 インシデント発生時には専門家とともにフェーズ毎の対応戦略を打ち出し、トリアージを含めてインシデントマネージャーに指示する。内部犯罪、サイバークライム案件については総務部や警察とともに活動する。
	社内PoC：自組織内連絡担当	
	リーガルアドバイザー：リーガルアドバイス担当	
	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、IT部門調整担当	
情報収集・分析	リサーチャー：情報収集担当	**兼任グループ２（SOC）** 脆弱性情報、脅威情報のリスク判定を対象システム、ネットワーク環境、ネット上のリサーチから判定する。 脅威情報から得られる不審なURLのアクセスやメールの受信、端末に存在するファイルのハッシュ値など、資産管理ツールを用いて定例的に確認・対応する。 セキュリティ機器から発せられる情報の正当性や影響範囲を確認し、該当部門に連絡・対応する。 必要であれば、デジタルフォレンジックも行う。
	キュレーター：情報分析担当	
	脆弱性診断士：脆弱性の診断・評価担当	**兼任グループ３（セキュティ戦略・製品評価）** 自社のセキュリティ機器の有効性確認を行い、セキュリティ機器設置計画を策定、実施する。また、自社のシステムについての脆弱性診断の実施と評価を行い、是正させる。
	セルフアセスメント担当	**兼任グループ４（資産管理・教育）** 自社の資産管理に基づくリスクアセスメントを行い、対応を行う。また、従業員教育を行う。
	ソリューションアナリスト：セキュリティ戦略担当	**兼任グループ３（セキュティ戦略・製品評価）**

機能分類	役割名称	兼任グループの実施内容・注意点
インシデント対応	コマンダー：CSIRT全体統括担当	**兼任グループ１（連絡・全体統括）**
	インシデントマネージャー：インシデント管理担当	**兼任グループ5（インシデント対応）** 全体統括の戦略に基づき、作業をタスク化し、実行する。 実施にあたっては、自社インフラ部門やアプリ部門と協力して行う。また、SOCから上がってくるアラートを該当システム部門と調整、調査する。 インテリジェンスを含めた脆弱性情報の適用可否やリスク判断をSOCとともに行い、関係者に連絡、調整、対応依頼をする。
	インシデントハンドラー：インシデント処理担当	
	インベスティゲーター：調査・捜査担当	**兼任グループ１（連絡・全体統括）**
	トリアージ担当：優先順位選定担当	**兼任グループ１（連絡・全体統括）**
	フォレンジック担当	**兼任グループ２（SOC）**
自組織内教育	教育担当：教育・啓発担当	**兼任グループ４（資産管理・教育）**
経営者	CISO、CSO、社長など	―
組織運営 ※CSIRTが特定の部署に属さない場合	CSIRT運営管理担当	―
システム運用 ※CSIRT内でもシステム運用部門でもよい。	システム運用担当	―

5.CSIRTのモデルと実装例

- 本資料ではCSIRTを以下のように区分し、モデルA～Dに関しての実装例を記載する。
- 実装例は一例であり、各企業においては記載事例をそのまま適用するのではなく、各企業の事業内容や体制を踏まえて取捨選択してほしい。

モデル	定義
A	ユーザ企業で総務部門等を主体として構築・運用されているCSIRT
B	ユーザ企業でIT系子会社、または情報セキュリティに関する専門部門を主体として構築・運用されているCSIRT
C	IT系、セキュリティベンダー系企業において構築・運用されているCSIRT
D	上記に当てはまらない大学など
E	その他(学術機関、政府機関、法執行機関など)

※本資料においてモデルEは対象としていない

モデルA

ユーザ企業で総務部門等を主体として構築・運用されているCSIRTを想定

自組織内で情報共有はするが、システム維持についてはベンダーに委託する。ミッションとしてはベンダーの報告を受け、プロアクティブな予防処置を行い、インシデント発生時には社として守るべき優先順位の判断を行う。最低限の自警団の機能として活動する。自警団では対応できない場合にのみ、セキュリティ専門ベンダーに支援を要請する。

モデルA 実装例

- モデルAの実装例として、実例を基に以下の項目について例示する。
  - 自組織で保有する役割とアウトソーシングする役割
  - 自組織内での教育プログラム

自組織で保有する役割とアウトソーシングする役割

下記の役割はすべて実施するが、黄色の部分はアウトソーシングする。CSIRTには、ベンダーと会話できるスキル、自組織内情報共有としてベンダーの言葉を伝えられるスキル、優先順位を決定できるスキル、自組織内教育ができるスキルが必要となる。

機能分類	業務内容	役割名称
情報共有	社内、社外との連絡窓口。経営者に対してはCSIRT全体統括者とともに連絡を行う。 社外の例：NCA、JPCERT/CC、CSIRT、警察、監督官庁、等々 社内の例：法務、渉外、広報、各事業部、等々	社外PoC：自組織外連絡担当
		社内PoC：自組織内連絡担当、
	コンプライアンス、法的要求内容や法令の解釈において、法務部門とCSIRTの橋渡しを行う。	リーガルアドバイザー：リーガルアドバイス担当
	脅威情報、脆弱性情報などを自組織内へ情報発信したり、対応調整などを行う。	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、IT部門調整担当
情報収集・分析	セキュリティ機器から発せられるアラートの調査や予兆を分析し、情報分析担当とともに状況を調査し、インシデント管理担当に報告する。また、脅威情報や自社にかかわる漏えい情報なども収集する。	リサーチャー：情報収集担当
	情報収集担当が集めたデータを分析し、自社に適応すべきかの判断やトリアージを行う際に必要な情報を整理してインシデント管理担当に報告する。	キュレーター：情報分析担当
	自社のシステムについてアプリやインフラに脆弱性があるか検査、診断を行い、評価する。	脆弱性診断士：脆弱性の診断・評価担当
	自社の資産管理の維持管理を行い、最新に保つよう、自社の部門に働きかける。 また、リスクアセスメントを行い、改善項目があれば計画立てて実施する。	セルフアセスメント担当
	自社のセキュリティ機器類の全体設計を行い、有効性評価とともに企画、導入を行う。	ソリューションアナリスト：セキュリティ戦略担当

機能分類	業務内容	役割名称
インシデント対応	平常時、インシデント対応時のCSIRT全体統括を行う。必要であれば、PoCとともに経営者に説明を行う。	コマンダー：CSIRT全体統括担当
	インシデントの情報を情報収集担当や情報分析担当から収集し、CSIRT全体統括へ情報共有する。また、インシデント処理担当へ対応指示を行い、状況を管理し、インシデントレポートを記録する。	インシデントマネージャー：インシデント管理担当
	発生しているインシデント対応を行う。また、影響しているシステムへの対応支援も行う。 セキュリティベンダーを利用している場合にはベンダーとの連携を行う。	インシデントハンドラー：インシデント処理担当
	内部犯罪やサイバークライム事案などの調査を必要であれば警察と連携して行う。	インベスティゲーター：調査・捜査担当
	平常時にはインシデントが発生した時のシステム停止、再開の対応基準を準備しておく。また、インシデント発生時には対応の優先順位をCSIRT全体統括を支援しながら決定する。	トリアージ担当：優先順位選定担当
	機器類の証拠保全やシステム的な鑑識を行い、内部で何が起きているのかの足跡を調査する。また、発見されたマルウェアの解析も行う。	フォレンジック担当
自組織内教育	自組織の一般の役職員に対してセキュリティ教育を行う。CSIRT要員に対する教育は専門家が行う。	教育担当：教育・啓発担当
経営者	セキュリティにかかわる人的、システム的なリソースの手配、インシデント対応も含めたセキュリティ施策の最終判断と責任を持つ。	CISO、CSO、社長など
組織運営 ※CSIRTが特定の部署に属さない場合	CSIRTの予算申請・管理、要員調整、労務管理、工数管理に係わる関係部署との調整を行う。	CSIRT運営管理担当
システム運用 ※CSIRT内でもシステム運用部門でもよい。	CSIRTで利用するセキュリティ機器やネットワーク機器のシステム的な維持管理を行う。	システム運用担当

