一般社団法人
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 人材の育成

Ver 1.0

CSIRT 人材 WG

2022 年 3 月 31 日

目次

図表

1章 はじめに

1.1 本資料について

CSIRT の設立については一般化しつつあるが、その一方、慢性的に要員が不足している、要員を CSIRT の特定業務へ配属したがどのように育成すればよいのかわからない、という声も多く聞く。

本資料では、「CSIRT 人材の定義と確保 Ver.2.1[1]」により定義された CSIRT に必要な役割とスキルをベースとして、その役割毎にどのように育成していくのかという解決策、また要員不足に対しては兼任できる役割をグループ化して育成するという解決策を WG メンバーのベストプラクティスとして集約し作成した。育成方法について悩まれている組織の CSIRT 活動の参考になれば幸いである。

1.2 本資料の使い方について

本資料はベストプラクティスである。CSIRT に求められるものは、その役務や組織の規模によって異なることから、グループ分けなど、必ずしも本資料に準拠しなければならないということではない。

特にインシデントの終息・再発防止まですべてを行う CSIRT とインシデントレスポンスサービスを提供する CSIRT ではグループの分け方が異なる場合もあるが、それぞれの組織に合わせて柔軟に考えて欲しい。

1.3 本資料で記載する役割

本資料では CSIRT 要員を下記の役割にわけ、それぞれの育成手段について記載する。

- 連絡/全体統括
- インシデント対応
- 監視/調査/解析（SOC/監視）
- 監視/調査/解析（脆弱性管理/診断業務）
- 監視/調査/解析（フォレンジック）
- セキュリティマネジメント
- 開発/開発支援

[1] https://www.nca.gr.jp/activity/imgs/recruit-hr20201211.pdf

1.4 育成の STEP の定義

本資料では、育成の各 STEP を下記のとおり定義する。役割毎の詳細は、それぞれの章を参照すること。STEP4 以降は、本資料では記載しない。

表 1-1 育成の STEP の定義

STEP	対象者	説明	目標
0	新規配属者	CSIRT もしくはセキュリティ部門に配属された要員が、これから自社のセキュリティに関する業務を行うために必要な基礎知識を身につけるための教育を受ける。この STEP を終了すると基礎教育修了者となる。	基礎教育修了者
1	基礎教育修了者	基礎教育を終えて担当役割に配属されたばかりの担当者が、その役割内容を学び、組織における自分の役割、立ち位置を理解する導入教育期間に相当する。この STEP を修了すると担当役割の初心者レベルに到達する。	担当役割の初心者
2	担当役割の初心者	担当役割の初心者が、自分の担当役割のより深い知識を身に着け、OJT を通じて経験を積む。この STEP を修了すると、上位職が支援すれば業務をこなせる担当役割の見習いレベルに到達する。	担当役割の見習い
3	担当役割の見習い	実践、訓練を通じて、知識経験を慣熟させる。この STEP を修了すると、担当役割の通常業務に関しては独り立ちできる一人前になる。	担当役割の一人前
4	担当役割の一人前(トレーナー)	どの役割グループの業務でも通常起きている事象以外の想定外の事象が起きることがある。この想定外の事象に対応できるスキルは教育で学べるものではなく、STEP 3 の経験を積み上げて得られるものである。万人が必ず習得できるレベルではないため、本資料からは除外する。	担当役割の熟練技術者、または業務マネジメント
5	熟練技術者/マネジメント	－	－

2章 役割グループ

本資料で記載する役割と、CSIRT 人材の定義と確保 Ver.2.1 の「CSIRT の兼任可能な役割」で記載されている兼任グループとの対応を以下に示す。

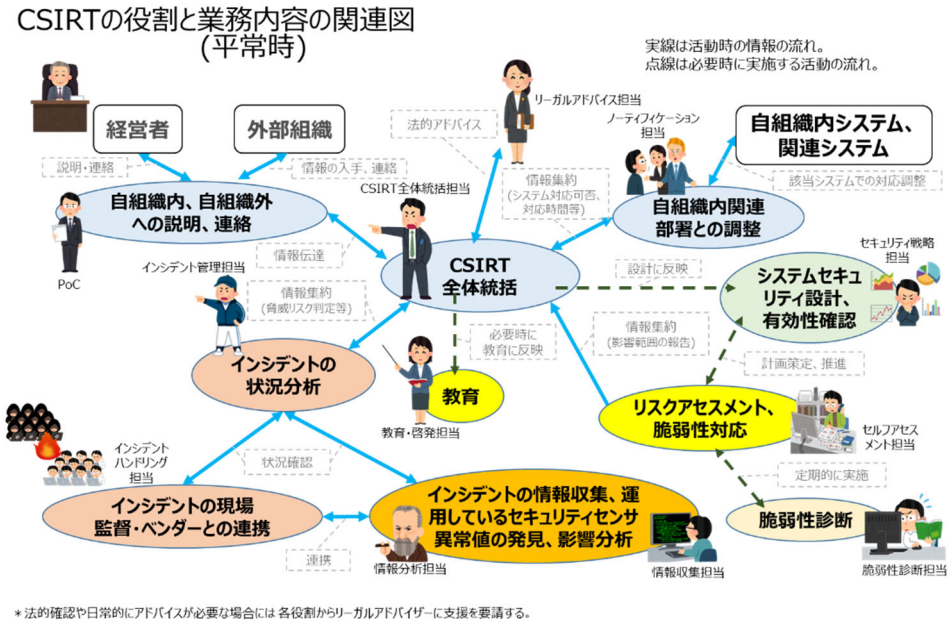


図 2-1 CSIRT 人材の定義と確保との対応（平常時）

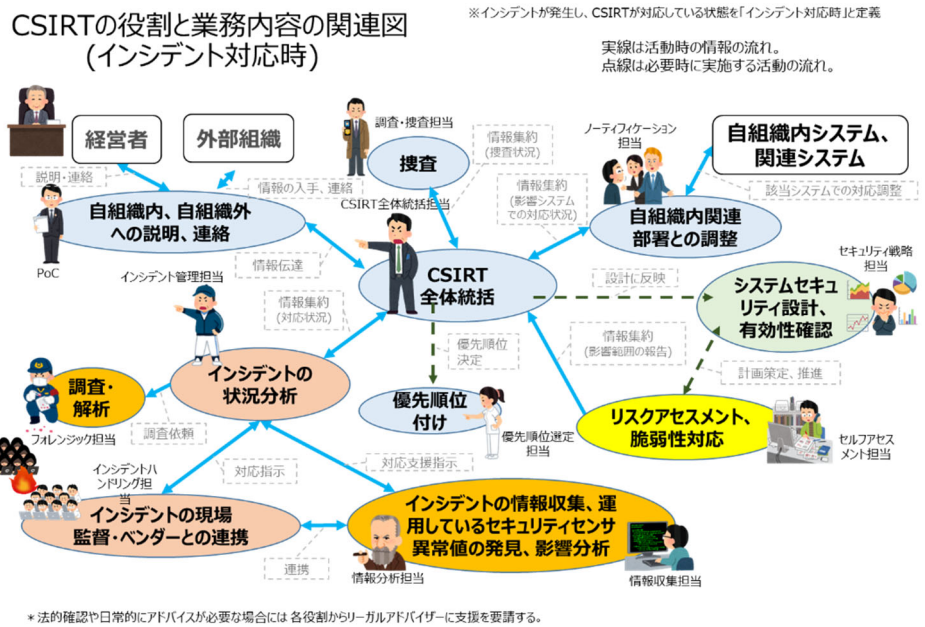


図 2-2 CSIRT 人材の定義と確保との対応（インシデント対応時）

表 2-1 CSIRT 人材の定義と確保との対応表

機能分類	役割名称	兼任グループ「本資料での役割」
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」** （業務内容の詳細は、「4.1.1 役割の説明」参照）
	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	
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」** （業務内容の詳細は、「4.1.1 役割の説明」参照）
	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 2「インシデント対応」** （業務内容の詳細は、「4.2.1 役割の説明」参照）
	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」** （業務内容の詳細は、「4.1.1 役割の説明」参照）
	トリアージ担当：優先順位選定担当	
	フォレンジック担当	**兼任グループ 5「フォレンジック」** （業務内容の詳細は、「4.5.1 役割の説明」参照）
情報収集・分析	リサーチャー：情報収集担当	**兼任グループ 3「情報収集/情報分析（SOC/監視）」** （業務内容の詳細は、「4.3.1 役割の説明」参照）
	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 4「脆弱性管理/診断」** （業務内容の詳細は、「4.4.1 役割の説明」参照）
	セルフアセスメント担当	**兼任グループ 6「セキュリティマネジメント」** （業務内容の詳細は、「4.6.1 役割の説明」参照）
	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 7「開発/開発支援」** （業務内容の詳細は、「4.7.1 役割の説明」参照）

自組織内教育	教育担当：教育・啓発担当	**兼任グループ 6「セキュリティマネジメント」** （業務内容の詳細は、「4.6.1 役割の説明」参照）
経営者	CISO、CSO、社長など	-
組織運営	CSIRT 運営管理担当	-
システム運用	システム運用担当	-

CSIRT 要員としてそれぞれの役割を担うにあたり、それぞれの役割で必要となるスキルが存在する。しかし、それぞれの役割に対して個別に教育体系を作り、要員を育成するというのは現実的に難しい場合が多い。本資料では類似のスキルを必要とする役割をグループ化し、そのグループ毎の育成手段を記載することによってより現実的な要員の育成手段としている。なお、関連する役割としての経営者、組織運営、システム運用に関しては本資料の対象とはしていない。

本資料では、4 章からこれらのグループに必要なスキルを身につけるための育成手段を記載しているが、その前に各グループ共通で必要となる教育項目を基礎教育として 3 章に記載している。本資料では、CSIRT やセキュリティ部門に配属された場合、まずセキュリティの基礎として 3 章の基礎教育を学び、担当する CSIRT の役割に応じて、それぞれの役割グループの共通教育を受け、ステップアップしていくことを想定している。

3章 基礎教育

基礎教育は、CSIRT もしくはセキュリティ部門に配属された要員が、これから自社のセキュリティに関する業務を行うために必要な基礎知識を身につけるための教育である。自社のポリシー、セキュリティガイドラインの理解に始まり、セキュリティ事象の理解、自社のセキュリティ防御機器、CSIRT 体制、関連法令の理解など、以下のような項目を理解させる教育を実施する。

- 自社のセキュリティポリシー、セキュリティガイドライン、セキュリティマネジメントシステムの理解
- 一般的なセキュリティ事象、攻撃手法などの概要の理解
- 自社システムを構成するネットワーク、サーバーなどの概要の理解
- 自社に関するセキュリティ的な防御機構、防御機能、適用されるポリシーやルールの理解
  - 物理セキュリティ対策の実施内容
  - ゾーニング、通信の安全性を含めたネットワークセキュリティ対策の実施内容、ネットワークのセキュリティポリシー
  - 認証・アクセス制御
  - 侵入検知・侵入防御・侵入後対応の仕組み
  - バックアップ
  - 内部不正対策の実施内容、内部不正への対応
  - 本番環境・開発環境・OA 環境の分離などのルール
  - 在宅業務・クラウド利用・モバイルデバイス利用などのルール
- セキュリティ確保のためのシステム構築、運用維持に関する理解
  - システムやソフトウェアの設計
  - システムやソフトウェアの設定
  - バージョンアップ
  - パッチ適用
  - ライフサイクル管理
- CSIRT の役割と守備範囲、サービス提供内容、SLA などの社としての CSIRT の理解
- 関連法令に関する理解
  - 電気通信事業法（通信の秘密に関する法律）
  - 不正指令電磁的記録に関する罪（ウイルス作成罪）や電子計算機使用詐欺罪に関する刑法
  - 不正アクセス行為の禁止等に関する法律

- 営業秘密、限定提供データに関する不正競争防止法
- データの権利やリバースエンジニアリングに関する著作権法
- 差し押さえや捜査関係事項紹介のための刑事訴訟法
- その他業界特有の遵守すべき法令・ガイドライン
- 契約不履行、損害賠償請求に関する民法、善管注意義務に関する会社法、個人情報保護法、マイナンバー法に関しては、特に CSIRT 業務に限らずとも理解しておくべき法令のため、全社教育で実施されているものとする

4章 役割別教育

4.1 連絡・全体統括

4.1.1. 役割の説明

連絡・全体統括業務の内容を以下に示す。

- 連絡窓口となり、話し相手に合わせるコミュニケーションスキルを用いて報告・説明を関係者、経営者に行う。
- 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対応を指示する。
- 内部犯罪やクレジットカード詐欺、不正売買などの案件については必要に応じて社内外関係部署とともに活動する。

