CSIRT人材の定義と確保(Ver.1.5)

2017年3月13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人材サブワーキンググループ(CSIRT人材SWG)

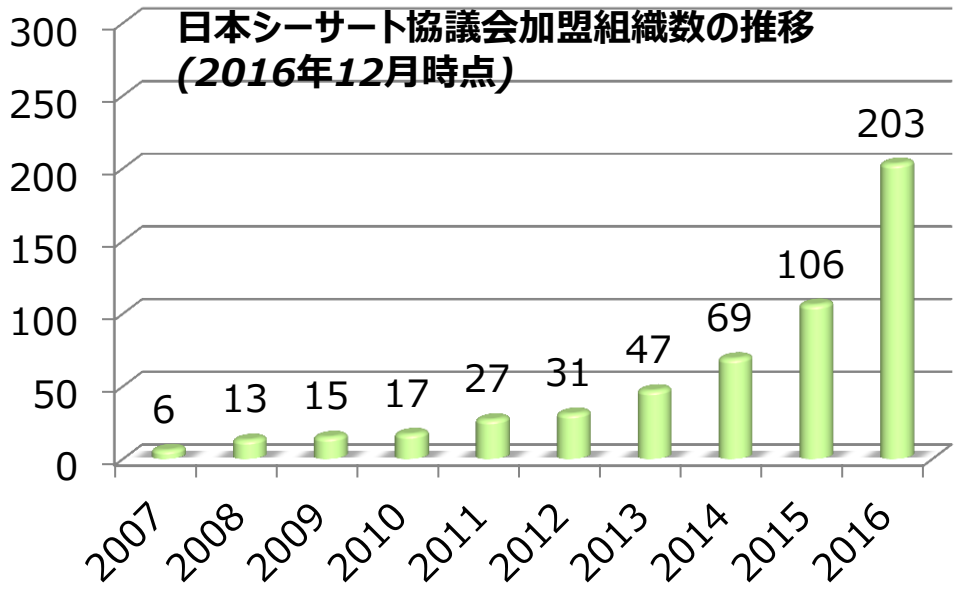
目次

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3つのモデルに分けて解説している。なお、 CSIRT人材SWG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、３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を組織する役割りの定義 ✓ 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	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

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、IT部門調整担当

社外窓口として、JPCERT/CC、NISC、警察、監督官庁、NCA、他CSIRT等との連絡窓口となり、情報連携を行う。
社内窓口として、IT部門、法務、渉外、IT部門、広報、各事業部等との連絡窓口となり、情報連携を行う。

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」

法務担当

情報技術やサイバーセキュリティなどにおける法課題やコンプライアンス問題が発生した時に法的アドバイスを行う。法務部がITスキルに乏しい場合にはIT担当が法務部向けに翻訳して橋渡しする形でもよい。

任用前提スキル

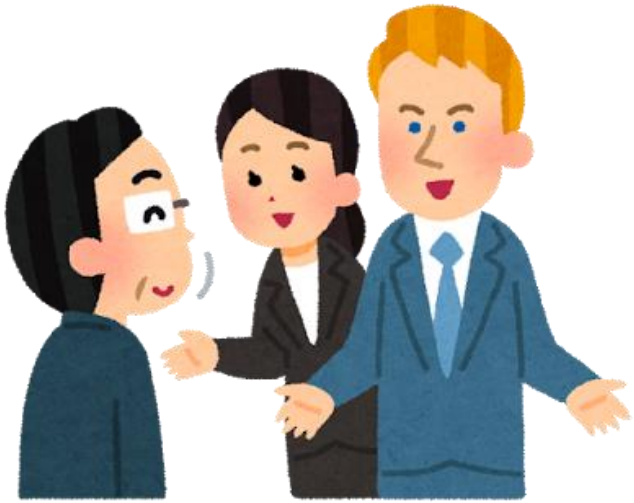
- ✓ セキュリティに関わる関連法の知識、もしくはITSSレベル２程度の基礎的なITリテラシー
- ✓ サイバーセキュリティに関連する技術的動向、法的なトレンドの追跡、解析ができる能力。
- ✓ 情報を正しく伝えるコミュニケーション能力