CSIRTの役割と業務内容の関連図（平常時）

【凡例】
アウトソーシング
自組織保有

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。


経営陣

外部組織

説明・連絡、判断・指示

情報の入手、連絡


PoC

自組織内、自組織外への説明、連絡

情報伝達


リーガルアドバイス担当

法的アドバイス


システム運用担当


ノーティフィケーション担当

自組織内システム、関連システム担当

該当システムでの対応調整

情報集約（システム対応可否、対応時間等）

自組織内関連部署との調整

CSIRT全体統括担当


CSIRT全体統括

設計に反映


セキュリティ戦略担当

システムセキュリティ設計、有効性確認

インシデント管理担当


情報集約（脅威リスク判定等）

インシデントの状況分析

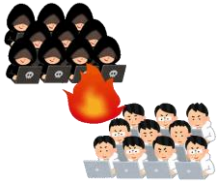
必要時に教育に反映


教育

教育・啓発担当

情報集約（影響範囲の報告）

計画策定、推進


インシデント処理担当

状況確認


リスクアセスメント、脆弱性対応

セルフアセスメント担当

定期的に実施

インシデントの現場監督・ベンダーとの連携

連携


インシデントの情報収集、運用しているセキュリティセンサー異常値の発見、影響分析

情報分析担当


情報収集担当


脆弱性診断

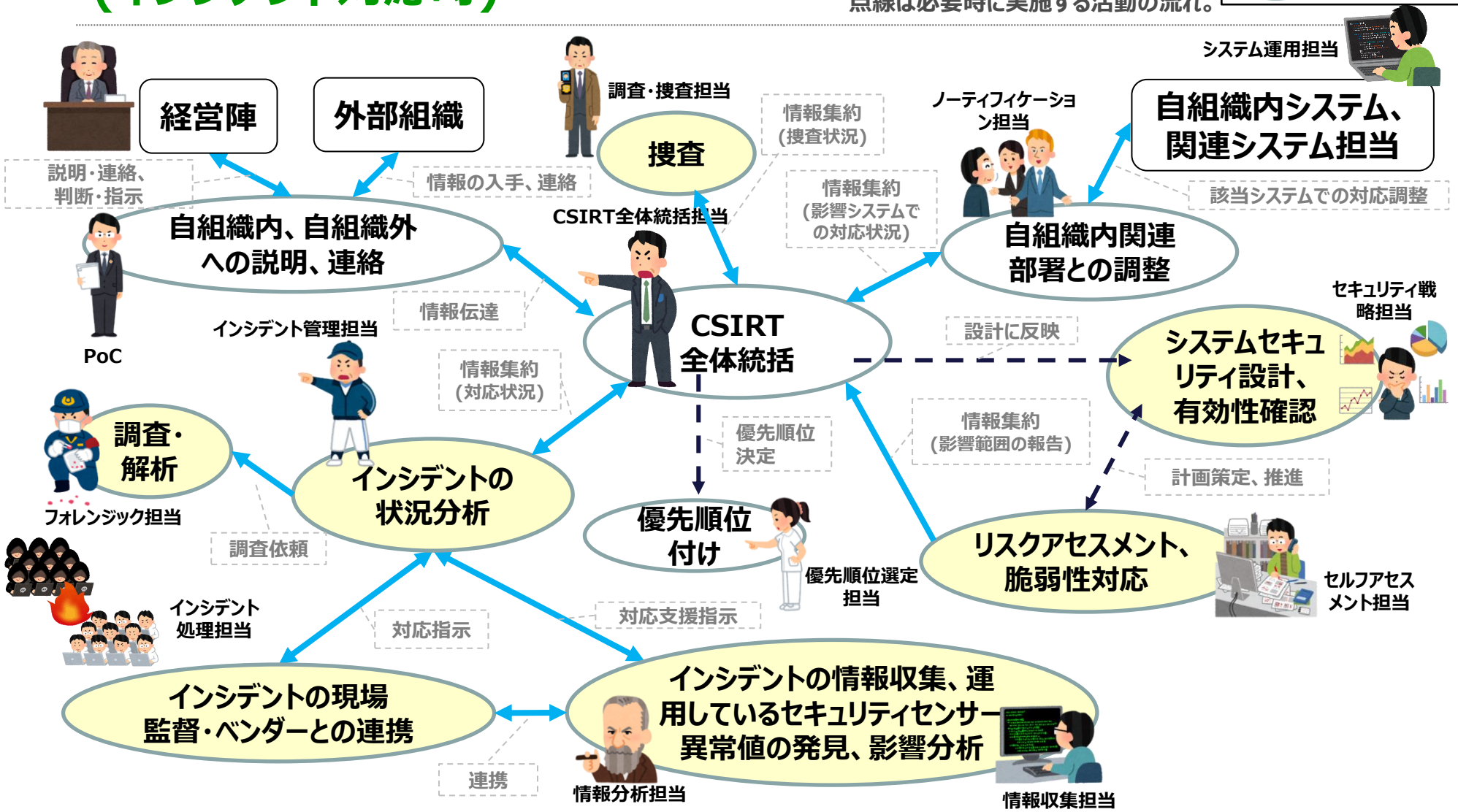
脆弱性の診断・評価担当

＊CSIRT運営管理担当は上記活動のバックグラウンドとして必要である。図には記載していない。
＊システム運用担当は、「自組織内システム、関連システム担当」と同じ場合もあれば、別の場合もある。上記は同じ場合を例示した。

CSIRTの役割と業務内容の関連図（インシデント対応時）

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。

【凡例】
アウトソーシング
自組織保有



＊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
＊法的確認が必要な場合には 各役割からリーガルアドバイザーに支援を要請する。

自組織内での教育プログラム

- 以下の教育プログラムを自組織内で提供
  - 全役割共通の教育プログラム
    - 自組織のポリシー、セキュリティ規定、管理細則類
    - ISMSやPCIDSSなどの一般的な規定
    - 自組織の運用規定類、業務システム概要
    - セキュリティ機器、設備の詳細、SOC判断基準
    - CSIRT行動要領
    - インシデント対応を想定した演習
  - 役割ごとの教育プログラム
    - CSIRTとしての平常時、インシデント対応時の役割毎OJT
    - 他CSIRTとの意見交換

モデルB

ユーザ企業でIT系子会社、または情報セキュリティに関する専門部門を主体として構築・運用されているCSIRTの一例

システムの維持管理は自組織で運用しているが、平常時の脆弱性診断やSOCの一部、インシデント対応時のフォレンジックなど、自組織のコア事業以外の部分をアウトソーシングする例を示す。CSIRTの役割としてはアウトソーシング先とのコミュニケーションを通じて、プロアクティブな予防処置を行う。また、インシデント発生時には自組織として守るべき優先順位の判断を行い、インシデント対応を行う。
自組織内の体制、スキルでインシデント対応を賄えない場合にはセキュリティ専門ベンダーに不足部分の支援を要請する。