4.1.2. 役割の全体的な位置づけ

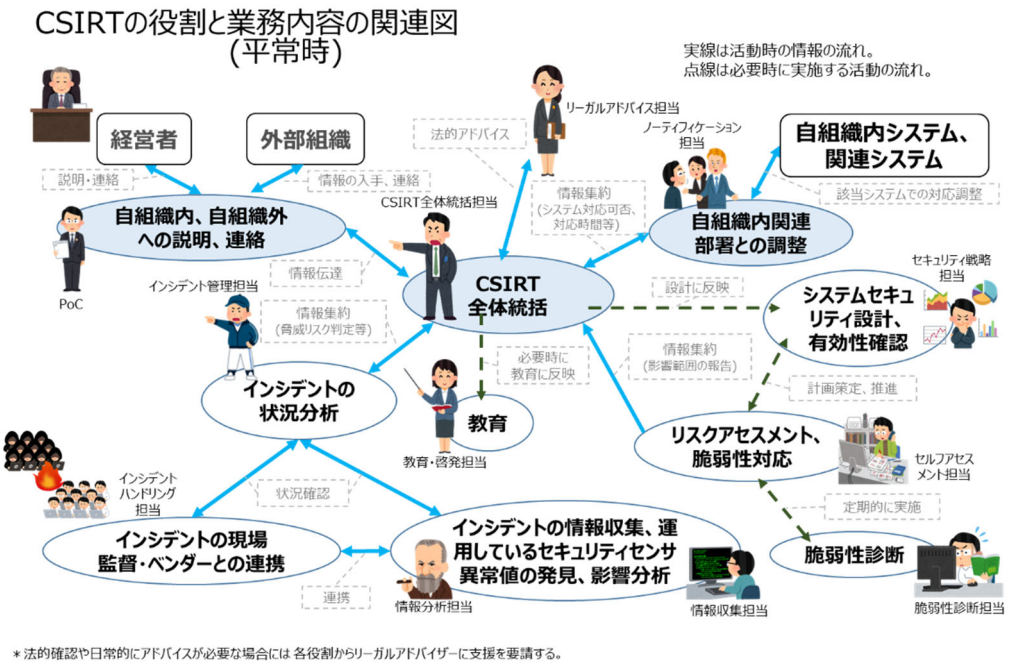


図 4-1 連絡・全体統括の全体的な位置づけ（平常時）

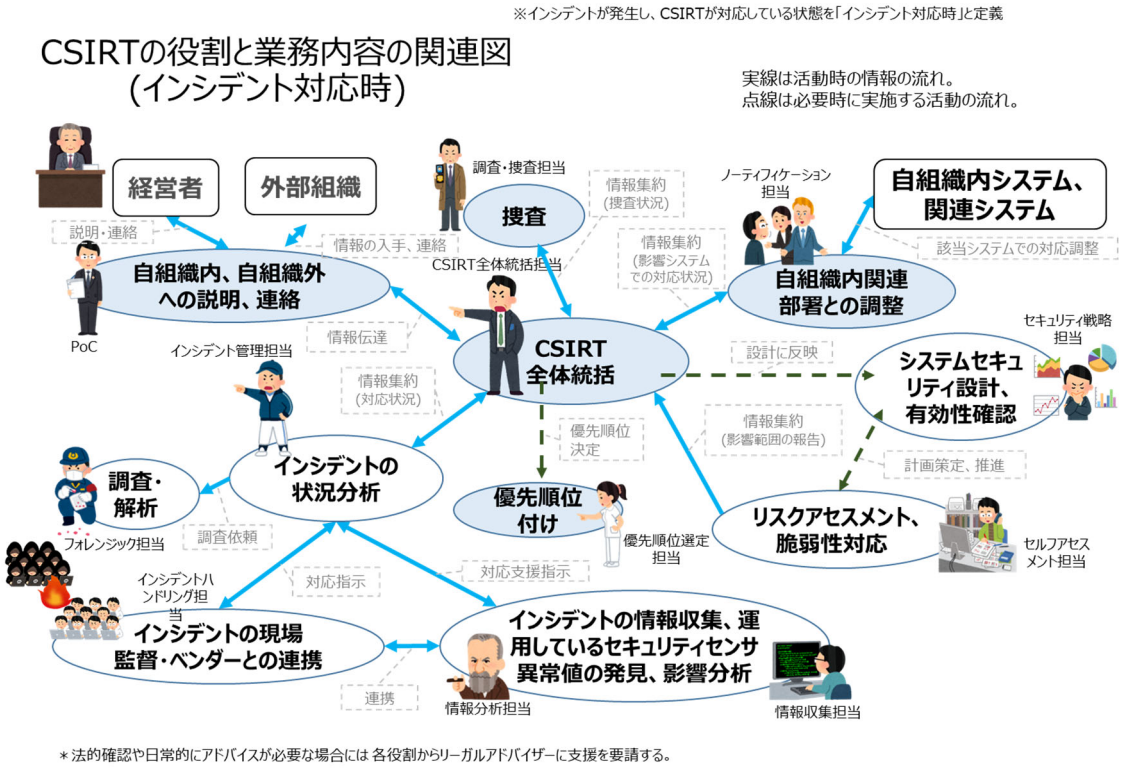


図 4-2 連絡・全体統括の全体的な位置づけ（インシデント対応時）

4.1.3. 育成 STEP の説明

表 4-1 育成 STEP の説明（連絡・全体統括）

STEP	対象者	説明
1	基礎教育修了者	基礎教育を終え、役割別の共通教育も終えた連絡・全体統括の新規配属者が、さらに学習や経験を通じて PoC、全体統括の役割、業務内容を把握する
2	担当役割の初心者	より深い知識を身につけ、OJT を通じて経験を積む。上位職が支援しての報告や調整、インシデント対応戦略の策定などの業務をこなせるようになることをめざす
3	担当役割の見習い	実践、訓練を通じて、知識、経験を慣熟する。一般的な業務に関しては独り立ちし、関係各所への報告や自組織内の調整ができるようになる。普通のインシデントであれば、発生時に一人で対応に向けての戦略の策定やインシデント対応担当への指示ができるようになる

4.1.4. 共通教育

役割別の共通教育として、連絡・全体統括業務に必要な基礎知識、技術を以下に示す。

- コミュニケーション手法
  - IT やセキュリティ知識に乏しい人々に正しく伝える技術
- 対人能力（各部門との調整が必要となるため）
- 論理的思考（インシデントに対しては仮説検証にて戦略を立てる必要があり、論理的推論が必要）
- 限られた時間で対応するための優先順位決定とリスク算定手法

4.1.5. STEP1：基礎教育修了者から担当役割の初心者にいたるまでの育成

連絡・全体統括業務へ新規配属された基礎教育修了者への教育内容を以下に示す。

4.1.5.1. 目標・目的

- 自分の役割と CSIRT それぞれの役割を理解する
- 関係者との連絡がスムーズにできるようになる

4.1.5.2. 学習項目/経験させる業務

- CSIRT で発生している平常時の状況をレポートし、定期的に関係者へ報告する
- 平時の学習として連絡・窓口担当として全体感をつかむために、自社のルールに基づいてインシデント対応フローを理解し、関係者に全体フローを説明する
- インシデントが発生した場合には、事象発生・対応状況、業務影響、被害・復旧状況をそれぞれ時系列で記載した報告書を作成する。さらに、（実施している場合は）暫定処置の状況、関係者への連絡状況、原因究明状況も記載してまとめ、関係者へ説明する
- 外部関係者との接点を構築し、積極的にワーキンググループなどへ参加する

4.1.5.3. 参考となる外部講習、外部のドキュメント

- 特になし

4.1.5.4. 達成目安

- 平常時には毎月の報告を 1 年間実施する
- インシデント対応報告をあらかじめ決められた回数こなす（例えば、過去に対応実績があるようなインシデント対応を 3 回実施する）
- 外部関係者との会合に年 4 回以上参加する

4.1.6. STEP2：担当役割の初心者から担当役割の見習いにいたるまでの育成

連絡・全体統括業務の初心者への教育内容を以下に示す。

4.1.6.1. 目標・目的

- STEP1 の報告を深化させる。インシデント発生時には全体像を絵で表現し、どのシステム、業務がどのような順番・経路で侵害され、どのような影響が発生しているのか、どのような調査を行っているのかを一覧で記載できるようになる
- インシデントへの対応戦略が立てられるようになる

4.1.6.2. 学習項目/経験させる業務

- 対象となるシステム・業務・ネットワーク構成を理解し、事象を絵で表現する訓練を行う
- 平常時に SOC から上がってくるアラートの状況を指導者とともに分析し、対応要否判断、トリアージスキルを習得する
- インシデント発生時には指導者とともに対応戦略を策定し、インシデントマネージャーへの指示を補佐する

4.1.6.3. 参考となる外部講習、外部のドキュメント

- 特になし

4.1.6.4. 達成目安

- 対象となるシステム・業務・ネットワーク構成のおおよその理解

- 平常時の対応要否判断、トリアージを指導者とともに 3 回行う
- インシデント発生には事象を絵で表現し、指導者にレビューを受けながら、戦略の策定やインシデントマネージャーへの指示を 3 回行う

4.1.7. STEP3：担当役割の見習いから担当役割の一人前にいたるまでの育成

連絡・全体統括業務の見習いへの教育内容を以下に示す。

4.1.7.1. 目標・目的

- 通常のインシデントに対して、戦略や指示が的確にできる
- 外部関係者と連携して情報の活用ができる

4.1.7.2. 学習項目/経験させる業務

以下のようなケースを通じ、全体統括・連絡担当として CSIRT 全体が機能するように活動できるよう訓練する。

- 脆弱性情報の入手と対応（対応要否判断、対応を行う場合、対応できずに他の方法でリスク低減を図る場合）
- サービス妨害攻撃（Denial of Service Attack、DoS 攻撃）の検知と対応（対応方針の確認と対応）
- 外部からのインジェクション攻撃の検知と対応（失敗ケースと成功ケースそれぞれでのシステム側との対応含む）
- 不審メールの受信報告と開いた場合の対応（受信のみの報告の場合と開いてしまったという報告を受けた場合）
- 自社のなりすましメールが他社へ着信した場合の対応（他社への対応、なりすまされた自社社員他への対応）
- ランサムウェアなどのデータ破壊マルウェアへの対応（特定の端末で収まっている場合、ファイルサーバーまで侵害された場合）
- 不審な Ｃ２サーバー（遠隔操作に関すると思われるサイトなど）との通信の検知と対応。侵入フェーズ（初期侵入で検知、ダウンローダーで検知、内部に不正に導入されたリモートアクセスツールの動作を検知、外部へのデータ持ち出し時で検知）毎に実施
- Web ページ改ざん対応（表示の改ざん、マルウェアを埋め込まれたことによる改ざ

ん、埋め込んだ外部サービスに起因する改ざん）

4.1.7.3. 参考となる外部講習、外部のドキュメント

- 特になし

4.1.7.4. 達成目安

- 上記訓練ケースを一人で的確に対応できる
- 一度経験した類似ケースは一人で対応できる
- 未経験のケースは指導者の補佐をすることができる

4.2 インシデント対応

4.2.1. 役割の説明

インシデント対応業務の内容を以下に示す。

- 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システム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受け、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対応要否やリスク判断を SOC とともに行い、関係者に連絡、調整、対応依頼をする

4.2.2. 役割の全体的な位置づけ

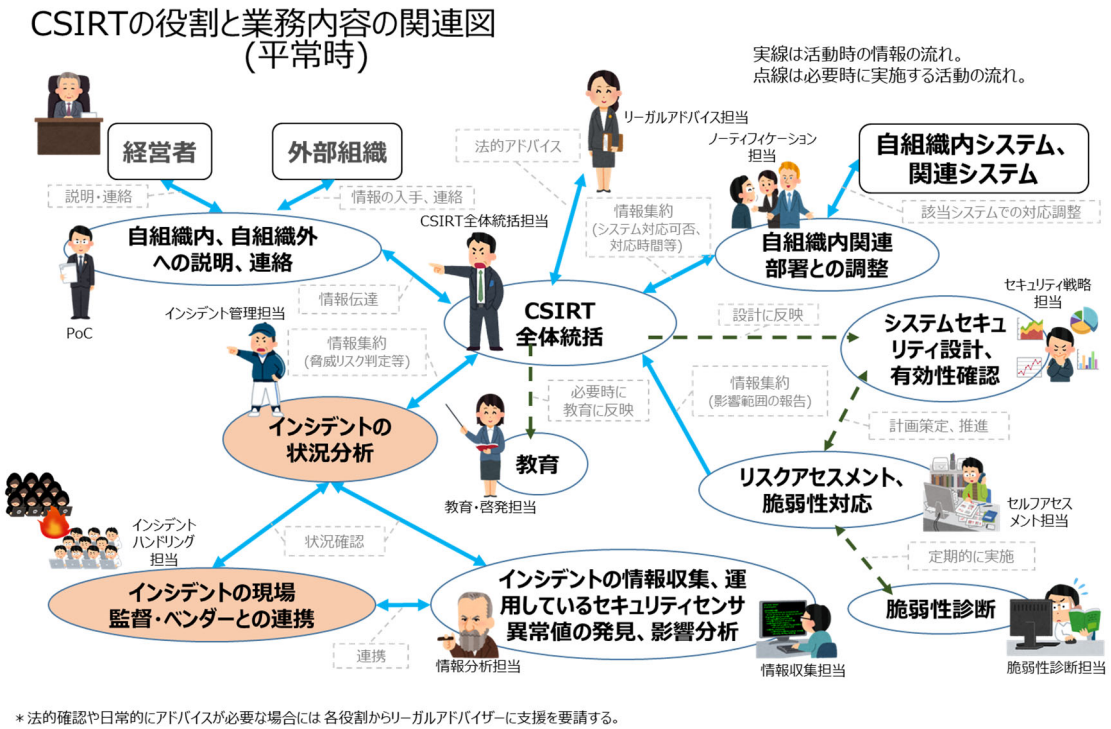


図 4-3 インシデント対応の全体的な位置づけ（平常時）

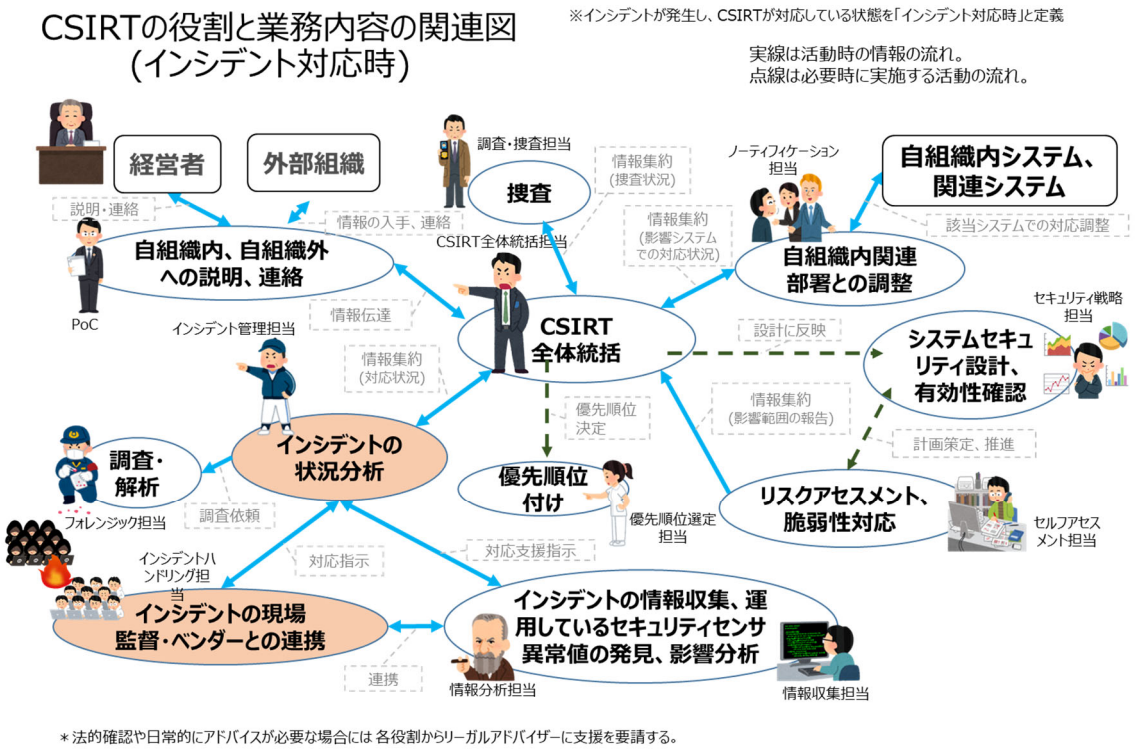


図 4-4 インシデント対応の全体的な位置づけ（インシデント対応時）

4.2.3. 育成 STEP の説明

表 4-2 育成 STEP の説明（インシデント対応）

STEP	対象者	説明
1	基礎教育修了者	基礎教育を終え、役割別の共通教育も終えたインシデント対応の新規配属者が、さらに学習や経験を通じてインシデント対応の役割、業務内容を把握する。共通教育で行った、一般的なセキュリティ事象、攻撃手法などの詳細の理解、自社システムに関するネットワーク構成、サーバー構成などの構成の深い知識、自社の構成に関するセキュリティ的な防御機器、役割を具体的な作業をイメージして深く理解する。
2	担当役割の初心者	データの流れを整理することにより、より深い知識を身に着け、インシデント対応の OJT を通じて経験を積む。上位職が支援すればインシデント対応戦略に基づいた対応タスクの作成や対応ができるようになる。
3	担当役割の見習い	実践、訓練を通じて、知識、経験を慣熟させる。一般的な業務に関しては独り立ちし、戦略の策定に基づいたタスクの作成やインシデント対応を該当部門と協力してできるようになる。