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
自組織内を調整し、各関連部署への情報発信を行う。自組織システムに影響を及ぼす場合にはIT部門と調整を行う。



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

セキュリティイベント、脅威情報、脆弱性情報、攻撃者のプロファイル情報、国際情勢の把握、メディア情報などを収集し、キュレーターに引き渡す。単独機器の分析は行うが、相関的な分析はしない。

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

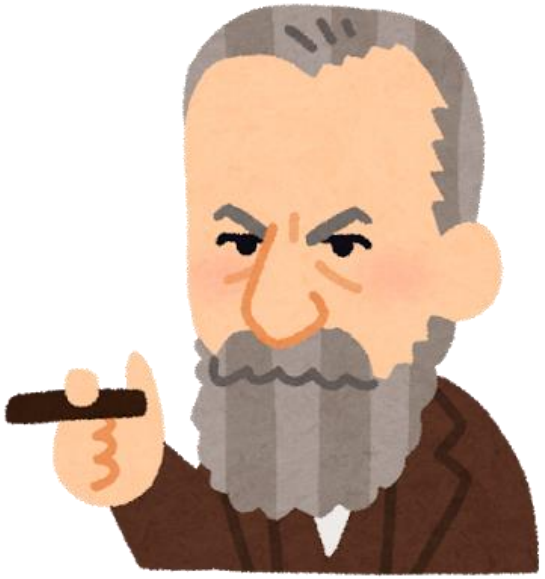
- ✓ 国家間の関係、ハクティビスト*に関する知識
- ✓ メディアの特性を知り、活用できる能力
- ✓ セキュリティ機器で検出される情報を正しく読む能力
- ✓ 攻撃戦術、ステージ、技術、手順に関する知識

*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

リサーチャーの収集した情報を分析し、その情報を自組織に適用すべきかの選定を行う。リサーチャーと合わせてSOC（セキュリティオペレーションセンター）で実施することが多い。



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
OS、ネットワーク、ミドルウェア、アプリケーションが安全かどうかの検査を行い、診断結果の評価を行う。

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
自組織環境や情報資産の現状分析を行う。平常時の際にアセスメントを実施しておき、インシデント発生時にはアセスメント結果に基づいて影響範囲を特定する。

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

自組織の事業計画に合わせてセキュリティ戦略を策定する。現在の状況とあるべき姿のFit&Gap分析からリスク評価を行い、ソリューションマップを作成して導入を推進する。導入されたソリューションの有効性を確認し、経営層と情報共有を行い、改善計画に反映する。

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

自組織で起きているセキュリティインシデントの全体統制を行う。重大なインシデントに関してはCISOや経営層との情報連携を行う。また、CISOや経営者が意思決定する際の支援を行う。

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
- ✓ 経営層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

インシデントハンドラーに指示を出し、インシデントの対応状況を把握する。対応履歴を管理するとともにコマンダーへ状況を報告する。

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
インシデントの処理を行う。セキュリティベンダーに処理を委託している場合には指示を出して連携し、管理を行う。状況はインシデントマネージャーに報告する。

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

外部からの犯罪、内部犯罪を捜査する。セキュリティインシデントはシステム障害とは異なり、悪意のある者が存在する。通常の犯罪捜査と同様に、動機の確認や証拠の確保、次に起こる事象の推測などを詰めながら論理的に捜査対象を絞っていくことが要求される。

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

発生している事象に対して優先順位を決定する。被害がある場合の復旧優先順位や、拡散している場合にはどのシステムから停止していくべきか等の判断を行う。

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

システム的な鑑識、精密検査、解析、報告を行う。悪意のある者は証拠隠滅を図ることもあるため、証拠保全とともに、消されたデータを復活させ、足跡を追跡することも要求される。