モデルB 実装例

- モデルBの実装例として、実例を基に以下の項目について例示する。
  - 自組織で保有する役割とアウトソーシングする役割
  - 自組織内での教育プログラム

自組織で保有する役割とアウトソーシングする役割

自組織内関連部署との調整や、ビジネスインパクトに関わる判断、インシデント対応に関する役割はすべて実施するが、自組織のコアビジネス以外の役割、専門性が要求される役割の黄色の部分はアウトソーシングする。

機能分類	業務内容	役割名称
情報共有	社内、社外との連絡窓口。経営者に対してはCSIRT全体統括者とともに連絡を行う。 社外の例：NCA、JPCERT/CC、CSIRT、警察、監督官庁、等々 社内の例：法務、渉外、広報、各事業部、等々	社外PoC：自組織外連絡担当
		社内PoC：自組織内連絡担当、
	コンプライアンス、法的要求内容や法令の解釈において、法務部門とCSIRTの橋渡しを行う。	リーガルアドバイザー：リーガルアドバイス担当
	脅威情報、脆弱性情報などを自組織内へ情報発信したり、対応調整などを行う。	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、IT部門調整担当
情報収集・分析	セキュリティ機器から発せられるアラートの調査や予兆を分析し、情報分析担当とともに状況を調査し、インシデント管理担当に報告する。また、脅威情報や自社にかかわる漏えい情報なども収集する。	リサーチャー：情報収集担当
	情報収集担当が集めたデータを分析し、自社に適応すべきかの判断やトリアージを行う際に必要な情報を整理してインシデント管理担当に報告する。	キュレーター：情報分析担当
	自社のシステムについてアプリやインフラに脆弱性があるか検査、診断を行い、評価する。	脆弱性診断士：脆弱性の診断・評価担当
	自社の資産管理の維持管理を行い、最新に保つよう、自社の部門に働きかける。 また、リスクアセスメントを行い、改善項目があれば計画立てて実施する。	セルフアセスメント担当
	自社のセキュリティ機器類の全体設計を行い、有効性評価とともに企画、導入を行う。	ソリューションアナリスト：セキュリティ戦略担当

機能分類	業務内容	役割名称
インシデント対応	平常時、インシデント対応時のCSIRT全体統括を行う。必要であれば、PoCとともに経営者に説明を行う。	コマンダー：CSIRT全体統括担当
	インシデントの情報を情報収集担当や情報分析担当から収集し、CSIRT全体統括へ情報共有する。また、インシデント処理担当へ対応指示を行い、状況を管理し、インシデントレポートを記録する。	インシデントマネージャー：インシデント管理担当
	発生しているインシデント対応を行う。また、影響しているシステムへの対応支援も行う。 セキュリティベンダーを利用している場合にはベンダーとの連携を行う。	インシデントハンドラー：インシデント処理担当
	内部犯罪やサイバークライム事案などの調査を必要であれば警察と連携して行う。	インベスティゲーター：調査・捜査担当
	平常時にはインシデントが発生した時のシステム停止、再開の対応基準を準備しておく。また、インシデント発生時には対応の優先順位をCSIRT全体統括を支援しながら決定する。	トリアージ担当：優先順位選定担当
	機器類の証拠保全やシステム的な鑑識を行い、内部で何が起きているのかの足跡を調査する。また、発見されたマルウェアの解析も行う。	フォレンジック担当
自組織内教育	自組織の一般の役職員に対してセキュリティ教育を行う。CSIRT要員に対する教育は専門家が行う。	教育担当：教育・啓発担当
経営者	セキュリティにかかわる人的、システム的なリソースの手配、インシデント対応も含めたセキュリティ施策の最終判断と責任を持つ。	CISO、CSO、社長など
組織運営 ※CSIRTが特定の部署に属さない場合	CSIRTの予算申請・管理、要員調整、労務管理、工数管理に係わる関係部署との調整を行う。	CSIRT運営管理担当
システム運用 ※CSIRT内でもシステム運用部門でもよい。	CSIRTで利用するセキュリティ機器やネットワーク機器のシステム的な維持管理を行う。	システム運用担当