4.2.4. 共通教育

役割別の共通教育として、インシデント対応業務に必要な基礎知識、技術を以下に示す。

- コミュニケーション手法
  - ネットワーク監視部門、SOC、自社の関連システム部門との関係を良好にしておくための手法（正確な指示、報告のためのメール作成力や文書作成力、報告聞き取り力）
- インシデントマネージャーとしての作業タスクの整理作成、管理手法
- ネットワーク、サーバー、セキュリティ機器のアラートなどを読み取るための基本的な IT 知識
- 限られた時間で対応するための優先順位決定とリスク算定手法

4.2.5. STEP1：基礎教育修了者から担当役割の初心者にいたるまでの育成

インシデント対応業務へ新規配属された基礎教育修了者への教育内容を以下に示す。

4.2.5.1. 目標・目的

- 自分の役割と CSIRT 内ですべきこと、他の役割との関係が理解できる
- 自組織のシステム構成やネットワークのセキュリティポリシーが理解できる

4.2.5.2. 学習項目/経験させる業務

- 自社ネットワークのイントラネット内、インターネット出入り口側の構成を理解し、それぞれのファイアウォールポリシーやフィルタリングポリシー、サーバー設計ポリシー、端末設計ポリシーを理解する
- 自社システムの概要と保持データを理解する。特に機密と思われるデータのありかを把握する
- インシデント発生時に協力していただく自社システム保守員との連絡手段やそれぞれが実施する役割を対応フェーズ（安全確保・封じ込め・暫定処置・原因調査・復旧・再発防止）毎に明確にする
- NOC や SOC、システム運用担当者と協力して出力されるログの見方を学習する

- 情報活用（インテリジェンス）とは何かを学び、自組織の CSIRT への活用プロセスを理解する

4.2.5.3. 参考となる外部講習、外部のドキュメント

- 特になし

4.2.5.4. 達成目安

- 平常時のログの分析を 1 年間行う
- 自社システム、ポリシーの理解。機密データのありかの理解
- OSINT（Open Source Intelligence）を題材としたインテリジェンスの理解と活用プロセスの理解

4.2.6. STEP2：担当役割の初心者から担当役割の見習いにいたるまでの育成

インシデント対応業務の初心者への教育内容を以下に示す。

4.2.6.1. 目標・目的

- STEP1 の理解を深化させる。インシデント発生時には全体像を絵で表現し、どのシステム、業務がどのような順番・経路で侵害されているのかをデータの流れとともに一覧で記載できるようになる
- インシデント発生時に関連する部署との関係を築き、的確な指示や対応ができるようになる

4.2.6.2. 学習項目/経験させる業務

- 対象となるシステム・業務・ネットワーク構成図を理解し、事象を絵で表現する訓練を行う
- SOC からのアラート対応や脆弱性対応のような平常時の活動を通して関連部署との関係を築く
- インシデント発生時には指導者の元で全体統括者から示される対応戦略や指示をタスク化し、対応者への指示や実績管理を行う。また、対応者としてはタスク化され

た内容について調査・対応を行う
- フォレンジック担当と連携して証拠保全を行い、また、フォレンジック調査を通じて原因究明への手がかりを得る。その内容を進行中の調査へフィードバックする

4.2.6.3. 参考となる外部講習、外部のドキュメント

- 特になし

4.2.6.4. 達成目安

- 対象となるシステム・業務・ネットワークへのデータの流れのおおよその理解
- 平常時のアラート対応、脆弱性対応を指導者とともに 3 回行う
- インシデント発生には事象を絵で表現し、指導者にレビューを受けながら、対応戦略に基づいたタスクの策定や関係部署への指示を 3 回行う

4.2.7. STEP3：担当役割の見習いから担当役割の一人前にいたるまでの育成

インシデント対応業務の見習いへの教育内容を以下に示す。

4.2.7.1. 目標・目的

- 通常のインシデントに対して、指示や対応が的確にできる
- インテリジェンスを活用して調査を効率的に行うことができる

4.2.7.2. 学習項目/経験させる業務

以下のようなケースを通じ、インシデント対応者として活動できるように訓練する。
- 脆弱性情報の入手と対応（対応要否判断、対応を行う場合、対応できずに他の方法でリスク低減を図る場合）
- サービス妨害攻撃（Denial of Service Attack、DoS 攻撃）の検知と対応（対応方針の確認と対応）
- 外部からのインジェクション攻撃の検知と対応（失敗ケースと成功ケースそれぞれでのシステム側との対応含む）
- 不審メールの受信報告と開いた場合の対応（受信のみの報告の場合と開いてしまっ

たという報告を受けた場合）
- 自社のなりすましメールが他社へ着信した場合の対応（他社への対応、なりすまされた自社社員他への対応）
- ランサムウェアなどのデータ破壊マルウェアへの対応（特定の端末で収まっている場合、ファイルサーバーまで侵害された場合）
- 不審な C2 サーバー（遠隔操作に関すると思われるサイトなど）との通信の検知と対応。侵入フェーズ（初期侵入で検知、ダウンローダーで検知、内部に不正に導入されたリモートアクセスツールの動作を検知、外部へのデータ持ち出し時で検知）毎に実施
- Web ページ改ざん対応（表示の改ざん、マルウェアを埋め込まれたことによる改ざん、埋め込んだ外部サービスに起因する改ざん）

4.2.7.3. 参考となる外部講習、外部のドキュメント

- 特になし

4.2.7.4. 達成目安

- 上記訓練ケースを一人で的確に対応できる
- 一度経験した類似ケースは一人で対応できる
- 未経験のケースは指導者の補佐をすることができる

4.3 情報収集/情報分析（SOC/監視）

4.3.1. 役割の説明

情報収集/情報分析（SOC/監視）業務の内容を以下に示す。

- SOC/監視システムと業務の設計/構築/導入/運用/維持（注：設計/構築/導入は熟練技術者レベル以上の業務である）
- セキュリティ機器から通知されたアラートを分析して、検知/誤検知を判定する
- 検知したアラートから監視対象システムへの影響の有無を推測する
- 監視対象システムへ影響するおそれのあるアラートの情報をまとめて、インシデント対応部門へ連絡する
- インシデント対応部門からの調査依頼に対応して、セキュリティ機器の情報を調査、分析する
- 定期的にアラートを統計的に分析して、定期レポートを作成する
- メーカー提供の新しい検知ルール、定期レポートの結果、独自に収集した攻撃情報、インシデント対応部門のフィードバックなどを使って、セキュリティ機器の検知精度を維持、向上する
- 定期的に作業記録を振り返って、業務の維持、改善を行う

脅威ハンティング（スレットハンティング）ができる人材の育成は、情報収集/情報分析（SOC/監視）業務の人材育成プログラムには含まれない。脅威ハンティング（スレットハンティング）ができる人材は、一人前（STEP 4 ）、熟練技術者（STEP 5 ）のレベルとなるため、本プログラムの対象外とする。

4.3.2. 役割の全体的な位置づけ

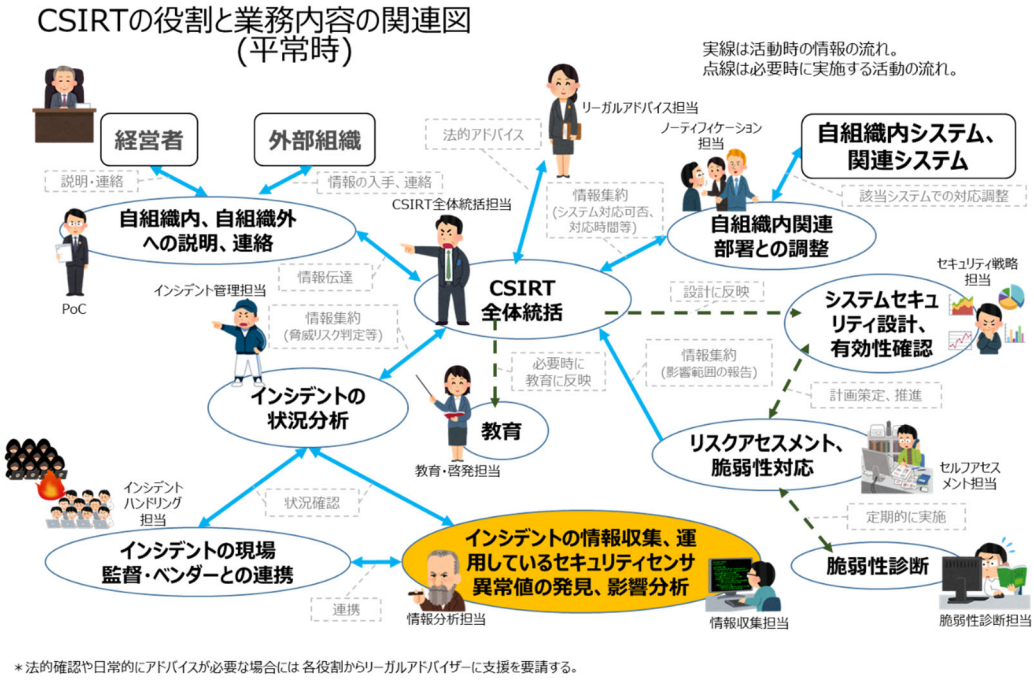


図 4-5 情報収集/情報分析（SOC/監視）の全体的な位置づけ（平常時）

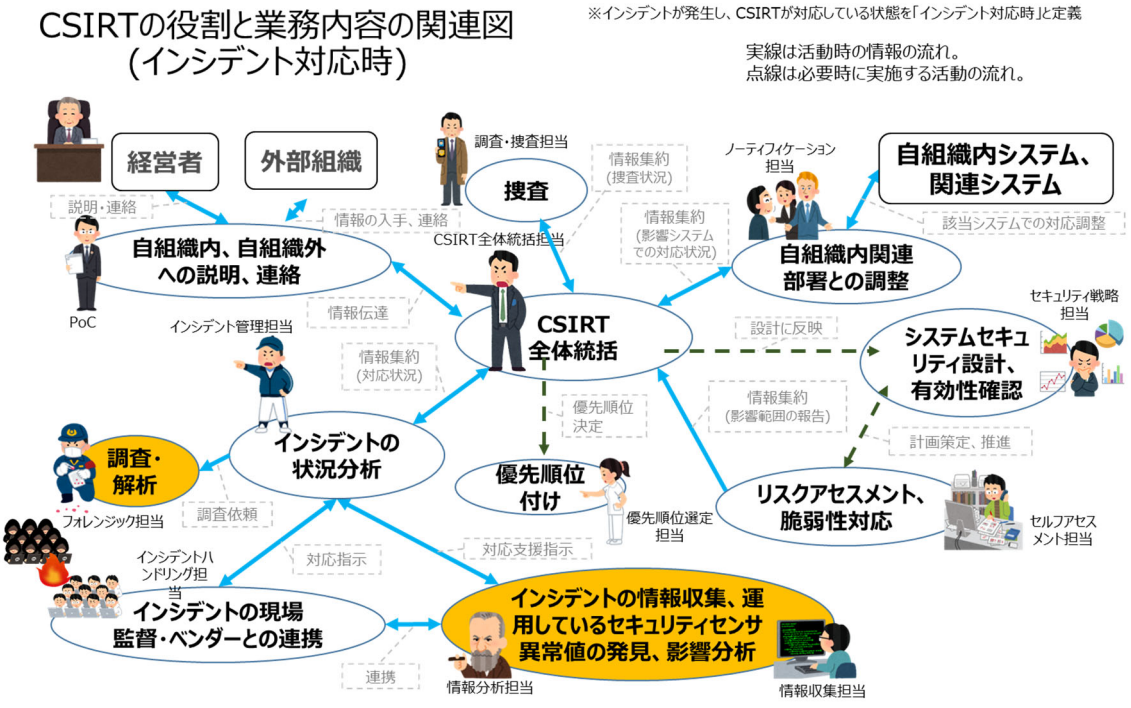


図 4-6 情報収集/情報分析（SOC/監視）の全体的な位置づけ（インシデント対応時）

4.3.3. 育成 STEP の説明

表 4-3 育成 STEP の説明（情報収集/情報分析（SOC/監視））

STEP	対象者	説明
1	基礎教育修了者	基礎教育を終え、役割別の共通教育も終えた情報収集/情報分析（SOC/監視）業務の新規配属者が、初心者をめざす。導入教育を受けて、監視業務の手順や監視機器の操作方法を学習する
2	担当役割の初心者	導入教育を完了した初心者が、見習いをめざす。一人前の情報収集/情報分析（SOC/監視）担当者から指導を受けながら、学習した監視業務の手順や監視機器の操作方法を実際の業務で実践する。通常の情報収集/情報分析（SOC/監視）業務の一部を一人で処理できるようになることをめざす
3	担当役割の見習い	通常の監視業務の一部を一人で処理できる見習いが、通常のすべての情報収集/情報分析（SOC/監視）業務を一人で処理できる一人前をめざす。一人前の監視担当者と一緒に業務を行い、経験を積む