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」

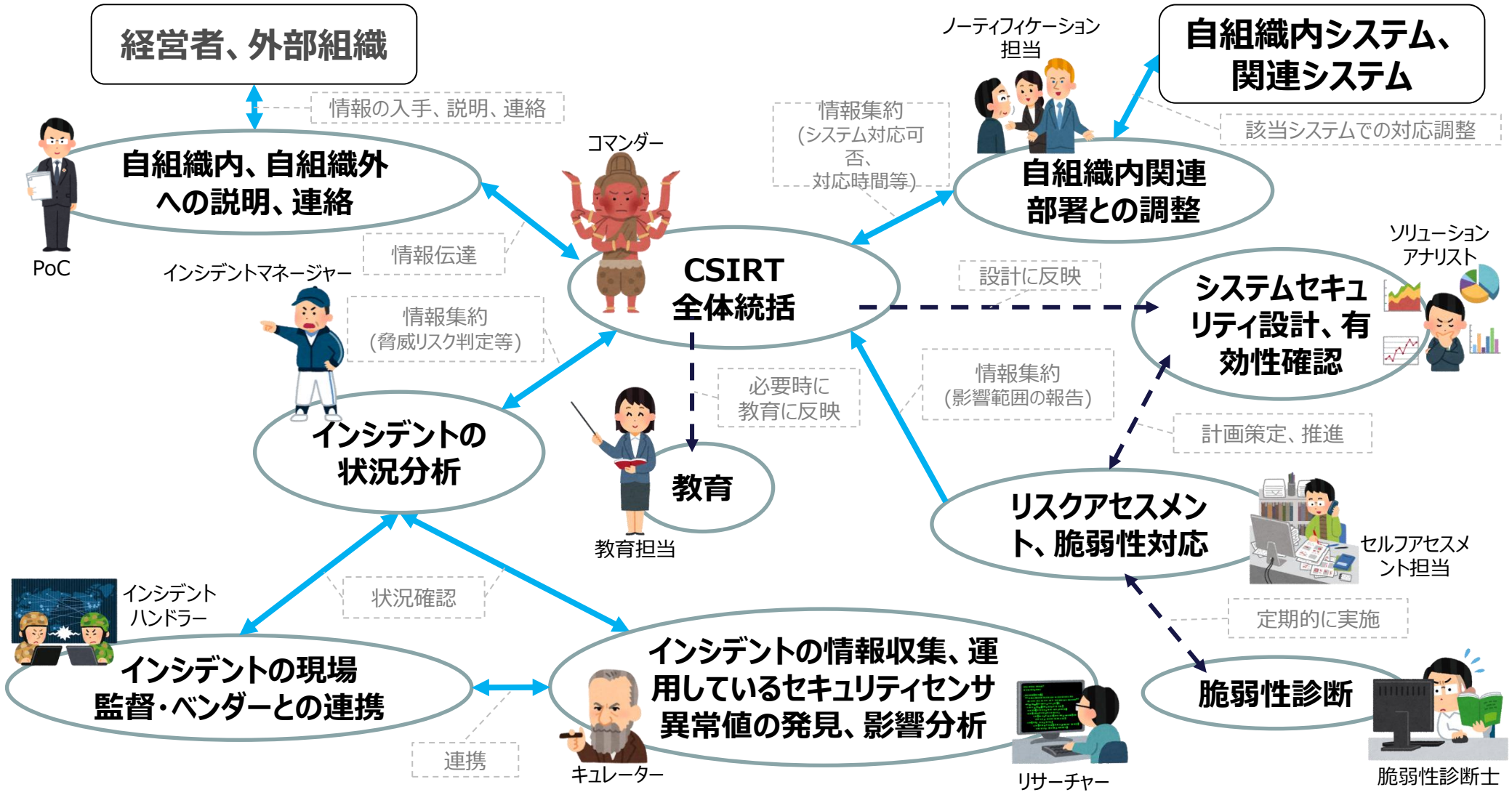
教育・啓発担当
主に役職員向けの教育を実施し、リテラシーの向上を図る。
CSIRT向けの専門トレーニングについては別担当にしてもよい。