CSIRTの役割と業務内容の関連図（平常時）

【凡例】
アウトソーシング
自組織保有

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。


経営陣

外部組織

説明・連絡、判断・指示

情報の入手、連絡


PoC

自組織内、自組織外への説明、連絡


リーガルアドバイス担当

法的アドバイス


CSIRT全体統括担当

情報集約（システム対応可否、対応時間等）


ノーティフィケーション担当

自組織内関連部署との調整


システム運用担当

自組織内システム、関連システム担当

該当システムでの対応調整

情報伝達

CSIRT全体統括

設計に反映


セキュリティ戦略担当

システムセキュリティ設計、有効性確認


インシデント管理担当

情報集約（脅威リスク判定等）

インシデントの状況分析

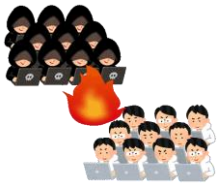
必要時に教育に反映


教育・啓発担当

教育

情報集約（影響範囲の報告）

計画策定、推進


インシデント処理担当

状況確認


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

定期的に実施

インシデントの現場監督・ベンダーとの連携

連携


情報分析担当

インシデントの情報収集、運用しているセキュリティセンサー異常値の発見、影響分析


情報収集担当

脆弱性診断

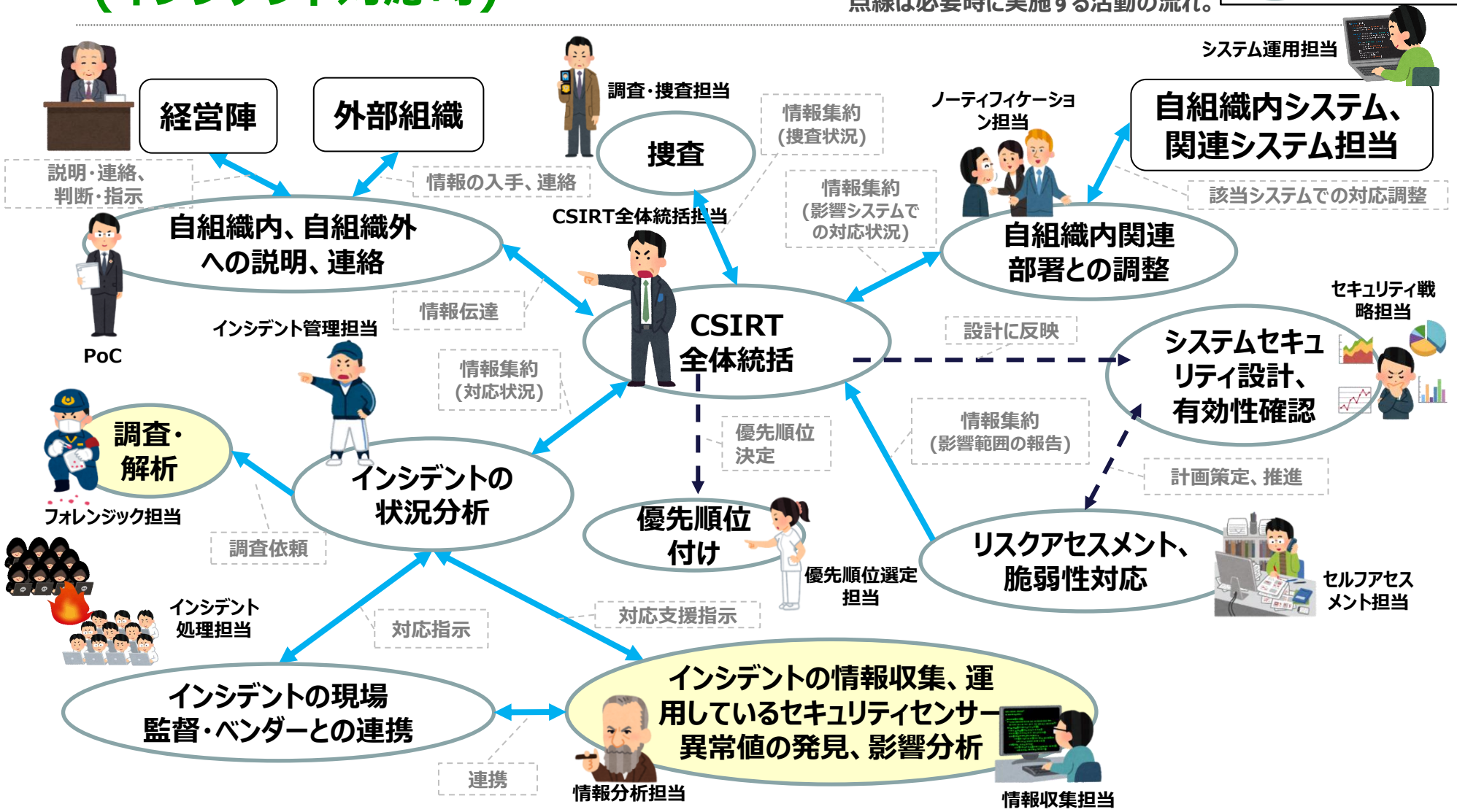

脆弱性の診断・評価担当

＊CSIRT運営管理担当は上記活動のバックグラウンドとして必要である。図には記載していない。
＊システム運用担当は、「自組織内システム、関連システム担当」と同じ場合もあれば、別の場合もある。上記は同じ場合を例示した。

CSIRTの役割と業務内容の関連図（インシデント対応時）

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。

【凡例】
アウトソーシング
自組織保有



＊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
＊法的確認が必要な場合には 各役割からリーガルアドバイザーに支援を要請する。

自組織内での教育プログラム

- 以下の教育プログラムを自組織内で提供
  - 全役割共通の教育プログラム
    - 自組織のポリシー、セキュリティ規定、管理細則類
    - ISMSやPCIDSSなどの一般的な規定
    - 自組織のシステム構築ガイドライン類
    - 自組織の運用規定類、業務システム概要
    - セキュリティ機器、設備の詳細、SOC判断基準
    - リスクアセスメント、監査手法
    - CSIRT行動要領
    - インシデント対応を想定した演習
  - 役割ごとの教育プログラム
    - CSIRTとしての平常時、インシデント対応時の役割毎OJT
    - 他CSIRTとの意見交換

モデルC

IT系、セキュリティベンダー系企業において構築・運用されているCSIRTの一例

自組織グループ向けCSIRTや企業向けにCSIRTが担う役務を提供する。
ほとんどすべてのCSIRT機能を自組織で保有し、研究・開発・未知の脅威の発見、情報発信なども公的に行う。

モデルC 実装例

- モデルCの実装例として、実例を基に以下の項目について例示する。
  - 自組織で保有する役割とアウトソーシングする役割
  - 自組織内での教育プログラム

自組織で保有する役割とアウトソーシングする役割

すべての役割を自組織保有とする。内製により得られる技術力・ノウハウが競争力の源泉であるため、すべての役割を自組織保有し、アウトソーシングは基本的には行わない。ただし、補助的にベンダーに作業をアウトソーシングすることはある。

機能分類	業務内容	役割名称
情報共有	社内、社外との連絡窓口。経営者に対してはCSIRT全体統括者とともに連絡を行う。 社外の例：NCA、JPCERT/CC、CSIRT、警察、監督官庁、等々 社内の例：法務、渉外、広報、各事業部、等々	社外PoC：自組織外連絡担当
		社内PoC：自組織内連絡担当、
	コンプライアンス、法的要求内容や法令の解釈において、法務部門とCSIRTの橋渡しを行う。	リーガルアドバイザー：リーガルアドバイス担当
	脅威情報、脆弱性情報などを自組織内へ情報発信したり、対応調整などを行う。	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、IT部門調整担当
情報収集・分析	セキュリティ機器から発せられるアラートの調査や予兆を分析し、情報分析担当とともに状況を調査し、インシデント管理担当に報告する。また、脅威情報や自社にかかわる漏えい情報なども収集する。	リサーチャー：情報収集担当
	情報収集担当が集めたデータを分析し、自社に適応すべきかの判断やトリアージを行う際に必要な情報を整理してインシデント管理担当に報告する。	キュレーター：情報分析担当
	自社のシステムについてアプリやインフラに脆弱性があるか検査、診断を行い、評価する。	脆弱性診断士：脆弱性の診断・評価担当
	自社の資産管理の維持管理を行い、最新に保つよう、自社の部門に働きかける。 また、リスクアセスメントを行い、改善項目があれば計画立てて実施する。	セルフアセスメント担当
	自社のセキュリティ機器類の全体設計を行い、有効性評価とともに企画、導入を行う。	ソリューションアナリスト：セキュリティ戦略担当

機能分類	業務内容	役割名称
インシデント対応	平常時、インシデント対応時のCSIRT全体統括を行う。必要であれば、PoCとともに経営者に説明を行う。	コマンダー：CSIRT全体統括担当
	インシデントの情報を情報収集担当や情報分析担当から収集し、CSIRT全体統括へ情報共有する。また、インシデント処理担当へ対応指示を行い、状況を管理し、インシデントレポートを記録する。	インシデントマネージャー：インシデント管理担当
	発生しているインシデント対応を行う。また、影響しているシステムへの対応支援も行う。 セキュリティベンダーを利用している場合にはベンダーとの連携を行う。	インシデントハンドラー：インシデント処理担当
	内部犯罪やサイバークライム事案などの調査を必要であれば警察と連携して行う。	インベスティゲーター：調査・捜査担当
	平常時にはインシデントが発生した時のシステム停止、再開の対応基準を準備しておく。また、インシデント発生時には対応の優先順位をCSIRT全体統括を支援しながら決定する。	トリアージ担当：優先順位選定担当
	機器類の証拠保全やシステム的な鑑識を行い、内部で何が起きているのかの足跡を調査する。また、発見されたマルウェアの解析も行う。	フォレンジック担当
自組織内教育	自組織の一般の役職員に対してセキュリティ教育を行う。CSIRT要員に対する教育は専門家が行う。	教育担当：教育・啓発担当
経営者	セキュリティにかかわる人的、システム的なリソースの手配、インシデント対応も含めたセキュリティ施策の最終判断と責任を持つ。	CISO、CSO、社長など
組織運営 ※CSIRTが特定の部署に属さない場合	CSIRTの予算申請・管理、要員調整、労務管理、工数管理に係わる関係部署との調整を行う。	CSIRT運営管理担当
システム運用 ※CSIRT内でもシステム運用部門でもよい。	CSIRTで利用するセキュリティ機器やネットワーク機器のシステム的な維持管理を行う。	システム運用担当