4.3.4. 共通教育

役割別の共通教育として、情報収集/情報分析（SOC/監視）業務に必要な基礎知識、技術を以下に示す。

- 一般的なセキュリティ事象、攻撃手法などの詳細理解
  - サイバー攻撃手法
- 自社システムを構成するネットワーク、サーバーなどの理解
  - 自社システムの概要の理解
  - 自社ネットワークの理解
  - 自社システムを構成するサーバーの理解
- 自社に関するセキュリティ的な防御機構、防御機能などの理解
  - インシデントや脆弱性のセキュリティ対応技術

4.3.5. STEP1：基礎教育修了者から担当役割の初心者にいたるまでの育成

情報収集/情報分析（SOC/監視）業務へ新規配属された基礎教育修了者への教育内容を以下に示す。

4.3.5.1. 目標・目的

- 情報収集/情報分析（SOC/監視）業務を理解する
- 情報収集/情報分析（SOC/監視）業務を実行するための知識と技術を習得する
- 情報収集/情報分析（SOC/監視）業務の手順を把握する

4.3.5.2. 学習項目/経験させる業務

- 情報収集/情報分析（SOC/監視）業務の概要の把握
- 情報収集/情報分析（SOC/監視）の対象システム/サービスの把握
- 情報収集/情報分析（SOC/監視）業務に使用しているセキュリティ機器、監視機器の理解
- 情報収集/情報分析（SOC/監視）業務の手順、操作の学習

4.3.5.3. 参考となる外部講習、外部のドキュメント

- IDS/IPS/SIEM などの不正侵入検知システムの入門書

4.3.5.4. 達成目安

- 情報収集/情報分析（SOC/監視）業務の導入教育で指示された資料、書籍の読了
- 情報収集/情報分析（SOC/業務）の概要、使用する監視対象システム/サービスの概要を説明できる

4.3.6. STEP2：担当役割の初心者から担当役割の見習いにいたるまでの育成

情報収集/情報分析（SOC/監視）業務の初心者への教育内容を以下に示す。

4.3.6.1. 目標・目的

- 情報収集/情報分析（SOC/監視）業務の一部を独力で実施できる
  - セキュリティ機器から通知されるアラートのうち、日常的に発生するアラートを分析して、検知/誤検知を判定できる
  - 日常的に発生するアラートについて、セキュリティ機器のログを検索してサイバ

ー攻撃の痕跡を抽出できる

- 情報収集/情報分析（SOC/監視）担当者の業務をサポートできる
- 指導者の指示にしたがって、すべての定常の情報収集/情報分析（SOC/監視）業務を実施できる

4.3.6.2. 学習項目/経験させる業務

- 情報収集/情報分析（SOC/監視）業務の手順、操作の習熟
- 指導者の指示にしたがって、日常的に発生するアラートを分析
- 情報収集/情報分析（SOC/監視）業務に使用しているセキュリティ機器、監視機器の操作方法の習得
- セキュリティ機器のアラート/ログの分析手法の学習

4.3.6.3. 参考となる外部講習、外部のドキュメント

- ベンダー研修、トレーニングの受講
- ログ分析トレーニング（JPCERT/CC）[2]
- 有償のログ解析セミナーや研修の受講

4.3.6.4. 達成目安

- 日常的に発生するアラートの検知アルゴリズムの理解
- 指導者とペアで情報収集/情報分析（SOC/監視）業務を規定回数実施する
- 情報収集/情報分析（SOC/監視）業務の一部を独力で規定回数実施する
- 日常的に発生するアラートを分析して、検知/誤検知判定の正答率が規定値を満たすこと（分析回数が規定回数を満たし、かつ正答率が規定割合以上であること）

4.3.7. STEP3：担当役割の見習いから担当役割の一人前にいたるまでの育成

情報収集/情報分析（SOC/監視）業務の見習いへの教育内容を以下に示す。

[2] https://blogs.jpcert.or.jp/ja/2020/07/log_analysis_training.html

4.3.7.1. 目標・目的

- 定型の情報収集/情報分析（SOC/監視）業務を独力で実施できる
  - 自社のセキュリティ機器、監視機器の機能や操作をマスターする
  - セキュリティ機器から通知されるほとんどのアラートを分析して、検知/誤検知を判定できる
  - 検知したアラートから監視対象システムへの影響の有無を推測できる
  - 監視対象システムへ影響するおそれのあるアラートの情報をまとめて、インシデント対応部門へ連絡できる
- 検知解析能力を維持、向上できる
  - セキュリティ機器のルールをチューニングして、誤検知を削減できる
  - メーカー提供の新しい検知ルールの評価、追加判断ができる
  - 自身の検知解析能力を維持、向上できる
- 後進(新規配属者や初心者、見習い)の育成ができる

4.3.7.2. 学習項目/経験させる業務

- 自社のセキュリティ機器、監視機器の新しい機能やその操作を常に把握する
- セキュリティ機器から通知される発生頻度の低いアラートを分析して、検知/誤検知を判定する。手順化して情報収集/情報分析（SOC/監視）担当者へレクチャする
  - 検知したアラートから監視対象システム/サービス監視対象システム/サービスを構成するソフトウェアの基本的な動作原理を理解する
  - 監視対象システム/サービスのインベントリ情報や業務の情報を収集して把握する
  - サイバー攻撃によって監視対象システム/サービスで発生する異常動作/影響を検討する
- インシデント対応部門との連携業務
  - インシデント対応部門へ引継ぐ情報、報告書の作成方法を理解する、インシデント対応業務を理解する
  - インシデント対応部門からの調査依頼に対応して、セキュリティ機器の情報を調査、分析する
- 定期的にアラートを統計分析して、定期レポートを作成する
- 定期的に作業記録や定期レポートを振り返って、業務の維持、改善を行う
- セキュリティ機器の検知精度を維持、向上する
  - セキュリティ監視機器のチューニング技術を習得する
  - メーカー提供のセキュリティ監視機器の新しい検知ルールを分析して導入可否

を検討する
- インシデント対応部門のフィードバックなどを使って、検知ルールの改善を検討する
- 新しいサイバー攻撃の情報を収集して、検知方法を検討する

4.3.7.3. 参考となる外部講習、外部のドキュメント

- ログ分析トレーニング（JPCERT/CC）[3]
- ログを活用した Active Directory に対する攻撃の検知と対策（JPCERT/CC）[4]
- 高度サイバー攻撃への対処におけるログの活用と分析方法（JPCERT/CC）[5]

4.3.7.4. 達成目安

- 定型の情報収集/情報分析（SOC/監視）業務を独力で実施できる
- 情報収集/情報分析（SOC/監視）業務を規定した期間以上経験する
- インシデント対応部門と相互連携できる
- アラートを統計分析して、定期レポートを作成できる
- セキュリティ機器へメーカー提供の新しい検知ルールを導入してチューニングできる
- 定期的に業務を振り返って、業務の維持、改善を検討できる

[3] https://blogs.jpcert.or.jp/ja/2020/07/log_analysis_training.html

[4] https://www.jpcert.or.jp/research/AD.html

[5] https://www.jpcert.or.jp/research/apt-loganalysis.html

4.4 脆弱性管理/診断

4.4.1. 役割の説明

脆弱性管理/診断業務の内容を以下に示す。脆弱性管理とは、バージョン管理、脆弱性/パッチ情報の収集と周知、適用を行うことと定義する。脆弱性管理/診断業務の担当者は、脆弱性管理業務と脆弱性診断業務のいずれか、または両方の業務を行う。

- 社内の各種システム/ソフトウェア(開発製造時、運用時)の脆弱性管理ルールの作成と施行
  - 社内の各種システム/ソフトウェアのリリース前/維持運用中の脆弱性診断ルール/合格基準の作成、ルールの施行
  - パッチ/脆弱性情報の収集と社内配信、注意喚起、パッチ適用指示の実施
  - 社内の各種システム/ソフトウェアのインベントリ情報、パッチ/脆弱性情報の管理
  - 社内の各種システム/ソフトウェアのインベントリ、パッチ/脆弱性の適用管理
  - 社外/第三者からの脆弱性情報の連絡窓口の設置、対応業務の整備/維持運営（脆弱性対応プログラムの整備/維持運営）
- 脆弱性診断の請負業務（業務範囲に依存）
  - 各種脆弱スキャナを使った社内の各種システム/ソフトウェアの脆弱性診断業務の請負（ソフトウェア製品、構築システムの運用受託型、SaaS/クラウドサービス提供型、社内基幹/OA システム）
  - 各種脆弱スキャナを使った脆弱性診断業務の設計/構築/導入/維持運用
- 自社製品/サービスの脆弱性対応業務（業務範囲に依存）
  - 自社が維持運用/販売しているシステム/ソフトウェア/サービスの脆弱性対応業務全般
  - 自社で開発したソフトウェア製品に関連する脆弱性情報の収集（CVE 公開、ホワイトハッカー/研究者からの公式・非公式な情報連携/セミナー学会発表）
  - 自社で開発したソフトウェア製品で発見された脆弱性情報の脆弱性ハンドリング（IPA、JPCERT/CC 連携、広報/取材対応、脆弱性修正の技術的な支援）
  - バグバウンティプログラムの実施

ペネトレーションテストができる人材の育成プログラムは、脆弱性管理/診断業務の人材育成プログラムには含まれない。ペネトレーションテストができる人材は、脆弱性関連業務とインシデント対応業務の両方のスキルに加えて、サイバー攻撃に関するスキルが必要である。そのため、本プログラムの対象外とする。

4.4.2. 役割の全体的な位置づけ

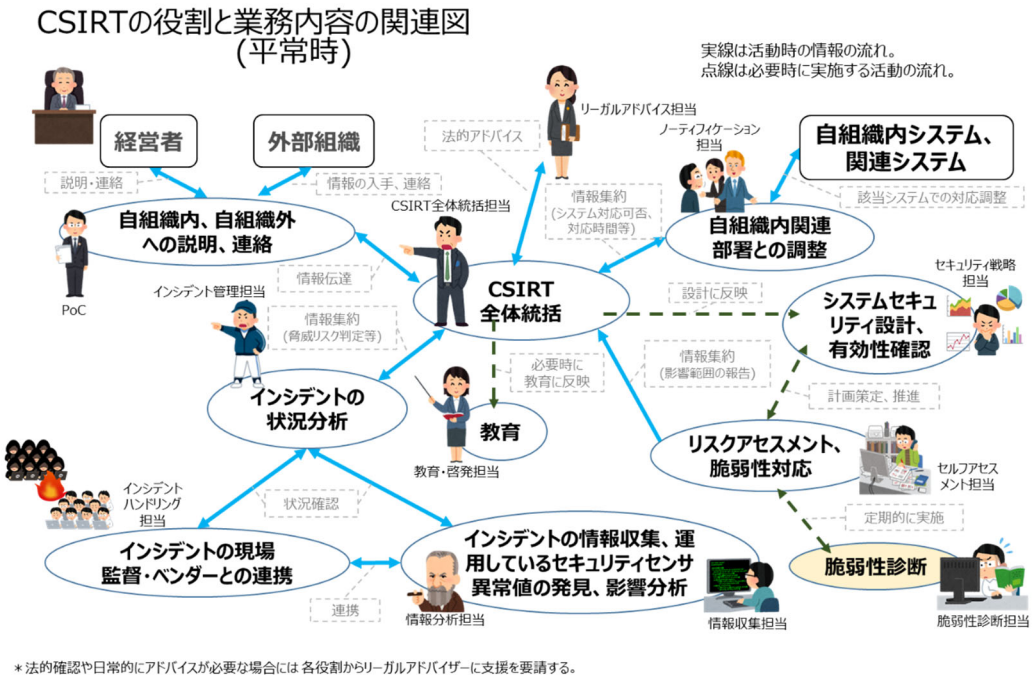


図 4-7 脆弱性管理/診断の全体的な位置づけ（平常時）

4.4.3. 育成 STEP の説明

表 4-4 育成 STEP の説明（脆弱性管理/診断）

STEP	対象者	説明
1	基礎教育修了者	基礎教育を終え、役割別の共通教育も終えた脆弱性管理/診断業務の新規配属者が、初心者をめざす。導入教育を受けて、業務の手順や機器の操作方法を学習する
2	担当役割の初心者	導入教育を完了した初心者が、見習いをめざす。一人前の脆弱性管理/診断担当者から指導を受けながら、学習した脆弱性対応や脆弱性診断業務の手順、脆弱性関連業務で使用する機器の操作方法を実際の業務で実践する。通常の脆弱性関連業務の一部を一人で処理できるようになることをめざす
3	担当役割の見習い	通常の脆弱性関連業務の一部を一人で処理できる見習いが、一人前のセキュリティ技術者になって担当業務を一人で処理できる一人前をめざす。一人前の脆弱性管理/診断業務担当者と一緒に業務を行い、経験を積む

4.4.4. 共通教育

役割別の共通教育として、脆弱性管理/診断業務に必要な基礎知識、技術を以下に示す。

- 一般的な OS、ネットワーク、システムの理解
- 一般的なセキュリティ事象、攻撃手法などの詳細理解
  - サイバー攻撃手法
- 自社システムを構成するネットワーク、サーバーなどの理解
  - 自社システムの概要の理解
  - 自社ネットワークの理解
  - 自社システムを構成するサーバーの理解
- 自社に関するセキュリティ的な防御機構、防御機能などの理解
  - インシデントや脆弱性のセキュリティ対応技術