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

4.16 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。

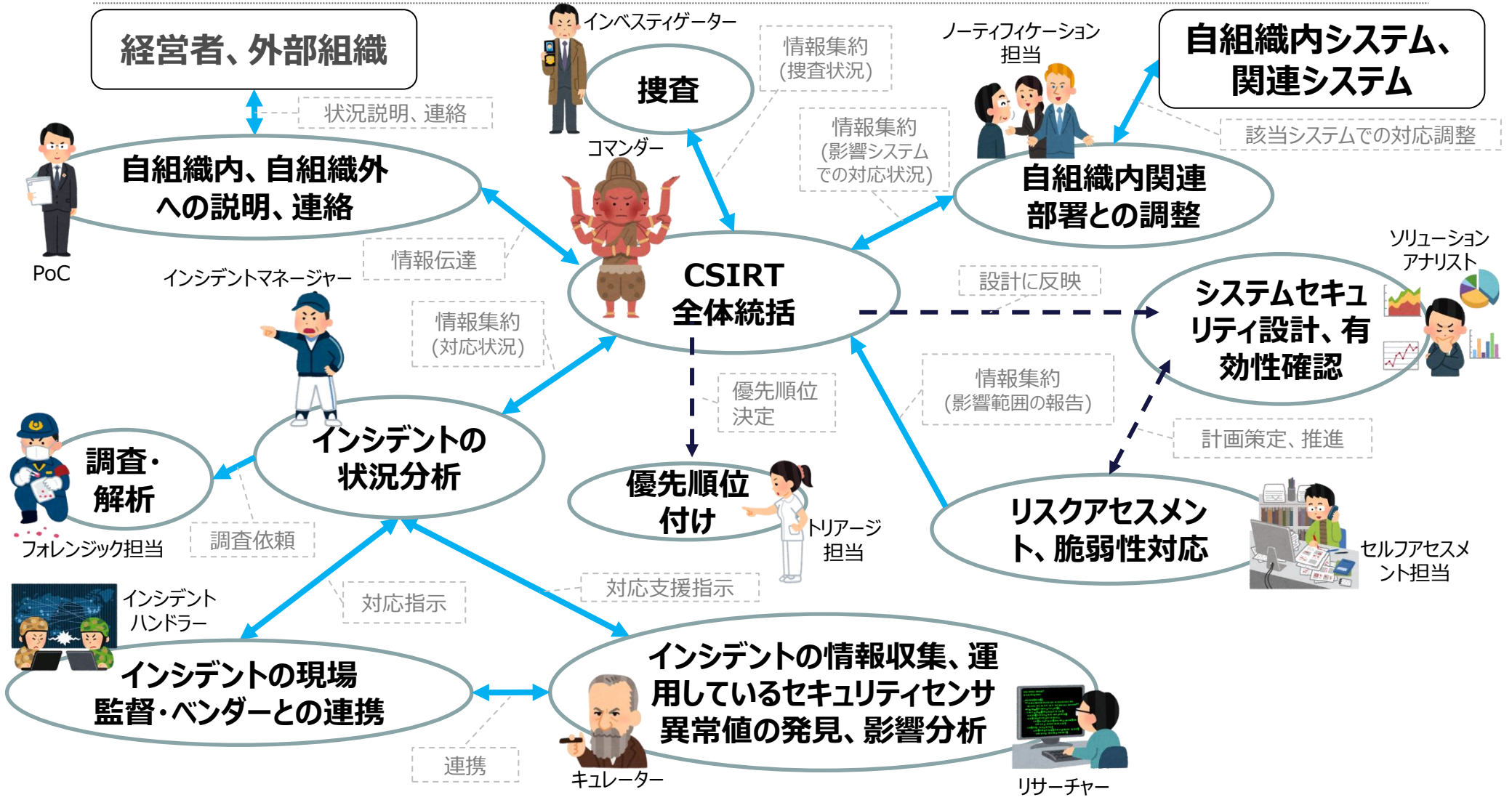


＊法的確認や日常的にアドバイスが必要な場合には 各役割からリーガルアドバイザーに支援を要請する。

※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

4.16 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。



＊法的確認や日常的に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。

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～C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	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D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。