CSIRTの役割と業務内容の関連図（平常時）

【凡例】
アウトソーシング
自組織保有

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。


経営陣

外部組織

説明・連絡、判断・指示

情報の入手、連絡


PoC

自組織内、自組織外への説明、連絡


リーガルアドバイス担当

法的アドバイス


ノーティフィケーション担当


システム運用担当

自組織内システム、関連システム担当

該当システムでの対応調整

情報集約（システム対応可否、対応時間等）

自組織内関連部署との調整

CSIRT全体統括担当

情報伝達

CSIRT全体統括

設計に反映


セキュリティ戦略担当

システムセキュリティ設計、有効性確認

インシデント管理担当

情報集約（脅威リスク判定等）

必要時に教育に反映

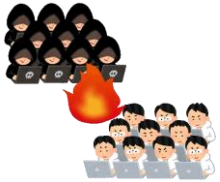
情報集約（影響範囲の報告）

計画策定、推進

インシデントの状況分析


教育・啓発担当

教育


インシデント処理担当

状況確認


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

定期的に実施

インシデントの現場監督・ベンダーとの連携

連携


情報分析担当

インシデントの情報収集、運用しているセキュリティセンサー異常値の発見、影響分析


情報収集担当

脆弱性診断

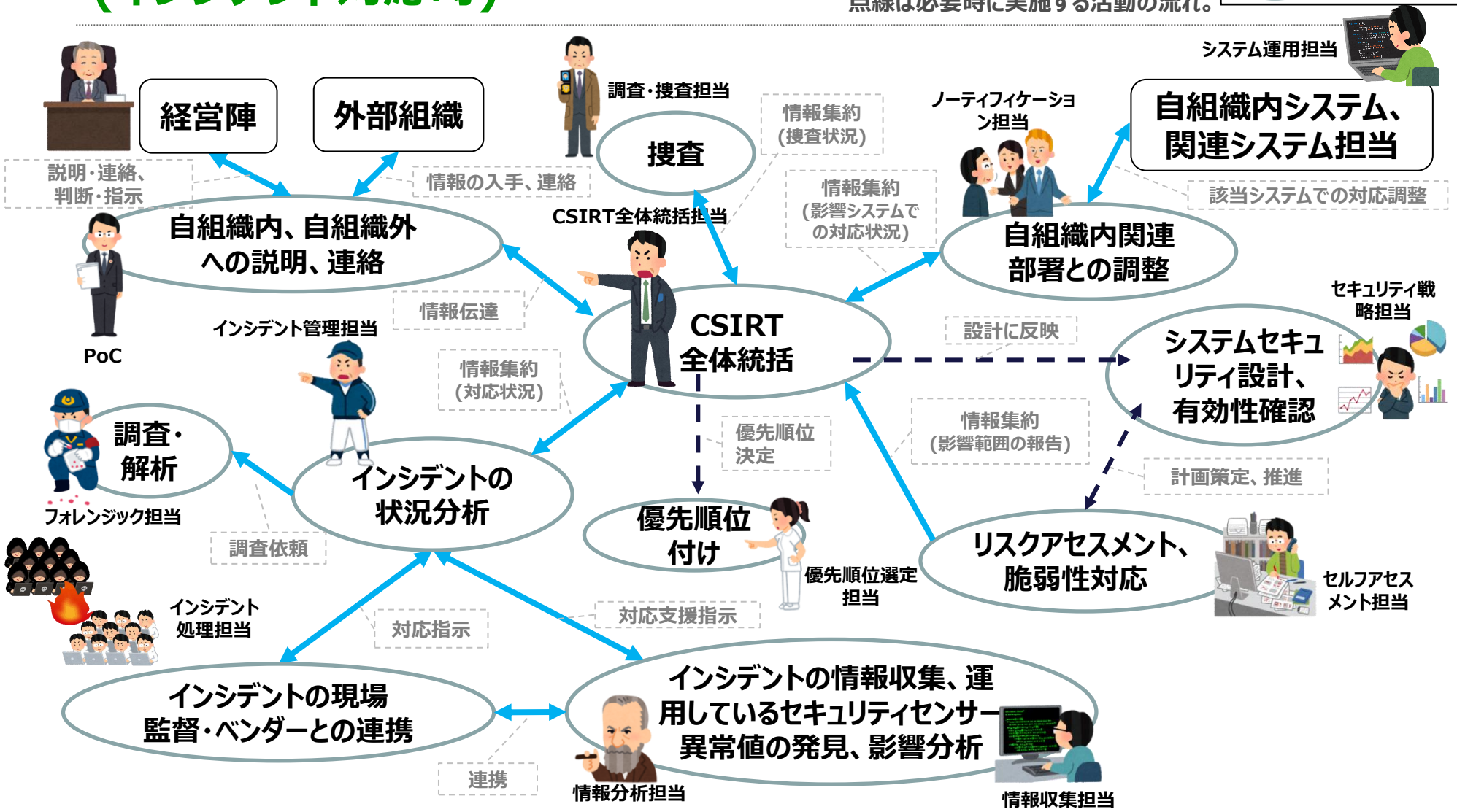

脆弱性の診断・評価担当

＊CSIRT運営管理担当は上記活動のバックグラウンドとして必要である。図には記載していない。
＊システム運用担当は、「自組織内システム、関連システム担当」と同じ場合もあれば、別の場合もある。上記は同じ場合を例示した。

CSIRTの役割と業務内容の関連図（インシデント対応時）

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。

【凡例】
アウトソーシング
自組織保有



＊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
＊法的確認が必要な場合には 各役割からリーガルアドバイザーに支援を要請する。

自組織内での教育プログラム

- 以下の教育プログラムを自組織内で提供
  - 全役割共通の教育プログラム
    - 情報セキュリティに関する独自通信教育プログラム
    - 他社の通信教育プログラム
  - 役割ごとの教育プログラム
    - フォレンジック担当向け独自教材
    - 脆弱性診断士向け独自教材
    - リサーチャー・キュレーター向け独自教材
    - インシデントマネージャー・インシデントハンドラー向け独自教材

モデルD

モデルA～Cに当てはまらない一部の大学などおいて構築・運用されているCSIRTの一例

モデルAに近く、事務の方を中心として、一部の役割をアウトソースしている大学。事務の方が全体統括としてCSIRTを取りまとめている。
モデルBに近く、情報センターを持ち、情報センターの方を中心としてCSIRTを構築している大学。CISO、または情報センターの副CISOがCSIRTを取りまとめている。

モデルD 実装例

- モデルDの実装例として、実例を基に以下の項目について例示する。
  - 自組織で保有する役割とアウトソーシングする役割
  - 自組織内での教育プログラム

自組織で保有する役割とアウトソーシングする役割

下記の役割はすべて実施するが、黄色の部分はアウトソーシングする。CSIRTには、ベンダーと会話できるスキル、自組織内情報共有としてベンダーの言葉を伝えられるスキル、優先順位を決定できるスキル、自組織内教育ができるスキルが必要となる。