4.4.5. STEP1：基礎教育修了者から担当役割の初心者にいたるまでの育成

脆弱性管理/診断業務へ新規配属された基礎教育修了者への教育内容を以下に示す。

4.4.5.1. 目標・目的

- 脆弱性管理/診断業務を理解する
- 脆弱性管理/診断業務を実行するための知識と技術を習得する
- 脆弱性管理/診断業務の手順を把握する
- 脆弱性情報やパッチ情報を収集できる

4.4.5.2. 学習項目/経験させる業務

- 脆弱性管理/診断業務の概要の把握
- 脆弱性管理/診断の対象システム/サービスの把握
- 脆弱性管理/診断業務に使用しているセキュリティ機器、監視機器の理解
- 脆弱性管理/診断業務の手順、操作の学習
  - 脆弱性診断ツールの操作方法の学習
  - パッチ/脆弱性情報の管理システムの操作方法の学習
- 脆弱性関連の基礎知識の学習(CVE、CWE、CVSS、脆弱性の仕組みの理解)
- 脆弱性情報提供サイトやサービスの把握

4.4.5.3. 参考となる外部講習、外部のドキュメント

- 脆弱性診断システムの入門書
- 脆弱性体験学習ツール AppGoat（IPA）[6]

4.4.5.4. 達成目安

- 脆弱性管理/診断業務の導入教育で指示された資料、書籍の読了
- 脆弱性管理/診断の概要、使用する脆弱性診断システム/サービスの概要を説明できる

4.4.6. STEP2：担当役割の初心者から担当役割の見習いにいたるまでの育成

脆弱性管理/診断業務の初心者への教育内容を以下に示す。

4.4.6.1. 目標・目的

- 脆弱性情報やパッチ情報を収集できる
- 脆弱性管理業務
  - 脆弱性管理対象の各種システム/ソフトウェアのインベントリ、パッチ/脆弱性情報の対応業務を手順にしたがって実施できる
  - パッチ/脆弱性情報の管理システムの操作方法を習得する
- 脆弱性診断業務
  - 脆弱性診断ツールを操作して、対象システムの脆弱性を診断できる
- 脆弱性管理/診断担当者の業務をサポートできる
- 指導者の指示にしたがって、定型の脆弱性管理/診断業務を実施できる

4.4.6.2. 学習項目/経験させる業務

- CVE、CWE、CVSS、脆弱性の仕組みなどの脆弱性関連の基礎知識の学習
- 脆弱性情報を提供するサイトやサービスの把握

[6] https://www.ipa.go.jp/security/vuln/appgoat/

- 脆弱性管理/診断業務の手順、操作の習熟
- 脆弱性診断ツールの操作方法の学習
- パッチ/脆弱性情報の管理システムの操作方法の学習
- 指導者の指示にしたがって、分析する
- 脆弱性がシステムや業務へ与える影響の検討

4.4.6.3. 参考となる外部講習、外部のドキュメント

- 脆弱性体験学習ツール AppGoat（IPA）
- ベンダー研修、トレーニングの受講によるネットワーク/脆弱性診断ツールの習得

4.4.6.4. 達成目安

- 脆弱性管理業務
  - 脆弱性情報から対象システムへの影響有無を評価できる
  - パッチ/脆弱性情報の管理システムを使って対象システムの脆弱性対応状況を管理できる
- 脆弱性診断業務
  - 脆弱性診断ツールを使って脆弱性を発見できる
  - 誤判断の割合が一定値未満であること。(診断回数が規定回数を満たすこと)
- 指導者の指示にしたがって、定型の脆弱性管理/診断業務を実施できる
- 指導者とペアで脆弱性管理/診断業務を規定回数実施する

4.4.7. STEP3：担当役割の見習いから担当役割の一人前にいたるまでの育成

脆弱性管理/診断業務の見習いへの教育内容を以下に示す。

4.4.7.1. 目標・目的

- 定型の脆弱性管理/診断業務を独力で実施できる
- 脆弱性管理業務
  - 脆弱性情報から対象システムがサイバー攻撃を受けるリスクの大きさ、影響の大きさを推測できる
  - 脆弱性情報を収集して関係組織へ配信、注意喚起、パッチ適用指示ができる

  - 脆弱性やパッチ適用に関する問い合わせ対応ができる
  - パッチ適用を計画/周知/指示できる
- 脆弱性診断業務
  - 脆弱性診断ツールの診断結果を分析して、リスクを評価できる
  - 診断対象システムに合わせて、診断計画を作成できる
  - 脆弱性のリスク評価結果から、報告書を作成できる
  - 診断対象システムに合わせて、脆弱性診断ツールのルールや手順をチューニングして最適化できる
- 最新の脆弱性情報を把握して、分析やリスク評価能力を維持、向上できる
- 後進(新規配属者や初心者、見習い)の育成ができる

4.4.7.2. 学習項目/経験させる業務

- 脆弱性管理業務
  - パッチ/脆弱性情報の管理システムの新しい機能やその操作を習得する
  - パッチ/脆弱性情報の管理システムを使って全対象システムの脆弱性対応状況を管理する
  - 関係組織へ脆弱性情報の配信、注意喚起、パッチ適用指示を行う
- 脆弱性診断業務
  - 脆弱性診断システムの新しい機能やその操作を習得する
  - 脆弱性診断システムのチューニング技術を習得する
- 対象システムの詳細を理解する
  - 対象システム/サービスを構成するソフトウェアの基本的な動作原理を理解する
  - 対象システムを構成するソフトウェアや通信プロトコルのアーキテクチャを理解する
  - 対象システム/サービスの設計書やインベントリ情報などから動作やデータフローを理解する

4.4.7.3. 参考となる外部講習、外部のドキュメント

- ベンダー研修、トレーニングの受講によるセキュリティ監視機器の新機能の習得
- 脆弱性の解説、検証レポートの購読、セミナー参加
- 新しいサイバー攻撃に関するレポートの購読、セミナー参加

4.4.7.4. 達成目安

- 脆弱性管理業務
  - パッチ/脆弱性情報の管理システムを使って、全対象システムの脆弱性対応状況を管理できる。
  - 迅速かつ的確なパッチ適用の計画/周知/指示ができる
  - 脆弱性管理業務を規定した期間/回数以上経験する
- 脆弱性診断業務
  - 脆弱性診断ツールを使って、脆弱性診断および脆弱性診断報告書を作成できる
  - 脆弱性管理業務を規定した期間/回数以上経験する
- 新しい脆弱性のリスクを評価、実システムへの影響を推測できる

4.5 フォレンジック

4.5.1. 役割の説明

フォレンジック業務の内容を以下に示す。

- データ収集/data collection
  - 事前ヒアリング
  - フォレンジック対象の特定
  - 証拠保全（物理記憶媒体ダンプ、メモリダンプ、ネットワークダンプ、クラウド他）
  - 証拠の運搬と保管
- 解析/抽出/examination
  - 削除データ復元
  - 分析対象データ/ファイル/ログの抽出（Acquisition、パケット解析）
  - 各種正規化(タイムスタンプ時刻、文字コード変換)
  - タイムライン作成
- 分析/Analysis
  - 基礎分析（決められた定型手順の分析）
    - 特定パターンの調査、検知
    - 異常発見
  - 特定領域の分析
    - マシン分析/アーティファクト分析
    - ミドルウェア/アプリケーションソフトウェア分析
    - マルウェア/プログラム分析
    - ネットワークフォレンジック/パケット分析/通信ログ分析
    - メモリフォレンジック
    - クラウドフォレンジック
- 報告/reporting
  - 原因分析
  - 侵害経路分析
  - 被害分析（侵害有無、漏えい有無、被害範囲）
  - 対策検討
  - 報告書作成

4.5.2. 役割の全体的な位置づけ

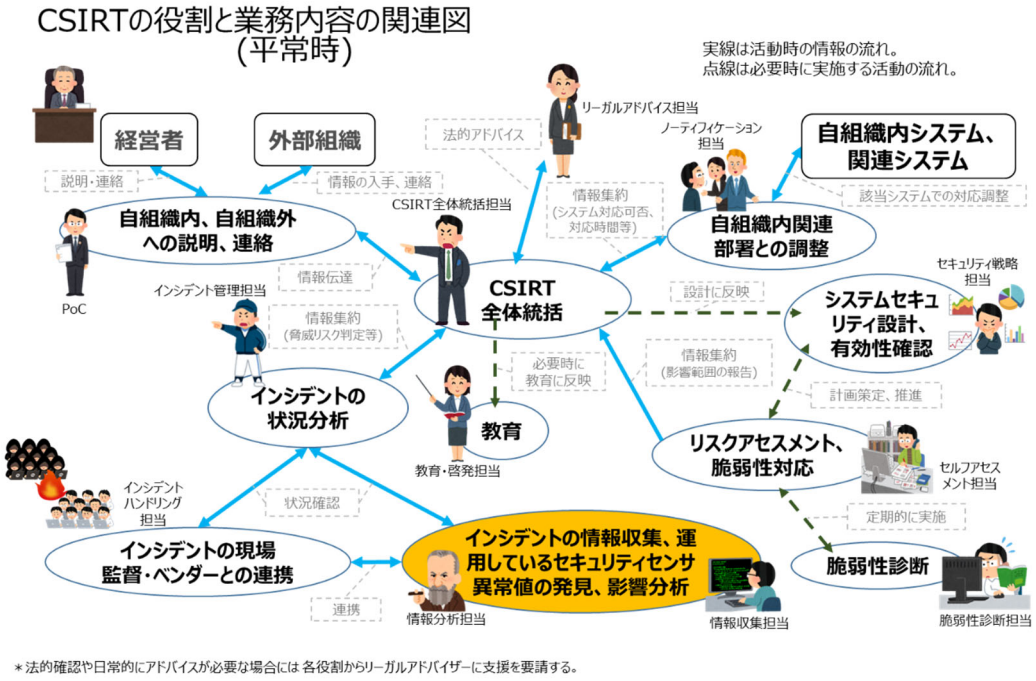


図 4-8 フォレンジックの全体的な位置づけ（平常時）

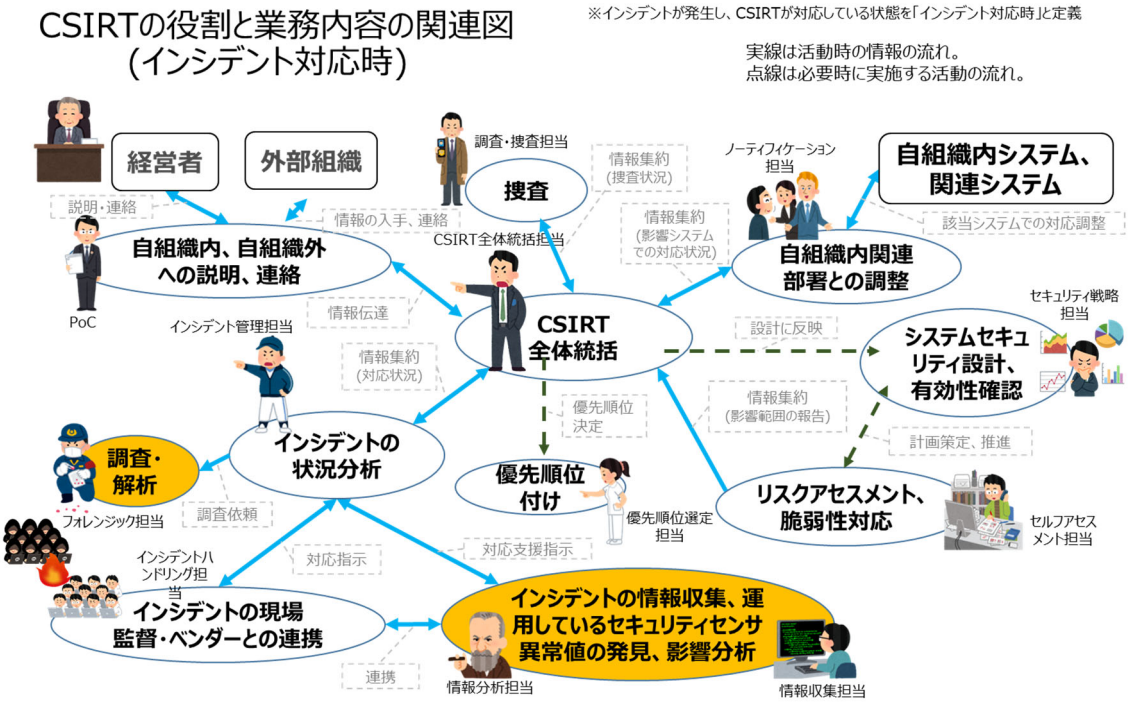


図 4-9 フォレンジックの全体的な位置づけ（インシデント対応時）

4.5.3. 育成 STEP の説明

表 4-5 育成 STEP の説明（フォレンジック）

STEP	対象者	説明
1	基礎教育修了者	基礎教育を終え、役割別の共通教育も終えたフォレンジック業務の新規配属者が、初心者をめざす。導入教育を受けて、フォレンジックの基本的な手順やフォレンジック用の機材や解析ソフトウェアの操作方法を学習する
2	担当役割の初心者	導入教育を完了した初心者が、見習いをめざす。一人前のフォレンジック担当者から指導を受けながら、学習したフォレンジックの基本的な手順やフォレンジック用の機材や解析ソフトウェアの操作方法を実際の業務で実践する。発生事例の多いインシデントのフォレンジック作業の一部を一人で処理できるようになることをめざす
3	担当役割の見習い	フォレンジック作業の一部を一人で処理できる見習いは、すべてのフォレンジック業務を一人で処理できる一人前をめざす。一人前のフォレンジック担当者と一緒に業務を行い、経験を積む

4.5.4. 共通教育

役割別の共通教育として、フォレンジック業務に必要な基礎知識、技術を以下に示す。

- 一般的な OS、ネットワーク、システムの理解
- ファイルシステムや OS 動作など、詳細な OS 関連の知識
- 通信プロトコルやパケットなどの詳細な通信関連の知識
- 一般的なセキュリティ事象、攻撃手法などの理解
  - サイバー攻撃の知識や手法の理解
  - マルウェアの知識
- 自社システムを構成するネットワーク、サーバーなどの理解
  - 自社システムの概要の理解
  - 自社ネットワークの理解
  - 自社システムを構成するサーバーの理解
- 自社関するセキュリティ的な防御機構、防御機能などの理解
  - インシデントや脆弱性のセキュリティ対応技術