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	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	自組織内のリテラシー向上、底上げ

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。また、青線や黒線は自組織における連携、緑線はアウトソーシング先との連携を意味している。

【凡例】
アウトソーシング
自組織保有

経営者、外部組織

自組織内、自組織外への説明、連絡

PoC

コマンダー

CSIRT全体統括

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

自組織内関連部署との調整

対応ベンダー(設計提案)

ソリューションアナリスト

システムセキュリティ設計、有効性確認

インシデントマネージャー

インシデントの状況分析

対応ベンダー(調査統括)

教育

教育担当

対応ベンダー(実施)

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

インシデントハンドラー

インシデントの現場監督・ベンダーとの連携

対応ベンダー(インシデント対応)

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異常値の発見、影響分析

キュレーター

リサーチャー

脆弱性診断

脆弱性診断士

対応ベンダー(実施)

対応ベンダー(MSS、インテリジェンス)

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)

※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。また、青線や黒線は自組織における連携、緑線はアウトソーシング先との連携を意味している。

【凡例】
アウトソーシング
自組織保有

経営者、外部組織

自組織内、自組織外への説明、連絡

PoC

インベスティゲーター

捜査

対応ベンダー(調査実施)

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

コマンダー

自組織内関連部署との調整

対応ベンダー(有効性確認)

ソリューションアナリスト

CSIRT全体統括

システムセキュリティ設計、有効性確認

インシデントマネージャー

対応ベンダー(インシデント対応統括)

対応ベンダー(フォレンジック実施)

調査・解析

フォレンジック担当

インシデントの状況分析

優先順位付け

トリアージ担当

対応ベンダー(影響調査実施)

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

インシデントハンドラー

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異常値の発見、影響分析

キュレーター

リサーチャー

対応ベンダー(インシデント対応)

対応ベンダー(MSS、インテリジェンス)

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。
  - アウトソーシング役割
  - 自組織内での教育プログラム

アウトソーシング役割

- 自組織のビジネスインパクトに関わる判断部分、自組織内連絡の役割以外はアウトソーシングする。

機能分類	役割名称	業務内容
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	セキュリティ機器類の状況監視、インシデント判断などの定例業務を行う。ただし、自組織システムの状況と相関分析して判断する場合が多いため、自組織システムの維持要員と協力して行う。 ベンダー、外部からの入手情報については、専門性を活かした分析や国際情勢の把握に基づき、リスク判断を行う。インシデント対応時には事象の背景なども調査する。
	脆弱性診断士：脆弱性の診断担当	ツールを使用したインフラの検査やアプリケーションの検査などは自組織で行うことも可能であるが、ペネトレーションレベルに対してはアウトソーシングして専門家に委託する。
	脆弱性診断士：脆弱性の評価担当	ツールを使用した分析は自組織で行うことも可能であるが、評価の妥当性については専門家の意見を参考にする。
	セルフアセスメント担当	自組織保有の情報資産のリスクアセスメントを行い、脆弱性対応に対する影響調査や、インシデント対応時の影響調査に役立てる。
	ソリューションアナリスト：セキュリティ戦略担当	セキュリティ全体計画の策定や有効性の評価を行う。
インシデント対応	インシデントマネージャー：インシデント管理担当	インシデント全体の把握。コマンダーへの報告。対応履歴把握を行う。
	インシデントハンドラー：インシデント処理担当	インシデント対応を行う。
	インベスティゲーター：調査・捜査担当	内偵の場合には自組織内の総務部などと連携して調査を行う。
	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、マルウェア解析については専門家に委託する。