機能分類	業務内容	役割名称
情報共有	社内、社外との連絡窓口。経営者に対してはCSIRT全体統括者とともに連絡を行う。 社外の例：NCA、JPCERT/CC、CSIRT、警察、監督官庁、等々 社内の例：法務、渉外、広報、各事業部、等々	社外PoC：自組織外連絡担当
		社内PoC：自組織内連絡担当、
	コンプライアンス、法的要求内容や法令の解釈において、法務部門とCSIRTの橋渡しを行う。	リーガルアドバイザー：リーガルアドバイス担当
	脅威情報、脆弱性情報などを自組織内へ情報発信したり、対応調整などを行う。	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、IT部門調整担当
情報収集・分析	セキュリティ機器から発せられるアラートの調査や予兆を分析し、情報分析担当とともに状況を調査し、インシデント管理担当に報告する。また、脅威情報や自社にかかわる漏えい情報なども収集する。	リサーチャー：情報収集担当
	情報収集担当が集めたデータを分析し、自社に適応すべきかの判断やトリアージを行う際に必要な情報を整理してインシデント管理担当に報告する。	キュレーター：情報分析担当
	自社のシステムについてアプリやインフラに脆弱性があるか検査、診断を行い、評価する。	脆弱性診断士：脆弱性の診断・評価担当
	自社の資産管理の維持管理を行い、最新に保つよう、自社の部門に働きかける。 また、リスクアセスメントを行い、改善項目があれば計画立てて実施する。	セルフアセスメント担当
	自社のセキュリティ機器類の全体設計を行い、有効性評価とともに企画、導入を行う。	ソリューションアナリスト：セキュリティ戦略担当

機能分類	業務内容	役割名称
インシデント対応	平常時、インシデント対応時のCSIRT全体統括を行う。必要であれば、PoCとともに経営者に説明を行う。	コマンダー：CSIRT全体統括担当
	インシデントの情報を情報収集担当や情報分析担当から収集し、CSIRT全体統括へ情報共有する。また、インシデント処理担当へ対応指示を行い、状況を管理し、インシデントレポートを記録する。	インシデントマネージャー：インシデント管理担当
	発生しているインシデント対応を行う。また、影響しているシステムへの対応支援も行う。 セキュリティベンダーを利用している場合にはベンダーとの連携を行う。	インシデントハンドラー：インシデント処理担当
	内部犯罪やサイバークライム事案などの調査を必要であれば警察と連携して行う。	インベスティゲーター：調査・捜査担当
	平常時にはインシデントが発生した時のシステム停止、再開の対応基準を準備しておく。また、インシデント発生時には対応の優先順位をCSIRT全体統括を支援しながら決定する。	トリアージ担当：優先順位選定担当
	機器類の証拠保全やシステム的な鑑識を行い、内部で何が起きているのかの足跡を調査する。また、発見されたマルウェアの解析も行う。	フォレンジック担当
自組織内教育	自組織の一般の役職員に対してセキュリティ教育を行う。CSIRT要員に対する教育は専門家が行う。	教育担当：教育・啓発担当
経営者 （理事会）	セキュリティにかかわる人的、システム的なリソースの手配、インシデント対応も含めたセキュリティ施策の最終判断と責任を持つ。	理事会
組織運営 ※CSIRTが特定の部署に属さない場合	CSIRTの予算申請・管理、要員調整、労務管理、工数管理に係わる関係部署との調整を行う。	CSIRT運営管理担当
システム運用 ※CSIRT内でもシステム運用部門でもよい。	CSIRTで利用するセキュリティ機器やネットワーク機器のシステム的な維持管理を行う。	システム運用担当

CSIRTの役割と業務内容の関連図（平常時）

CSIRT担当が一括して行う場合

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。

【凡例】
アウトソーシング可
自組織保有


理事会

外部組織

説明・連絡、判断・指示

情報の入手、連絡

自組織内、自組織外への説明、連絡


PoC

情報伝達


リーガルアドバイス担当

法的アドバイス


システム運用担当
学部教授

ノーティフィケーション担当

自組織内システム、関連システム担当

該当システムでの対応調整

情報集約（システム対応可否、対応時間等）

自組織内関連部署との調整

CSIRT全体統括担当


CSIRT全体統括

設計に反映

セキュリティ戦略担当

システムセキュリティ設計、有効性確認

インシデント管理担当


情報集約（脅威リスク判定等）

インシデントの状況分析

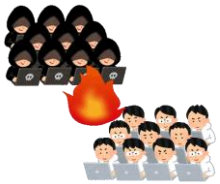
必要時に教育に反映


教育

教育・啓発担当

情報集約（影響範囲の報告）

計画策定、推進


インシデント処理担当

状況確認

リスクアセスメント、脆弱性対応


セルフアセスメント担当

定期的に実施

インシデントの現場監督・ベンダーとの連携


インシデントの情報収集、運用しているセキュリティセンサー異常値の発見、影響分析


情報収集担当

脆弱性診断


脆弱性の診断・評価担当

連携

情報分析担当

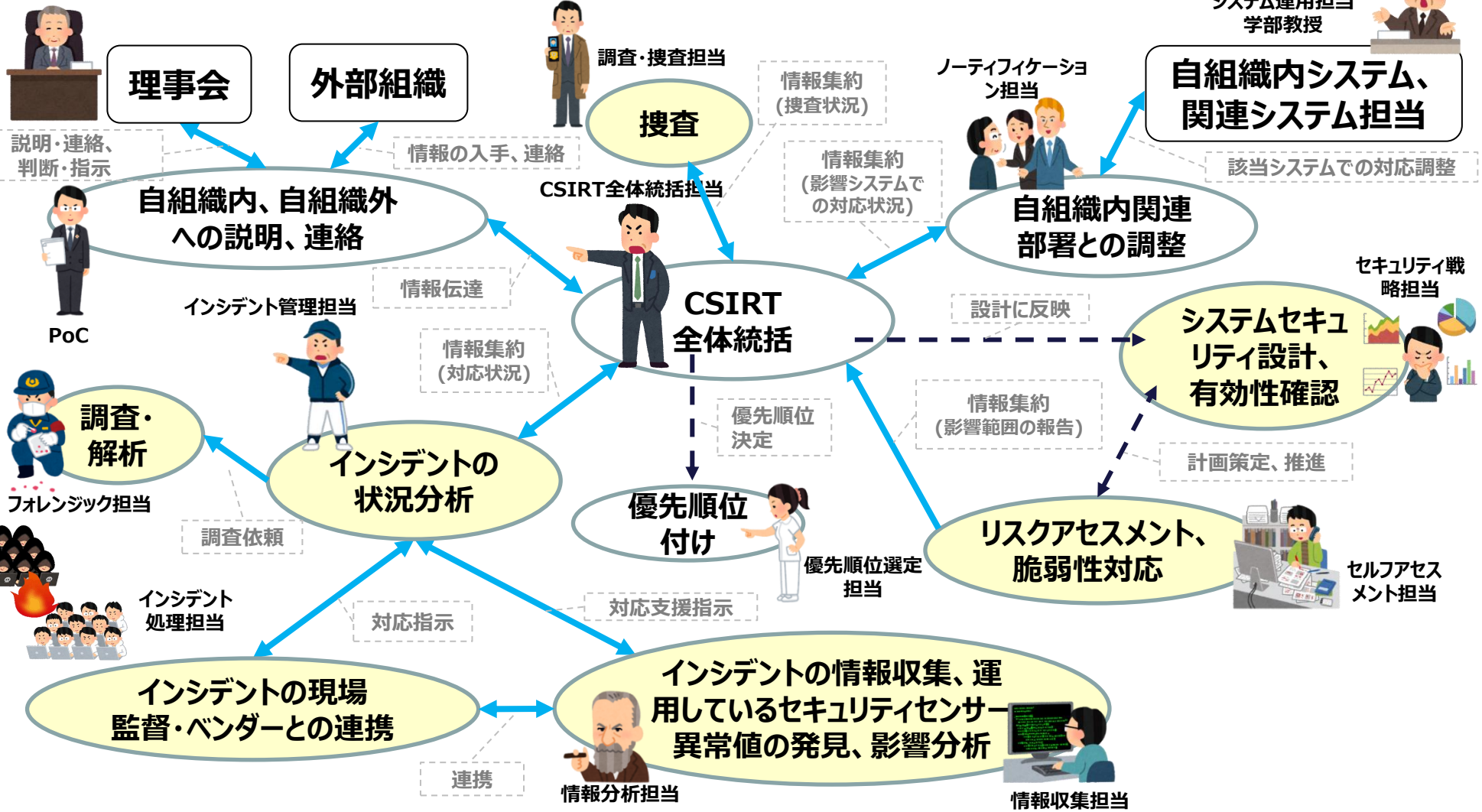
＊CSIRT運営管理担当は上記活動のバックグラウンドとして必要である。図には記載していない。
＊システム運用担当は、「自組織内システム、関連システム担当」と同じ場合もあれば、別の場合もある。上記は同じ場合を例示した。