4.5.5. STEP1：基礎教育修了者から担当役割の初心者にいたるまでの育成

フォレンジック業務へ新規配属された基礎教育修了者への教育内容を以下に示す。

4.5.5.1. 目標・目的

- フォレンジック業務を理解する
- フォレンジック作業の共通フレームワーク[7]を把握する
- 「データ収集/data collection」の基本的な作業を習得する
- 「解析/抽出/examination」の基本的な作業を習得する

4.5.5.2. 学習項目/経験させる業務

- フォレンジック業務の概要の把握
- フォレンジック業務のうち、「データ収集/data collection」や「解析/抽出/examination」に使用している機材と解析ソフトウェアの操作
- 「データ収集/data collection」の基本的な作業
  - 事前ヒアリング、フォレンジック対象の特定
  - 証拠保全作業
  - 証拠の運搬と保管
- 「解析/抽出/examination」の基本的な作業
  - 削除データ復元
  - 分析対象データ/ファイル/ログの抽出（Acquisition、パケット解析）
  - 各種正規化（タイムスタンプ時刻、文字コード変換）
  - タイムライン作成

4.5.5.3. 参考となる外部講習、外部のドキュメント

- 基礎から学ぶデジタル・フォレンジック　―入門から実務での対応まで―(安冨 潔・上原 哲太郎　編著、特定非営利活動法人デジタル・フォレンジック研究会　著）[8]
- デジタル・フォレンジックの基礎と実践（佐々木 良一　編著、上原 哲太郎／櫻庭 信之／白濱 直哉／野崎 周作／八槇 博史／山本 清子　著）[9]

---

[7] Guide to Integrating Forensic Techniques into Incident Response
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

[8] https://digitalforensic.jp/home/act/products/df-forensic/

[9] https://digitalforensic.jp/home/act/products/df_textbook/

4.5.5.4. 達成目安

- 業務の導入教育で指示された資料、書籍の読了
- SOC 業務の概要、使用する監視対象システム/サービスの概要を説明できる
- 指導者が指示した証拠保全の操作、作業を実施できる
- 指導者が指示した削除データの復元やデータ抽出の操作、作業を実施できる
- 指導者とペアで証拠保全からデータ抽出までの業務を規定回数実施する

4.5.6. STEP2：担当役割の初心者から担当役割の見習いにいたるまでの育成

フォレンジック業務の初心者への教育内容を以下に示す。

4.5.6.1. 目標・目的

- 「分析/Analysis」の基本的な分析作業を習得する
  - 「分析/Analysis」の特定の「分析技術」について、決められた定型手順の基礎分析を行い、特定パターンの痕跡を発見できる
  - 1 つ以上の分析技術を習得する
- フォレンジック業務のデータ収集から分析までの作業を実施できる
  - 発生事例の多いインシデントは、データ収集から分析まで独力で実施できる
  - その他のインシデントは、指導者の指示にしたがえば、データ収集から分析まで実施できる
- フォレンジック担当者の分析作業をサポートできる

4.5.6.2. 学習項目/経験させる業務

- 「分析/Analysis」の基本的な分析作業
  - 「分析/Analysis」の 1 つの「分析技術」について、決められた定型手順を使った基礎分析作業
  - 指導者とペアで、インシデントのマシン分析/アーティファクト分析、またはネットワークフォレンジック/パケット分析/通信ログ分析の作業
- フォレンジック業務のうち、「分析/Analysis」に使用している機材と解析ソフトウェアの操作

- 指導者の指示にしたがって、発生事例の多いインシデントのデータ収集から分析までを実施

4.5.6.3. 参考となる外部講習、外部のドキュメント

- 証拠保全ガイドライン第８版（特定非営利活動法人デジタル・フォレンジック研究会 「証拠保全ガイドライン」改訂ワーキンググループ編）[10]
- 改訂版 デジタル・フォレンジック事典（佐々木良一 監修、舟橋信 編集責任、安冨潔 編集責任、特定非営利活動法人デジタル・フォレンジック研究会 編）[11]
- 有償のフォレンジック研修

4.5.6.4. 達成目安

- 初心者向け教材として指示された資料、書籍を読了する
- 解析ソフトウェアを使って、指導者が指示した分析の操作、作業を実施できる
- 指導者とペアで証拠保全から分析までの業務を規定回数実施する
- 発生事例の多いインシデントは、データ収集から分析まで独力で実施できる

4.5.7. STEP3：担当役割の見習いから担当役割の一人前にいたるまでの育成

フォレンジック業務の見習いへの教育内容を以下に示す。

4.5.7.1. 目標・目的

- 「分析/Analysis」の応用的な分析作業を習得する
  - 「分析/Analysis」の特定の「分析技術」を用いた分析を行い、特定パターンの痕跡以外の異常な痕跡を発見できる
  - ２つ以上の分析技術を習得する
- 「報告/reporting」の基本的な作業を習得する
- フォレンジック業務のデータ収集から報告までの一連の作業を実施できる
  - 発生事例の多いインシデントは、データ収集から報告までの一連の作業を独力で実施できる

[10] https://digitalforensic.jp/home/act/products/home-act-products-df-guideline-8th/

[11] https://digitalforensic.jp/home/act/products/df-refernce/

  - その他のインシデントは、指導者の指示にしたがえば、データ収集から報告までの一連の作業を実施できる
- フォレンジック担当者の報告作業をサポートできる
- セキュリティ熟練技術者として、後進(見習い)の育成ができるようになる

4.5.7.2. 学習項目/経験させる業務

- 「分析/Analysis」の応用的な分析作業
  - 特定パターンの痕跡調査では分析できないインシデントについて、特定の「分析技術」を用いた分析作業（特定パターンの痕跡以外の異常な痕跡の発見）
  - トレーナーとペアで、マルウェア/プログラム分析やミドルウェア/アプリケーションソフトウェア分析などの未経験の分析作業
- 「報告/reporting」の基本的な作業
  - 原因分析
  - 侵害経路分析
  - 被害分析（侵害有無、漏えい有無、被害範囲）
  - 対策検討
- フォレンジック業務のうち、「報告/reporting」に使用している機材と解析ソフトウェアの操作
- 指導者の指示にしたがって、発生事例の多いインシデントのデータ収集から報告までの一連の作業

4.5.7.3. 参考となる外部講習、外部のドキュメント

- 有償のフォレンジック研修

4.5.7.4. 達成目安

- 指導者と証拠保全から報告までの業務を規定回数実施する
- 発生事例の多いインシデントは、データ収集から報告まで独力で実施できる
- マシン分析/アーティファクト分析、またはネットワークフォレンジック/パケット分析/通信ログ分析のどちらか 1 つの分析技術を使って、汎用的なインシデントの分析ができる
- 見習いレベルの人材の指導ができる

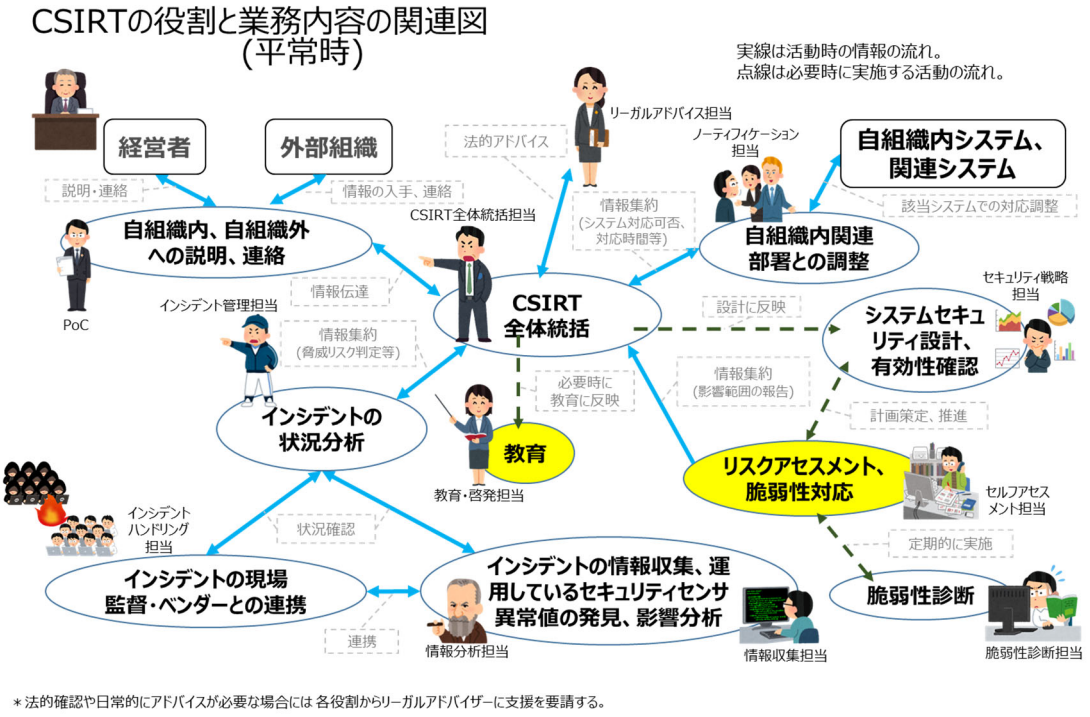
4.6 セキュリティマネジメント

4.6.1. 役割の説明

セキュリティマネジメント業務の内容を以下に示す。
なお、記載の一部の業務については実際の組織では CSIRT ではなく他部署の主体業務として割り当てられていると考えられる。しかし、CSIRT は原則として他部署の業務であってもインシデント発生時には対応が求められるため、CSIRT の積極的な関与（業務内容の把握や改善の支援）が必要と考えられる点について記載している。

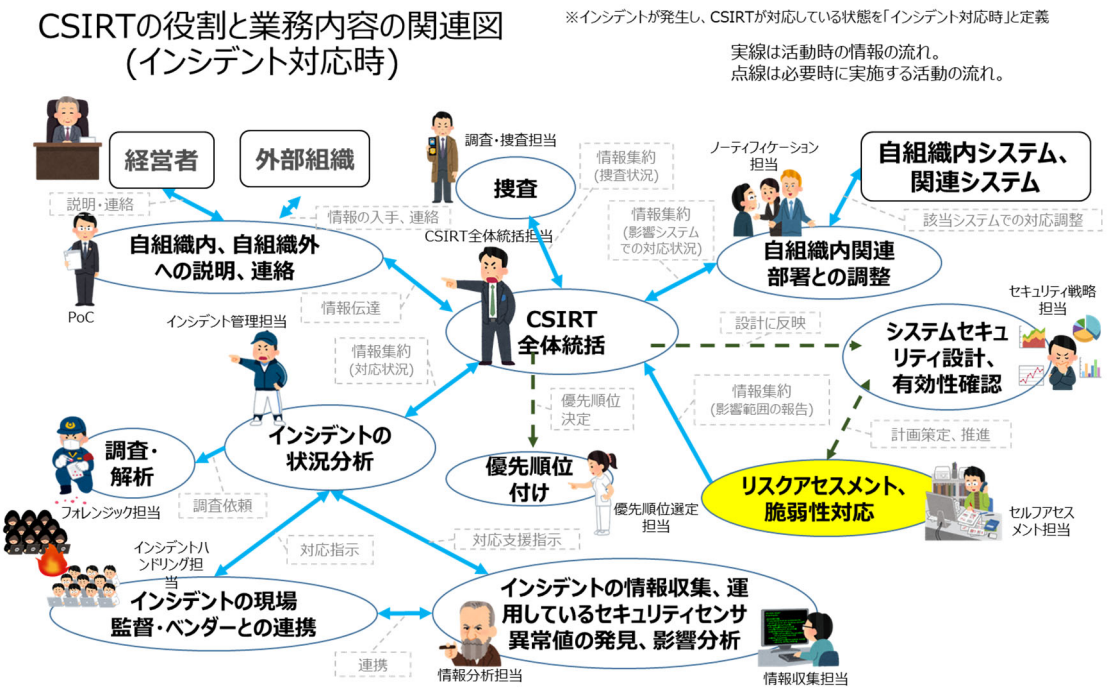
- 情報資産の管理や管理ルールの維持、改善を実施する
- リスクアセスメントを計画実行し、手法の問題点の改善を実施する
- リスク対策を維持し、既存対策の問題点の改善を実施する
- セキュリティインシデント管理（報告フローなどのインシデント管理システムを指す）を維持し、改善を実施する
- 情報セキュリティマネジメントシステム（ISMS）を維持し、改善を実施する
- 従業員に対して情報セキュリティ教育を実施し、改善を実施する
- 情報セキュリティガバナンスの取組みを維持する
- コンプライアンスを維持し、強化を実施する
- 事業継続計画（BCP）の定期的な見直しや訓練を実施する
- 災害対策（DR）の定期的な見直しや訓練を実施する

4.6.2. 役割の全体的な位置づけ



＊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。

図 4-11 セキュリティマネジメントの位置づけ（平常時）



＊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。

図 4-10 セキュリティマネジメントの位置づけ（インシデント対応時）

4.6.3. 育成 STEP の説明

表 4-6 育成 STEP の説明（セキュリティマネジメント）

STEP	対象者	説明
1	基礎教育修了者	基礎教育を終え、役割別の共通教育も終えたセキュリティマネジメント業務の新規配属者が、自社に導入済みで定期実施するセキュリティマネジメントの定型業務ができるようになる。
2	担当役割の初心者	自社に導入済みで定期実施するセキュリティマネジメントの定型業務において、指摘されている事項や現状の問題点を理解し、改善を検討できるようになる。
3	担当役割の見習い	自社に導入済みで定期実施するセキュリティマネジメントの定型業務において、指摘されている事項や現状の問題点について、改善策を実施できるようになる。

4.6.4. 共通教育

役割別の共通教育として、セキュリティマネジメント業務に必要な基礎知識、技術を以下に示す。

- コミュニケーション手法
  - IT やセキュリティ知識に乏しい人々に正しく伝える技術
  - 自社の経営陣、ビジネスオーナー、データーオーナーとの関係を良好にしておくための手法（経営戦略や事業戦略と矛盾しないセキュリティマネジメントプロセスを遂行するため）
- 対人能力（各部門との調整が必要となるため）