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
    - CSIRTとしての平常時、インシデント対応時の演習
  - 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。

自組織で保有する役割とアウトソーシングする役割

- 自組織内関連部著との調整や、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	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	自組織内のリテラシー向上、底上げ

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。また、青線や黒線は自組織における連携、緑線はアウトソーシング先との連携を意味している。

【凡例】
アウトソーシング
自組織保有

経営者、外部組織

自組織内、自組織外への説明、連絡

PoC

コマンダー

CSIRT全体統括

インシデントマネージャー

インシデントの状況分析

教育

教育担当

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

自組織内関連部署との調整

ソリューションアナリスト

システムセキュリティ設計、有効性確認

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

インシデントハンドラー

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異常値の発見、影響分析

キュレーター

リサーチャー

脆弱性診断

脆弱性診断士

対応ベンダー(実施)

対応ベンダー(MSS、インテリジェンス)

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)

※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。また、青線や黒線は自組織における連携、緑線はアウトソーシング先との連携を意味している。

【凡例】
アウトソーシング
自組織保有

経営者、外部組織

自組織内、自組織外への説明、連絡

PoC

インベスティゲーター

捜査

コマンダー

CSIRT全体統括

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

自組織内関連部署との調整

ソリューションアナリスト

システムセキュリティ設計、有効性確認

インシデントマネージャー

対応ベンダー(フォレンジック実施)

調査・解析

フォレンジック担当

インシデントの状況分析

優先順位付け

トリアージ担当

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

インシデントハンドラー

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異常値の発見、影響分析

キュレーター

リサーチャー

対応ベンダー(MSS、インテリジェンス)

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。
  - アウトソーシング役割
  - 自組織内での教育プログラム

アウトソーシング役割

- 自組織のコアビジネス以外の部分やスキルに高度な専門性を要する役割についてはアウトソーシングする。

機能分類	役割名称	業務内容
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	セキュリティ機器類の状況監視、インシデント判断などの定例業務を行う。ただし、自組織システムの状況と相関分析して判断する場合が多いため、自組織システム維持要員と協力して行う。 ベンダー、外部からの入手情報については、専門性を活かした分析や国際情勢の把握に基づき、リスク判断を行う。インシデント対応時には事象の背景なども調査する。
	脆弱性診断士：脆弱性の診断担当	ツールを使用したインフラの検査やアプリケーションの検査などは自組織で行うことも可能であるが、ペネトレーションレベルに対してはアウトソーシングして専門家に委託する。
	脆弱性診断士：脆弱性の評価担当	ツールを使用した分析は自組織で行うことも可能であるが、評価の妥当性については専門家の意見を参考にする。
インシデント対応	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、マルウェア解析については専門家に委託する。

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
    - CSIRTとしての平常時、インシデント対応時の演習
  - 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。

自組織で保有する役割とアウトソーシングする役割

■ すべての役割と自組織保有とする。

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	自組織内のリテラシー向上、底上げ

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。また、青線や黒線は自組織における連携を意味している。

【凡例】
アウトソーシング
自組織保有

経営者、外部組織

自組織内、自組織外への説明、連絡

PoC

コマンダー

CSIRT全体統括

インシデントマネージャー

インシデントの状況分析

教育

教育担当

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

自組織内関連部署との調整

ソリューションアナリスト

システムセキュリティ設計、有効性確認

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

インシデントハンドラー

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異常値の発見、影響分析

キュレーター

リサーチャー

脆弱性診断

脆弱性診断士

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。また、青線や黒線は自組織における連携を意味している。

【凡例】
アウトソーシング
自組織保有

経営者、外部組織

インベスティゲーター

捜査

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

自組織内、自組織外への説明、連絡

コマンダー

自組織内関連部署との調整

PoC

CSIRT全体統括

ソリューションアナリスト

システムセキュリティ設計、有効性確認

インシデントマネージャー

インシデントの状況分析

調査・解析

フォレンジック担当

優先順位付け

トリアージ担当

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

インシデントハンドラー

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異常値の発見、影響分析

キュレーター

リサーチャー

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。
  - アウトソーシング役割
  - 自組織内での教育プログラム