CSIRTの役割と業務内容の関連図 (インシデント対応時)

CSIRT担当が一括して行う場合

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。

【凡例】
アウトソーシング可
自組織保有



＊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
＊法的確認が必要な場合には 各役割からリーガルアドバイザーに支援を要請する。

CSIRTの役割と業務内容の関連図（平常時）

CSIRT担当とセンター運用者で役割を分割できる場合

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。

【凡例】
- アウトソーシング可
- 自組織保有

理事会

外部組織

説明・連絡、判断・指示

リーガルアドバイス担当

法的アドバイス

システム運用担当
学部教授

自組織内システム、関連システム担当

ノーティフィケーション担当

該当システムでの対応調整

情報の入手、連絡

情報集約（システム対応可否、対応時間等）

PoC

自組織内、自組織外への説明、連絡

情報伝達

CSIRT全体統括担当

CSIRT全体統括

自組織内関連部署との調整

CSIRT担当

インシデント管理担当

情報集約（脅威リスク判定等）

設計に反映

セキュリティ戦略担当

システムセキュリティ設計、有効性確認

必要時に教育に反映

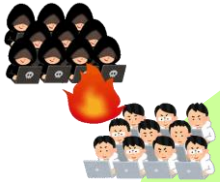
情報集約（影響範囲の報告）

教育

教育・啓発担当

インシデントの状況分析

計画策定、推進



インシデント処理担当

リスクアセスメント、脆弱性対応

セルフアセスメント担当

状況確認

定期的に実施

インシデントの現場監督・ベンダーとの連携

インシデントの情報収集、運用しているセキュリティセンサー異常値の発見、影響分析

情報収集担当

脆弱性診断

脆弱性の診断・評価担当

連携

情報分析担当

センター運用者

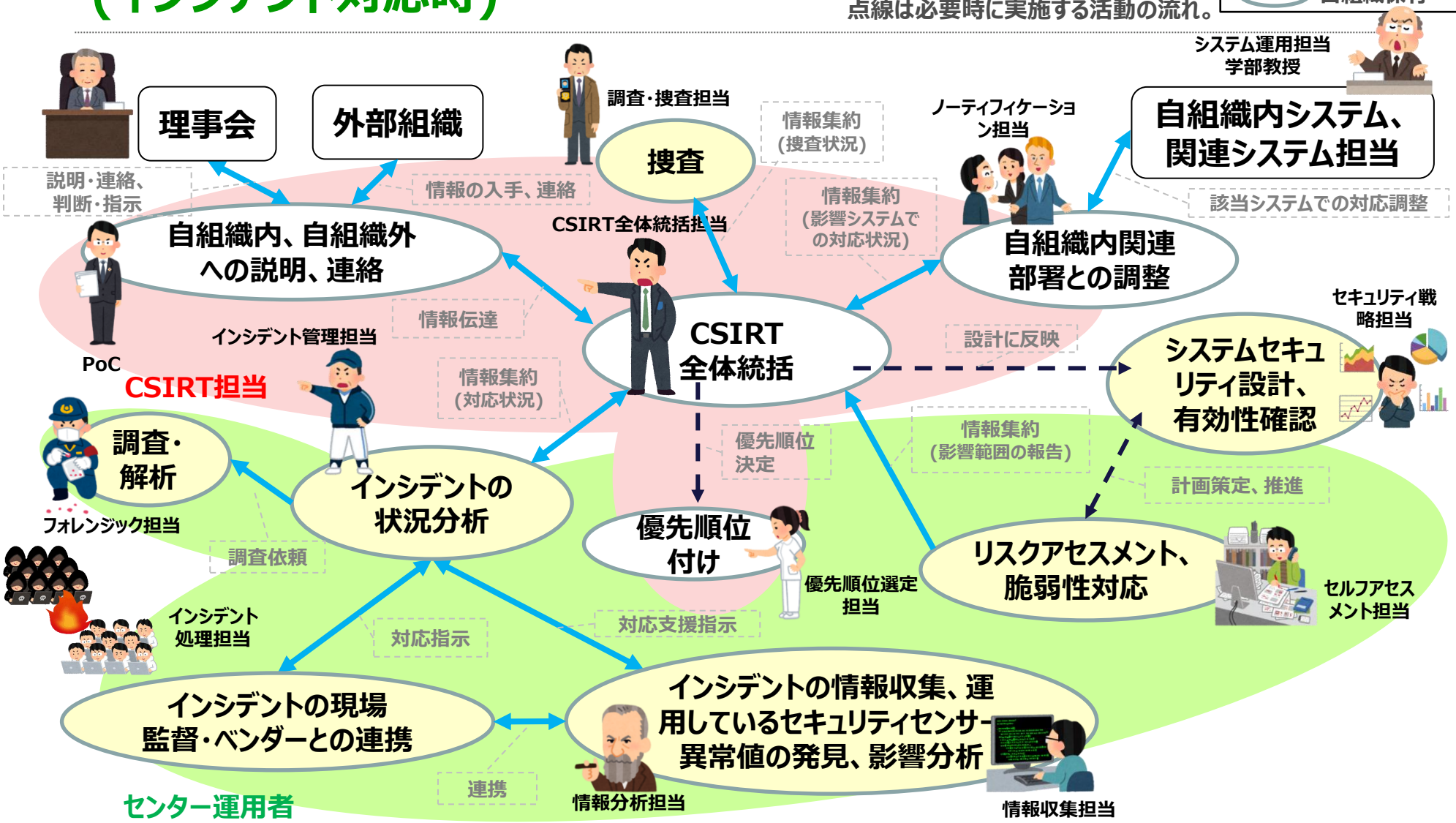
＊CSIRT運営管理担当は上記活動のバックグラウンドとして必要である。図には記載していない。
＊システム運用担当は、「自組織内システム、関連システム担当」と同じ場合もあれば、別の場合もある。上記は同じ場合を例示した。

CSIRT 日本シーサート協議会

CSIRTの役割と業務内容の関連図（インシデント対応時）

CSIRT担当とセンター運用者で役割を分割できる場合
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。

【凡例】
アウトソーシング可
自組織保有



＊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
＊法的確認が必要な場合には 各役割からリーガルアドバイザーに支援を要請する。