4.6.5. STEP1：基礎教育修了者から担当役割の初心者にいたるまでの育成

セキュリティマネジメント業務へ新規配属された基礎教育修了者への教育内容を以下に示す。

4.6.5.1. 目標・目的

- 自社に導入済みの情報資産の管理体制を維持する
- 自社に導入済みのリスクアセスメントの仕組みを維持する

- 自社に導入済みのリスク（セキュリティ）対策を維持する
- 自社の現状のセキュリティインシデント管理の仕組みを維持する
- 自社の情報セキュリティマネジメントシステム（ISMS）認証を維持する
- 自社の現状のセキュリティ教育の仕組みを維持する
- 自社の現状の情報セキュリティガバナンスを維持する
- 自社の現状のコンプライアンスを維持する
- 自社に導入済みの事業継続計画（BCP）を維持する
- 自社に導入済みの災害対策（DR）を維持する

4.6.5.2. 学習項目/経験させる業務

- 自社の情報資産の管理手順を学習する
- 自社のリスクアセスメントの手順を学習する
- 自社に導入済みのリスク対策ソリューションを学習する
- 自社のセキュリティインシデント管理の仕組みや導入済みのソリューションを学習する
- 自社の情報セキュリティマネジメントシステム（ISMS）認証を学習する
- 自社のセキュリティ教育の内容、導入済みソリューションを学習する
- 情報セキュリティガバナンスを学習する
- 自社の情報セキュリティガバナンス推進体制を学習する
- 自社のコンプライアンスに関わる規程を学習する
- 自社の事業継続計画（BCP）の手順を学習する
- 自社の災害対策（DR）を学習する
- 災害復旧の机上演習を実施する

4.6.5.3. 参考となる外部講習、外部のドキュメント

- 自社の情報資産の管理手順書を読む
- 自社に導入済みのリスクアセスメント手順書を読む
- ISO/IEC 31000（リスクアセスメント）の規程を読む
- ISO/IEC 31010（リスクアセスメント技法）の規程を読む
- 自社に導入済みのリスク対策ソリューションのホワイトペーパーを読む
- 自社のセキュリティインシデント管理の報告フローや導入ソリューションのホワイトペーパーを読む
- 情報セキュリティマネジメントシステム（ISMS）（ISO/IEC 27001、27002、27017）規程を読む

- 自社の情報セキュリティマネジメントシステム（ISMS）監査報告書を読む
- 自社のセキュリティ教育の内容や導入済みソリューションのホワイトペーパーを読む
- 自社で過去に実施したセキュリティ教育の報告書を読む
- ISO/IEC 27014（ガバナンス）の規程を読む
- 経済産業省発行の情報セキュリティガバナンス導入ガイダンスを読む
- 自社のガバナンス推進の文書や体制（組織図）を確認する
- 自社の社内規程、ガイドラインを読む
- 自社に導入済みの事業継続計画（BCP)、災害対策（DR）の計画書や手順書を読む
- 自社に導入済みの事業継続計画書を読む

4.6.5.4. 達成目安

- 自社の情報資産の管理手順を説明できるようになる
- 自社のリスクアセスメントの手順を説明できるようになる
- 自社に導入済みのリスク対策ソリューションの効果を説明できるようになる
- 自社のセキュリティインシデント管理の仕組みを説明できるようになる
- 自社の情報セキュリティマネジメントシステム（ISMS）認証の必要性について説明できるようになる
- 社員に対するセキュリティ教育の必要性について説明できるようになる
- 情報セキュリティガバナンスの必要性や自社の推進体制を説明できるようになる
- 自社のコンプライアンス規程を説明できるようになる
- 自社の事業継続計画（BCP）の手順を説明できるようになる
- 自社の事業継続計画（BCP）の定期的なテスト（演習）を行えるようになる
- 自社の災害対策（DR）の手順を説明できるようになる
- 自社の災害対策（DR）の定期的なテスト（演習）を行えるようになる

4.6.6. STEP2：担当役割の初心者から担当役割の見習いにいたるまでの育成

セキュリティマネジメント業務の初心者への教育内容を以下に示す。

4.6.6.1. 目標・目的

- 情報資産の管理の改善を検討する

- リスクアセスメント手法の改善を検討する
- リスク（セキュリティ）対策の改善を検討する
- セキュリティインシデントの管理フローの改善を検討する
- 情報セキュリティマネジメントシステム（ISMS）の維持の改善を検討する
- 社員のセキュリティ教育の改善を検討する
- 情報セキュリティガバナンスの強化を検討する
- コンプライアンスの強化を検討する
- 事業継続計画（BCP）の改善を検討する
- 災害対策（DR）の改善を検討する

4.6.6.2. 学習項目/経験させる業務

- 最新の情報資産の管理手法を学習する
- 自社の情報資産管理手法の問題点をビジネスオーナーやデータ管理者とディスカッションする
- 自社で発生した不正行為などインシデント発生状況を調べる
- 最新のリスクアセスメント手法やツールを学習し、導入済みの手法により自社の事業領域のリスクが十分に検出できているか比較する
- 最新のリスク対策ソリューションを学習する
- リスクアセスメントにより、検出した脅威に必要な対策が行えているかリスクアセスメントの結果と対策を比較する
- セキュリティインシデントの報告状況を調査し、関係者にヒアリングし、報告漏れや遅延、指摘などが発生していないか調査する
- インシデント報告フローの改善や管理ソリューションを検討する
- 情報セキュリティマネジメントシステム（ISMS）の監査報告書に記載の指摘事項について根本改善を検討する
- 内部監査者や被監査者と根本改善についてディスカッションする
- 過去のセキュリティ教育報告書とインシデントの発生状況を比較し、効果の有無や不足ポイントを調査する
- 最新のセキュリティ教育のツールやソリューションを検討する
- 自社の最新の事業戦略をビジネスオーナーにヒアリングして状況を把握する
- 自社の情報セキュリティガバナンスの強化について手法、ツール、ソリューションを検討する
- 最新の法令について、法務担当とディスカッションする
- 自社の事業に関わるコンプライアンス対策が自社の最新の事業戦略と整合性があるか検討する

- 既存の事業継続計画（BCP）が自社の最新の事業戦略と整合性があるか検討する
- 既存の災害対策（DR）が自社の最新の事業戦略と整合性があるか検討する
- 既存の災害復旧手順について、改良ポイントがないか関係者とディスカッションする

4.6.6.3. 参考となる外部講習、外部のドキュメント

- ベンダーから資産管理ソリューションの説明を受ける
- ベンダーからリスク管理ソリューションの説明を受ける
- ベンダーからリスク（セキュリティ）対策ソリューションの説明を受ける
- インシデント発生状況の報告書
- 自社の情報セキュリティ責任者に対するインシデント発生状況の報告書
- ベンダーからインシデント管理ソリューションの説明を受ける
- 自社の内部監査報告書
- 過去のセキュリティ教育報告書
- ベンダーからセキュリティ教育ソリューションの説明を受ける
- 自社の情報セキュリティ責任者に対するガバナンス報告書
- ベンダーから情報セキュリティガバナンス管理やモニタリングツール、ソリューションの説明を受ける

4.6.6.4. 達成目安

- 情報資産管理について、自社と最新の手法の違いを説明できる
- リスクアセスメント方法やツールについて、自社と最新の違いを説明できる
- リスク対策ソリューションについて、自社に欠けているものを説明できる
- 自社のセキュリティインシデントの報告状況や問題点について説明できる
- 自社の情報セキュリティマネジメントシステム（ISMS）内部監査における指摘事項を説明できる
- セキュリティ教育について、自社に不足しているポイントを説明できる
- 自社の情報セキュリティガバナンス遵守状況を説明できる
- 自社の情報セキュリティガバナンスについて、最新の手法、ツール、ソリューションを導入することで強化できるポイントを説明できる
- 自社の最新の事業戦略におけるコンプライアンスとの整合性について説明できる
- 自社の事業継続計画（BCP）が最新の事業戦略と整合性があるか説明できる
- 自社の災害対策（DR）が最新の事業戦略と整合性があるか説明できる

4.6.7. STEP3：担当役割の見習いから担当役割の一人前にいたるまでの育成

セキュリティマネジメント業務の見習いへの教育内容を以下に示す。

4.6.7.1. 目標・目的

- 情報資産の管理の改善を行う
- リスクアセスメント手法の改善を行う
- リスク（セキュリティ）対策の改善を行う
- セキュリティインシデント管理策の改善を行う
- 情報セキュリティマネジメントシステム（ISMS）の維持の改善を行う
- 社員のセキュリティ教育の改善を行う
- 情報セキュリティガバナンスの強化を行う
- コンプライアンスの強化を行う
- 事業継続計画（BCP）の改善を行う
- 災害対策（DR）の改善を行う

4.6.7.2. 学習項目/経験させる業務

- STEP2 を元に情報資産管理について、最新の手法を自社に適用することの効果とコストを調べる
- STEP2 を元にリスクアセスメントについて、方法の改善や最新のツール、ソリューションを自社に適用することの効果とコストを調べる
- STEP2 を元にリスクアセスメントの結果、自社のリスク対策が不十分と考えられるポイントについて、リスク対策ソリューションを導入することの効果とコストを調べる
- STEP2 を元に自社のインシデント管理策が不十分と考えられるポイントについて、フロー改善やツールやソリューションの導入について効果とコストを調べる
- STEP2 を元に情報セキュリティマネジメントシステム（ISMS）の内部監査報告書において、よく指摘される事項の根本対策を自社に導入することの効果とコストを調べる
- STEP2 を元に自社のセキュリティ教育が不十分と考えられるポイントについて、新たなソリューションを導入することの効果とコストを調べる
- STEP2 を元に情報セキュリティガバナンス強化の最新の手法、ツール、ソリューシ

ョンを自社に導入することの効果とコストを調べる
- STEP2 を元に自社の事業領域におけるコンプライアンス強化の必要性とコストを調べる
- STEP2 を元に事業継続計画（BCP）について、最新の事業計画とのギャップを解消する計画を立てる
- STEP2 を元に災害対策（DR）について、最新の事業計画とのギャップを解消する計画を立てる

4.6.7.3. 参考となる外部講習、外部のドキュメント

- 特になし

4.6.7.4. 達成目安

- 自社の情報資産管理の改善の必要性について、経営陣に説明できる
- 自社のリスクアセスメントの改善の必要性について、経営陣に説明できる
- 自社のリスク対策の必要性について、経営陣に説明できる
- 自社のインシデント管理策の改善の必要性について、情報セキュリティ責任者に説明できる
- 情報セキュリティマネジメントシステム（ISMS）の内部監査報告書において、よく指摘される事項の根本対策の導入の必要性について、経営陣に説明できる
- 自社のセキュリティ教育の改善の必要性について、経営陣に説明できる
- 自社の情報セキュリティガバナンス強化の必要性について、経営陣に説明できる
- 自社のコンプライアンス改善の必要性について、経営陣に説明できる
- 自社の事業継続計画（BCP）の改善計画を情報セキュリティ責任者に説明できる
- 自社の災害対策（DR）の改善計画を経営陣に説明できる