アウトソーシング役割

- 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
  - 補助的にベンダーに作業をアウトソーシングする場合はあり

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

6.おわりに

- 最新のバージョン（ver.1.5）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シーサート協議会事務局までお問い合わせください。

【日本シーサート協議会事務局】

- 住所：東京都千代田区神田錦町3-17 廣瀬ビル11階
- 電話番号： 03-3518-4600
- メール：nec-sec@nca.gr.jp

付録1.モデル別アウトソーシング役割の比較

機能分類	役割名称	モデル A	モデル B	モデル C
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、IT部門調整担当			
	リーガルアドバイザー：法務部CSIRT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			
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：脆弱性の診断担当	✓	✓	
	脆弱性診断士：脆弱性の評価担当	✓	✓	
	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	✓		
インシデント対応	コマンダー：CSIRT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	✓		
	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			

黄色の役割はアウトソーシング

付録2.募集要項のサンプル

【サンプル】XX-CSIRT担当者募集（リサーチャー、キュレーター）

募集件名	【急募】CSIRT担当者(リサーチャー、キュレーター)
採用数	若干名
職務内容(ロール)	セキュリティログを確認し、特異点を見つけて担当にエスカレーション。 典型的な職務内容(ロール)：PC操作
必要な経験、能力、資格	経験：サーバ、ネットワーク構築・運用経験 能力：PC、Linux操作一般 資格：特に規定なし ヒューマンスキル：緻密な作業が得意な方。会話が苦手な方も可
あると望ましい経験、能力、資格	経験：サーバログ、ファイアウォールログ等のログ分析経験 能力：持久力、集中力 資格：特になし
導入教育	ログの分析の仕方を要領書を基に教育します。
休日・休暇	週休2日制、短時間勤務、シフト勤務も要相談。
備考	成長産業！企業のリスク回避につながる注目の仕事です！ 高齢者、第二新卒も可。

【サンプル】XX-CSIRT担当者募集（ソリューションアナリスト）

募集件名	【急募】CSIRT担当者(ソリューションアナリスト)
採用数	若干名
職務内容(ロール)	セキュリティに関する機器類の全体設計やポリシーを維持、管理。 開発案件についてガイドラインを遵守しているかどうかのチェックを行う。
必要な経験、能力、資格	経験：サーバ、ネットワーク構築・運用経験 能力：PC、Linux知識一般 資格：特に規定なし ヒューマンスキル：開発者と会話できる持久力、対応力
あると望ましい経験、能力、資格	経験：サーバログ、ファイアウォールログ等のログ分析経験 能力：本質を見極める力、応用力 資格：情報処理関係
導入教育	現在のポリシーやガイドラインの背景・内容を教育します。
休日・休暇	週休２日制、短時間勤務、シフト勤務、自宅勤務も要相談。
備考	成長産業！日々発展するITを活用する最先端の仕事です。

【サンプル】XX-CSIRT担当者募集（セルフアセスメント・教育担当）

募集件名	【急募】CSIRT担当者(セルフアセスメント・教育担当)
採用数	若干名
職務内容(ロール)	各職場で培ってきた経験を生かして、職場のリスクアセスメントを行い、資料を作成。ガイドラインに基づいた教育を実施。
必要な経験、能力、資格	経験：要件調整、仕様調整の経験 能力：ヒアリング力、分析力、表現力、プレゼン力 資格：特になし ヒューマンスキル：コミュニケーション能力、温和で学習熱心な方
あると望ましい経験、能力、資格	経験：リスクアセスメント、監査などの経験、教育経験 能力：人と打ち解ける、安心させられる能力 資格：ISMS審査員、監査員
導入教育	アセスメント方針やチェックポイント、ガイドラインは事前に教育します。セキュリティ教育も実施します。
休日・休暇	時短・在宅勤務も要相談。
備考	セキュリティ教育制度あり。高齢者も可。