自組織内での教育プログラム

- 以下の教育プログラムを自組織内で提供
  - 全役割共通の教育プログラム
    - 自組織のポリシー、セキュリティ規定、管理細則類
    - ISMSやPCIDSSなどの一般的な規定
    - 自組織のシステム構築ガイドライン類
    - 自組織の運用規定類、業務システム概要
    - セキュリティ機器、設備の詳細、SOC判断基準
    - リスクアセスメント、監査手法
    - CSIRT行動要領
    - インシデント対応を想定した演習
  - 役割ごとの教育プログラム
    - CSIRTとしての平常時、インシデント対応時の役割毎OJT
    - 他CSIRTとの意見交換

※実施内容は大学によって異なる

6.おわりに

- 最新のバージョン（ver. 2.1）においてはCSIRT要員に必要なスキルや登用後の更なる成長や育成も踏まえた記述や、アウトソーシング・役割連携などの内容も拡充しています。本資料によって各組織内CSIRTにおける課題が解決または緩和されることを祈っております。
- なお、ご不明な点がある場合は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事務局までお問い合わせください。

【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事務局】
- 住所：東京都中央区日本橋本町 4-4-2 東山ビルディング 8 階
- 電話番号： 03-6271-8901
- メール：nca-sec@nca.gr.jp

付録1.モデル別アウトソーシング役割の比較

黄色の役割はアウトソーシング

機能分類	役割名称	モデルA	モデルB	モデルC	モデルD
情報共有	社外PoC：自組織外連絡担当				
	社内PoC：自組織内連絡担当、				
	リーガルアドバイザー：リーガルアドバイス担当				
	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、IT部門調整担当				
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	✓	✓		✓
	脆弱性診断士：脆弱性の診断・評価担当	✓	✓		✓
	セルフアセスメント担当	✓			✓
	ソリューションアナリスト：セキュリティ戦略担当	✓			✓

機能分類	役割名称	モデルA	モデルB	モデルC	モデルD
インシデント対応	コマンダー：CSIRT全体統括担当				
	インシデントマネージャー：インシデント管理担当	✓			✓
	インシデントハンドラー：インシデント処理担当	✓			✓
	インベスティゲーター：調査・捜査担当	✓			✓
	トリアージ担当：優先順位選定担当				
	フォレンジック担当	✓	✓		✓
自組織内教育	教育担当：教育・啓発担当				
経営者	CISO、CSO、社長など				
組織運営 ※CSIRTが特定の部署に属さない場合	CSIRT運営管理担当				
システム運用 ※CSIRT内でもシステム運用部門でもよい。	システム運用担当	✓			✓

付録2.各種標準のご紹介

- **ISMS : Information Security Management System**
  - （参考）ISMS適合性評価制度
    - URL： https://isms.jp/isms.html
- **ITSS : Information Technology Skill Standard**
  - （参考）ITスキル標準関連
    - URL： https://www.ipa.go.jp/jinzai/itss/
- **PCIDSS : Payment Card Industry Data Security Standard**
  - （参考）PCI DSSとは
    - URL： https://www.jcdsc.org/pci_dss.php

付録3.略称について

略称	詳細
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
CSO	Chief Security Officer
NCA	Nippon CSIRT Association
OJT	On the Job Training
PoC	Point of Contact
RFP	Request for Proposal
SOC	Security Operation Center

CSIRT人材ワーキンググループ著者一覧

阿部 恭一	ASY-CSIRT	ANAシステムズ株式会社
岩井 洋	ASY-CSIRT	ANAシステムズ株式会社
柴山 芳則	AW-CSIRT	株式会社アルファ・ウェーブ
吉田 美佐子	DMM.CSIRT	合同会社 DMM.com
細野 英朋	DMM.CSIRT	合同会社 DMM.com
青木 一郎	DMM.CSIRT	合同会社 DMM.com
大谷 なすか	DMM.CSIRT	合同会社 DMM.com
中島 亜理沙	DMM.CSIRT	合同会社 DMM.com
鬼松 嵩	FURUNO CSIRT	古野電気株式会社
原 健士	FURUNO CSIRT	古野電気株式会社
生田 有香	FURUNO CSIRT	古野電気株式会社
村上 暁	FURUNO CSIRT	古野電気株式会社
村上 祐介	FURUNO CSIRT	古野電気株式会社
田村 進司	FURUNO CSIRT	古野電気株式会社
川口 耕平	Glico-S	江崎グリコ株式会社
木村 和泉	Glico-S	江崎グリコ株式会社
松方 岩雄	JBS-CIRT	日本ビジネスシステムズ株式会社
林 健太郎	JBS-CIRT	日本ビジネスシステムズ株式会社
山尾 茂	JFE-SIRT	JFEホールディングス株式会社
稲井 紀茂	JST-CSIRT	株式会社Jストリーム
志田 勇太	KIRIN-CSIRT	キリンビジネスシステム株式会社
大塚 裕成	KIRIN-CSIRT	キリンビジネスシステム株式会社
村上 晃	LACERT	株式会社ラック
東梅 大輔	MARUI_CSIRT	株式会社エムアンドシーシステム
佐藤 芳紀	MB-SIRT	森ビル株式会社
寺西 照一	MI-CSIRT	株式会社 三越伊勢丹システム・ソリューションズ
下別府 遼	Mynavi-CSIRT	株式会社マイナビ
梶谷 恵介	Mynavi-CSIRT	株式会社マイナビ
鳥越　真理子	NCSIRT	NRIセキュアテクノロジーズ株式会社
佐藤 篤志	NTT EAST-CIRT	東日本電信電話株式会社
伊藤 祐樹	NTT-CERT	日本電信電話株式会社
杉浦 芳樹	NTT-CERT	日本電信電話株式会社
橋詰 真美	NTTDATA-CERT	株式会社 NTT データ
大谷 尚通	NTTDATA-CERT	株式会社 NTT データ
野呂 優介	NTTDATA-CERT	株式会社 NTT データ
馮 菲	NTTDATA-CERT	株式会社 NTT データ
野村 武史	OMRON-SIRT	オムロン株式会社
林 裕二	OMRON-SIRT	オムロン株式会社
井出 雄介	PIRATES	東京海上日動リスクコンサルティング株式会社
大河内 智秀	PIRATES	東京海上日動リスクコンサルティング株式会社
岡村 耕二	Qdai CSIRT	国立大学法人 九州大学
亀田 祥世	Rakuten-CERT	楽天ウォレット株式会社
丸岡 航太	SBT-CSIRT	SBテクノロジー株式会社
土屋 幸三	SBT-CSIRT	SBテクノロジー株式会社
前畑 隆志	Simplex-CSIRT	シンプレクス・ホールディングス株式会社
松本 勝之	SoftBank CSIRT	ソフトバンク株式会社
李 玉莉	SoftBank CSIRT	ソフトバンク株式会社
池田 望	TOPPAN-CERT	凸版印刷株式会社
石原 篤	transcosmos-CSIRT	トランスコスモス株式会社
高橋 祐一	UACJ-SIRT	株式会社UACJ
平井 重信	UACJ-SIRT	株式会社UACJ
堀江 剛史	UACJ-SIRT	株式会社UACJ
茂木 章	UACJ-SIRT	株式会社UACJ
山賀 正人	専門委員	日本シーサート協議会

※CSIRT名、会社名は執筆時点のもの

謝辞

本資料作成にご協力頂きましてありがとうございました。
厚く御礼申し上げます。

産業横断サイバーセキュリティ人材育成検討会 事務局長　　荒川 大　様
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の皆様

改版履歴

- 2015.11.16 Ver1.0 初版作成
- 2017.03.13 Ver1.5 改訂
- 2019.10.29 Ver2.0 改訂
- 2020.12.11 Ver2.1 改訂