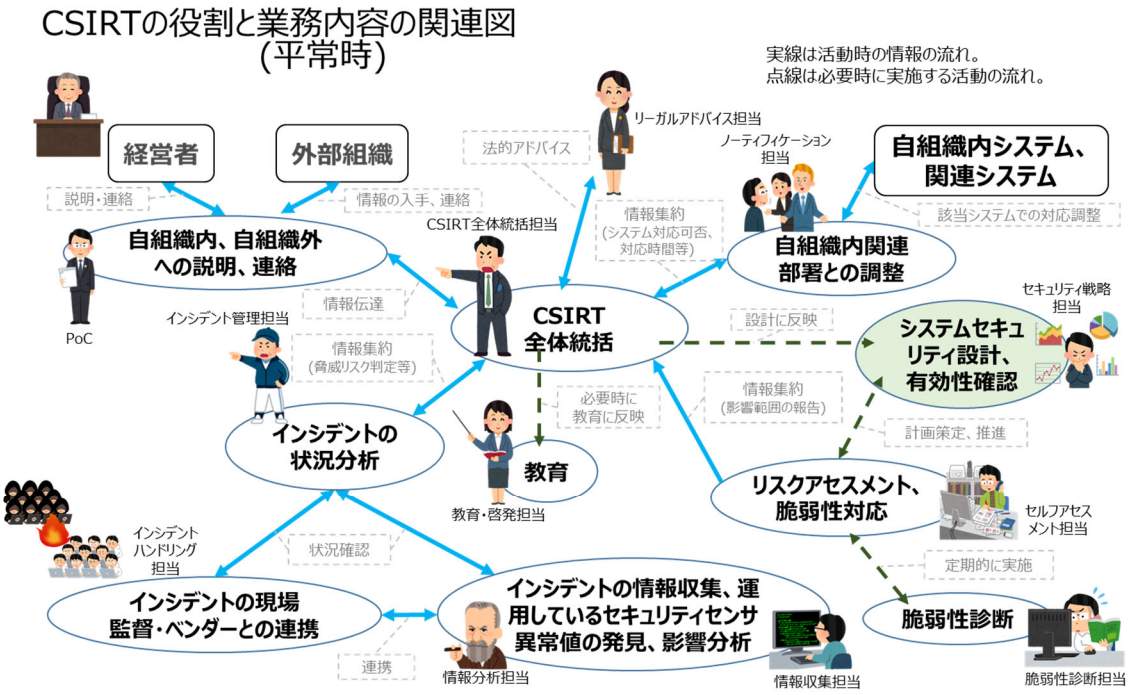
4.7 開発/開発支援

4.7.1. 役割の説明

開発/開発支援業務の内容を以下に示す。

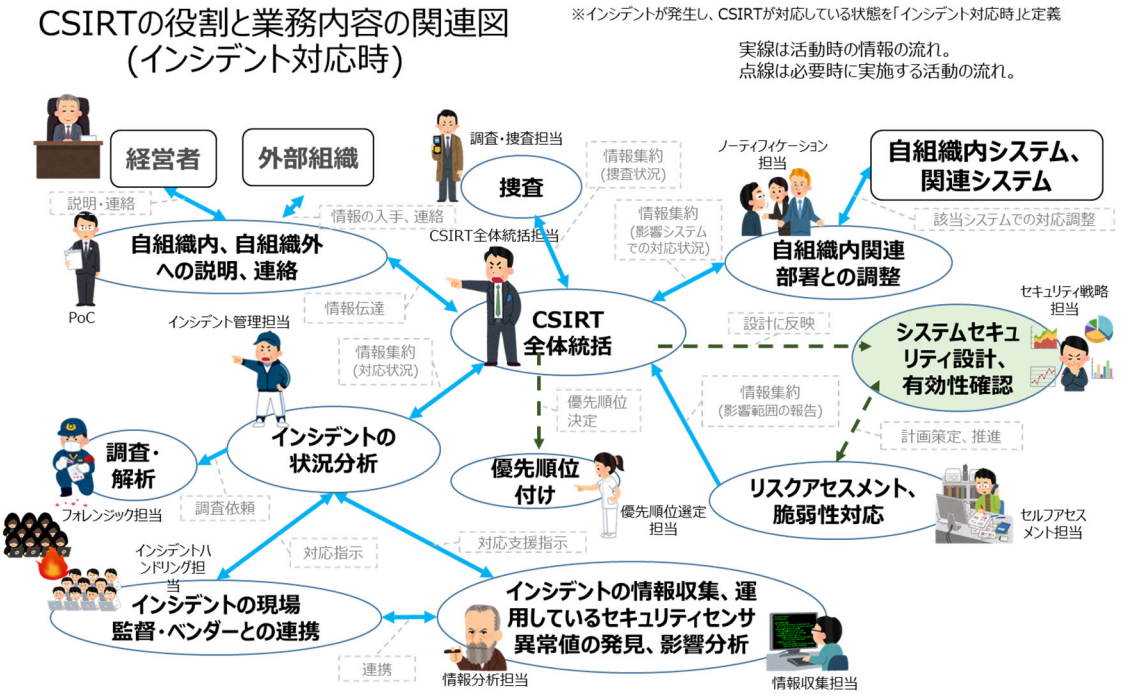
- 自社で開発するシステムのセキュリティ要件定義とセキュリティ基本設計を行う
- 自社で開発するアプリケーションがセキュリティ要件を満たし、適切なログが出力されるように開発者を支援する
- 自社で導入を検討しているパッケージ製品やクラウドサービスがセキュリティ要件を満たし、適切なログを出力できるかを確認する
- 自社システムのサーバーOS が要塞化要件満たし、適切なログが出力されるようにインフラ設計者を支援する
- 自社システムのネットワークにおいてネットワークアクセス権が最小になるように、また適切なログが出力されるようにネットワークエンジニアを支援する
- 自社システム環境に境界防御を行っている部分がある場合、侵入検知／侵入防御などの製品を導入し維持管理を行う
- 自社システムの利用する DB のアクセス権が最小になるように、また適切なログが出力されるように DB 設計者を支援する
- 統合ログシステムにすべてのログを集約し、適切な検知アラートや適切なレポートが SOC に出力されるように構築する
- マルウェア検知／除去／検疫などの基盤を整え、検知された場合は SOC に対してアラートが発報されるようにする
- 継続的脆弱性管理のシステムやサービス、改ざん／変更検知のシステム、DB Fire wall や WAF など他のセキュリティソリューションについても正しく機能するように維持管理を行う
- 自社システムの脆弱性の診断が定期的に行われるように計画し、調整し、実行する。脆弱性があった場合はアプリケーション開発やインフラの担当者が修正できるように支援する
- 自社システムが世の中のセキュリティ基準と比較して妥当な注意が払われている状態を維持するように公的機関や他のセキュリティ団体などが発表しているガイドラインを満たした自社のガイドラインを作成し維持する

4.7.2. 役割の全体的な位置づけ



＊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。

図 4-12 開発/開発支援の位置づけ（平常時）



＊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。

図 4-13 開発/開発支援の位置づけ（インシデント対応時）

4.7.3. 育成 STEP の説明

表 4-7 育成 STEP の説明（開発/開発支援）

STEP	対象者	説明
1	基礎教育修了者	共通教育を終え、役割別の共通教育も終えた開発/開発支援業務の新規配属者が、自社で稼働しているシステムがどのようなネットワーク構成で稼働し、セキュリティがどのように守られているか理解できることをめざす。 またセキュリティ設計をアシスタントとして一度は経験し、自分に割り当てられた役割を認識する
2	担当役割の初心者	STEP1 レベルの担当者が、自社に導入済みのセキュリティソリューションを使いこなせるようになり、簡単な開発案件のセキュリティ基本設計書を作成できるようになることをめざす
3	担当役割の見習い	STEP2 レベルの担当者が、機微情報を扱うアプリケーションのセキュリティ設計ができるようになり、世の中の脅威情報やインシデントから開発ガイドラインの不足に気付き、修正案を提示できるようになることをめざす

4.7.4. 共通教育

役割別の共通教育として、開発/開発支援業務に必要な基礎知識、技術を以下に示す。

- 一般的な OS、ネットワーク、システムの理解
- プログラミングや DB の理解
- サイバー攻撃手法
- セキュリティ対応技術
- 一般的な開発ガイドラインの知識
- 自社で独自に作成した開発ガイドラインの知識

4.7.5. STEP1：基礎教育修了者から担当役割の初心者にいたるまでの育成

開発/開発支援業務へ新規配属された基礎教育修了者への教育内容を以下に示す。

4.7.5.1. 目標・目的

- 自組織と世の中の現状をキャッチアップする
- 現行のセキュリティソリューションのアウトプットを理解する

4.7.5.2. 学習項目/経験させる業務

- 自社にどのようなシステムや情報資産があり、その利用目的を理解するために資産台帳を確認し、システムユーザーマニュアルを熟読する
- 自社のネットワークを理解するためにネットワーク設計書を熟読する
- 自社システム毎にセキュリティ要件定義書やセキュリティ基本設計書を読み、自社システムがどのような情報資産を持ち、どのように守られているかを理解する
- 公開されている世の中のセキュリティインシデントに関する情報に常日頃から関心を持ち自社のシステムにどのような脅威があるのかを理解する
- 自社が導入しているセキュリティソリューションの種類と導入目的を、基本設計書を読んで理解しアウトプットされる内容についてもマニュアルなどを参照し理解する
- 4.7.5.3 に記載するような公開または販売されているドキュメントを読み理解する

4.7.5.3. 参考となる外部講習、外部のドキュメント

- 安全なウェブサイトの作り方（IPA)[12]
- Web システム／Web アプリケーションセキュリティ要件書（脆弱性診断士スキルマッププロジェクト）[13]
- 体系的に学ぶ 安全な Web アプリケーションの作り方 第 2 版（徳丸 浩　著）
- 各セキュリティソリューションのベンダーが行うセミナー（初級・中級）
- セキュア Web アプリケーション開発講座
- 有償のセキュリティ研修

4.7.5.4. 達成目安

- 自社システムのセキュリティ要件定義書やセキュリティ基本設計書を読み、その設計意図が理解できること
- 新規システム構築時やシステム更改時に指導者と一緒にセキュリティ要件定義書や基本設計書を作成できること

---

[12] https://www.ipa.go.jp/security/vuln/websecurity.html

[13] https://github.com/OWASP/www-chapter-japan/tree/master/secreq

4.7.6. STEP2：担当役割の初心者から担当役割の見習いにいたるまでの育成

開発/開発支援業務の初心者への教育内容を以下に示す。

4.7.6.1. 目標・目的

- 高度なセキュリティ要件を求められない標準的なシステム（OWASP Application Security Verification Standard[14]レベルの Lv1 程度のシステム）の開発プロジェクトでセキュリティ基本設計書を自力で作成できる
- ネットワークや DB の最小アクセス権やサーバーOS の要塞化について各担当者に説明できるようになる
- 開発するシステムのビジネスロジック上にコンプライアンス違反がある場合は指摘できるようになる
- 現行のセキュリティソリューションを使いこなせるようになる

4.7.6.2. 学習項目/経験させる業務

- ガイドラインへの適合審査の結果をレビューし、指導者に指摘された不足分を修正することで審査能力を高める
- 高度なセキュリティ要件を求められない標準的なシステムの開発プロジェクトで、セキュリティ基本設計書のドラフトを自力で作成してレビューする
- 自社が導入しているセキュリティソリューションのマニュアルを読んで理解し、バージョンアップや設定変更の申請を自力で上げられるようにする
- セキュリティソリューションに対して変更作業を行った際には詳細設計書の更新をできるようにする
- システムに対する脆弱性診断を定期的に企画、実施、フォローする
- 以降で記載されている公開または販売されているドキュメントを読み理解する

4.7.6.3. 参考となる外部講習、外部のドキュメント

- サーバーの要塞化に関する CIS や Microsoft、SANS や NIST の SP800-123 などの

[14] https://owasp.org/www-project-application-security-verification-standard/

資料

- OWASP Application Security Verification Standard
- ISO 15001、PCI-DSS、FISC の安全対策基準、NIST SP800-171（連邦政府外のシステムと組織における管理された非格付け情報の保護）などの基準についての資料
- 個人情報の保護に関する法律についてのガイドライン
- 各セキュリティソリューションのベンダーが行うセミナー（上級）
- 有償のセキュリティ研修

4.7.6.4. 達成目安

- ガイドラインへの適合審査の結果をレビューした結果、指導者から何も指摘されなくなる
- 高度なセキュリティ要件を求められない標準的なシステムの開発プロジェクトでセキュリティ基本設計書が問題なく書けるようになる
- 現行のセキュリティソリューションの設定変更が自力で行える
- 後進にも教えられるようになる
- コンプライアンス違反を瞬時に判断できるようになる

4.7.7. STEP3：担当役割の見習いから担当役割の一人前にいたるまでの育成

開発/開発支援業務の見習いへの教育内容を以下に示す。

4.7.7.1. 目標・目的

- 保護を必要とする機微なデータを含むシステム（OWASP Application Security Verification Standard レベル 2 程度のシステム）の開発プロジェクトでセキュリティ基本設計書を自力で作成できる
- 世の中の脅威情報やインシデントを理解し自社の開発ガイドラインに修正が必要だと感じたら修正案を作成できる
- 現行のセキュリティソリューションの有効性を確認し、不足分がある場合は起案し、導入する

4.7.7.2. 学習項目/経験させる業務

- 保護を必要とする機微なデータを含むシステムの開発プロジェクトでセキュリティ基本設計書のドラフトを自力で作成してレビューする
- 世の中の脅威情報やインシデント情報、法改正の情報を入手しガイドラインの修正案を作成する
- 現行のセキュリティソリューションの有効性を確認し不足分がある場合には起案し、導入計画書を作成できる
- 自社が導入しているセキュリティソリューションのバージョンアップや設定変更の申請を自力で上げられるようにする
- セキュリティソリューションを新規導入する際のプロジェクト進捗を管理する経験を積む
- 継続的脆弱性管理ツールで脆弱性が発見された場合に、その脆弱性についての是正をシステオーナーに解説できるようにする

4.7.7.3. 参考となる外部講習、外部のドキュメント

- 新規導入を検討しているセキュリティソリューションのベンダーが行うセミナー
- 法改正などが行われる際に開催される外部セミナー
- PCI-DSS や FISC などが改定される際の外部セミナー
- 有償のセキュリティ研修

4.7.7.4. 達成目安

- 保護を必要とする機微なデータを含むシステムの開発プロジェクトでセキュリティ基本設計書が問題なく書けるようになる
- 世の中の脅威情報やインシデントを理解し自社のガイドラインに修正が必要だと感じたら修正案を作成できる
- 現行のセキュリティソリューションの有効性を確認し、不足分がある場合は導入を起案し、導入する

5章 おわりに

本資料は、CSIRT 人材の育成について取りまとめたものです。日本シーサート協議会の CSIRT 人材 WG の参加者の知見をもとに、具体的な業務に踏み込んだ記載を行い、現実的かつ実践的な内容となっております。本資料が各組織内 CSIRT における課題の解決または活動の一助となれば幸いです。

本資料について、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： 03-3270-0888
メール：nca-sec@nca.gr.jp

6章 著者一覧

ALPC-SIRT	弁護士法人アディーレ法律事務所	羽田 憲一郎
ALPC-SIRT	弁護士法人アディーレ法律事務所	吉岡 英一
ALPC-SIRT	弁護士法人アディーレ法律事務所	原田 圭二郎
ASY-CSIRT	ANA システムズ株式会社	阿部 恭一
ASY-CSIRT	ANA システムズ株式会社	岩井 洋
AW-CSIRT	株式会社アルファ・ウェーブ	柴山 芳則
DMM.CSIRT	合同会社 DMM.com	青木 一郎
FSAS-CSIRT	株式会社富士通エフサス	倉持 愼一郎
FUJIFILM CERT	富士フイルムホールディングス株式会社	大原 直子
Ierae-CSIRT	株式会社イエラエセキュリティ	鈴木 正泰
JBS-CIRT	日本ビジネスシステムズ株式会社	松方 岩雄
KC-SIRT	京セラ株式会社	酒井 啓光
LACERT	株式会社ラック	村上 晃
MB-SIRT	森ビル株式会社	佐藤 芳紀
MI-CSIRT	株式会社 三越伊勢丹システム・ソリューションズ	寺西 照一
NTT-CERT	日本電信電話株式会社	杉浦 芳樹
NTTDATA-CERT	株式会社 NTT データ	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
PIRATES	東京海上ディーアール株式会社	井出 雄介
PIRATES	東京海上ディーアール株式会社	大河内 智秀
Qdai CSIRT	国立大学法人 九州大学	岡村 耕二
Rakuten-CERT	楽天グループ株式会社	亀田 祥世
RM-CSIRT	楽天モバイル株式会社	伊藤 彰嗣
SBKG-CSIRT	株式会社新生銀行	小川 洋史
SBT-CSIRT	SB テクノロジー株式会社	丸岡 航太

Simplex-CSIRT	シンプレクス株式会社	前畑 隆志
SoftBank CSIRT	ソフトバンク株式会社	松本 勝之
SoftBank CSIRT	ソフトバンク株式会社	李 玉莉
TOPPAN-CERT	凸版印刷株式会社	池田 望
専門委員	日本シーサート協議会	山賀 正人
専門委員	日本シーサート協議会	北尾 辰也

（敬称略）

7章 改訂履歴

2021 年 3 月 31 日　Ver 0.9　β版作成
2022 年 3 月 31 日　Ver 1.0　β版に寄せられたコメントの反映、全体的な内容の改善