付録3.各種標準のご紹介

- **ISMS : Information Security Management System**
  - 情報セキュリティマネジメントシステム
    - 参考URL：https://www.isms.jipdec.or.jp/isms/
- **ITSS : Information Technology Skill Standard**
  - ITスキル標準
    - 参考URL： http://www.ipa.go.jp/jinzai/itss/
- **PCIDSS : Payment Card Industry Security Standards Council**
  - PCIデータセキュリティスタンダード
    - 参考URL： http://www.jcdsc.org/pci_dss.php

付録4.略称について

略称	詳細
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
FIRST	Forum of Incident Response and Security Teams
MSS	Managed Security Service
NCA	Nippon CSIRT Association
NISC	National center of Incident readiness and Strategy for Cybersecurity
OJT	On the Job Training
PoC	Point of Contact
RFP	Request for Proposal
SOC	Security Operation Center

CSIRT人材サブ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
羽場 満	Canon-CSIRT	キヤノン株式会社
川口 晃司	Canon MJ-CSIRT	キヤノンマーケティングジャパン株式会社
藤谷 あゆみ	Canon MJ-CSIRT	キヤノンマーケティングジャパン株式会社
伊藤 彰嗣	Cy-SIRT	サイボウズ株式会社
渡辺 文恵	DeNA CERT	株式会社ディー・エヌ・エー
橋村 泰慶	DIR-CSIRT	株式会社大和総研ホールディングス
青木 一郎	DMM.CSIRT	株式会社DMM.comラボ
寺西 一平	DMM.CSIRT	株式会社DMM.comラボ
吉川 利治	DOCOMO-CSIRT	株式会社 NTTドコモ
佳山 こうせつ	FJC-CERT	富士通株式会社
寺田 真敏	HIRT	株式会社日立製作所
沼田 亜希子	HIRT	株式会社日立製作所
徳田 敏文	IBM-CSIRT	日本アイ・ビー・エム株式会社
吉田 香織	iD-SIRT	株式会社インフォメーション・ディベロプメント
松方 岩雄	JBS-CIRT	日本ビジネスシステムズ株式会社
井出 雄介	JFE-SIRT	JFEホールディングス株式会社
高杉 秋子	JPBank CSIRT	株式会社ゆうちょ銀行
森下 明宏	JPBank CSIRT	株式会社ゆうちょ銀行
満永 拓邦	JPCERT/CC	一般社団法人JPCERTコーディネーションセンター
佐藤 芳紀	MB-SIRT	森ビル株式会社
大河内 智秀	MBSD-SIRT	三井物産セキュアディレクション株式会社
鳥島 由美子	MBSD-SIRT	三井物産セキュアディレクション株式会社
渡辺 隆志	mixirt	株式会社ミクシィ
杉浦 芳樹	NTT-CERT	日本電信電話株式会社
関戸 直生	NTT-CERT	日本電信電話株式会社
二関 学	NTT-CERT	日本電信電話株式会社
溝口 和寛	NTT-CERT	日本電信電話株式会社
大山 千尋	NTTDATA-CERT	株式会社NTTデータ
菊池　隆	OCE-CSIRT	株式会社大崎コンピュータエンヂニアリング
笹川 一宏	OCE-CSIRT	株式会社大崎コンピュータエンヂニアリング
松本 勝之	SoftBank CSIRT	ソフトバンク株式会社
萩原 健太	TM-SIRT	トレンドマイクロ株式会社
六宮 智悟	TM-SIRT	トレンドマイクロ株式会社
池田 望	TOPPAN-CERT	凸版印刷株式会社
大内 和博	YIRD	ヤフー株式会社
山賀 正人	専門委員	

改版履歴

- 2015.11.16 Ver.1.0 初版作成
- 2017.3.13 Ver1.5 改訂