CSIRT人材の定義と確保(Ver.1.0)
補足資料

2016年2月23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)

本資料について

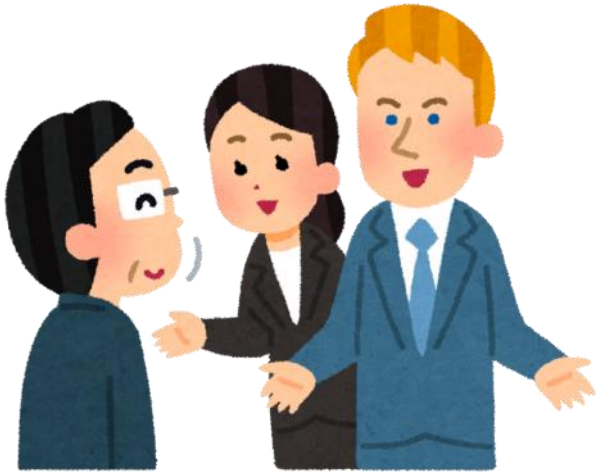
- 本資料は、「CSIRT人材の定義と確保(*)」の補足資料です。
  - (*) http://www.nca.gr.jp/imgs/recruit-hr20151116.pdf

- 「CSIRT人材の定義と確保」に記載されている代表的な役割名称毎に、その役割に任用するための前提スキルと、役割を遂行するために必要な追加スキルを記載しています。

PoC

- 社外・社内連絡担当
  - 社外窓口として、JPCERT、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部門調整担当社内の法務、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

ノーティフィケーション



- 社内情報発信・調整担当
  - 組織内を調整し、社内各関連部署への情報発信を行う。社内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
  - 自社システムに関する知識
- 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
  - 自社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

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Tobe像のFit&Gap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、改善計画に反映する。
- 任用前提スキル
  - 自社ビジネスビジョンに合わせて計画化する能力
  - 自社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
  - 自社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

脆弱性診断士

- 脆弱性の診断、評価担当
  - NW、OS、ミドルウェア、アプリケーションがセキュアプログラミングされている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、NW、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
  - 自社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

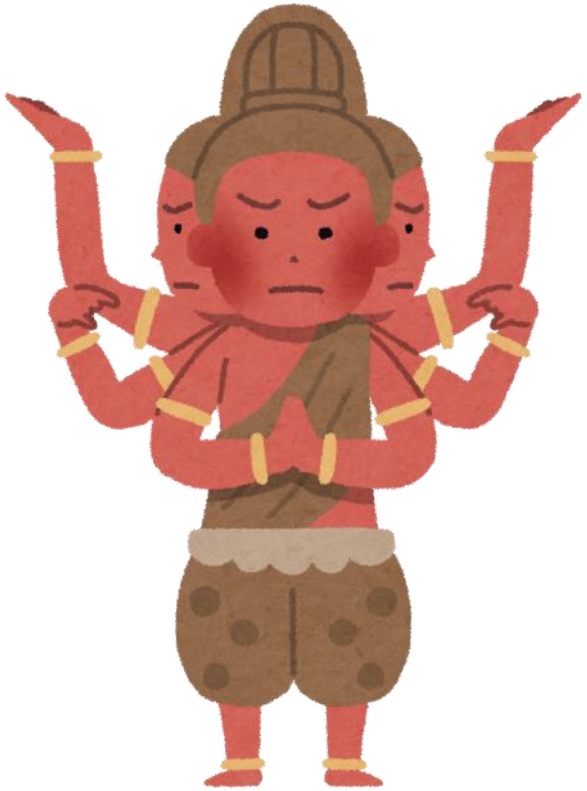
リサーチャー

- 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。収集のみで分析はしない。
- 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

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、その情報を自社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）とすることが多い
- 任用前提スキル
  - 自社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
  - 自社のセキュリティ対策に適用すべきか判断できる能力

コマンダー



- インシデント統制担当
  - 自社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
  - 自社のセキュリティアーキテクチャ、ビジネスに関する知識
  - 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

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
  - 自社のセキュリティアーキテクチャの知識
  - 自社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

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
  - 自社のセキュリティアーキテクチャの知識
  - 自社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

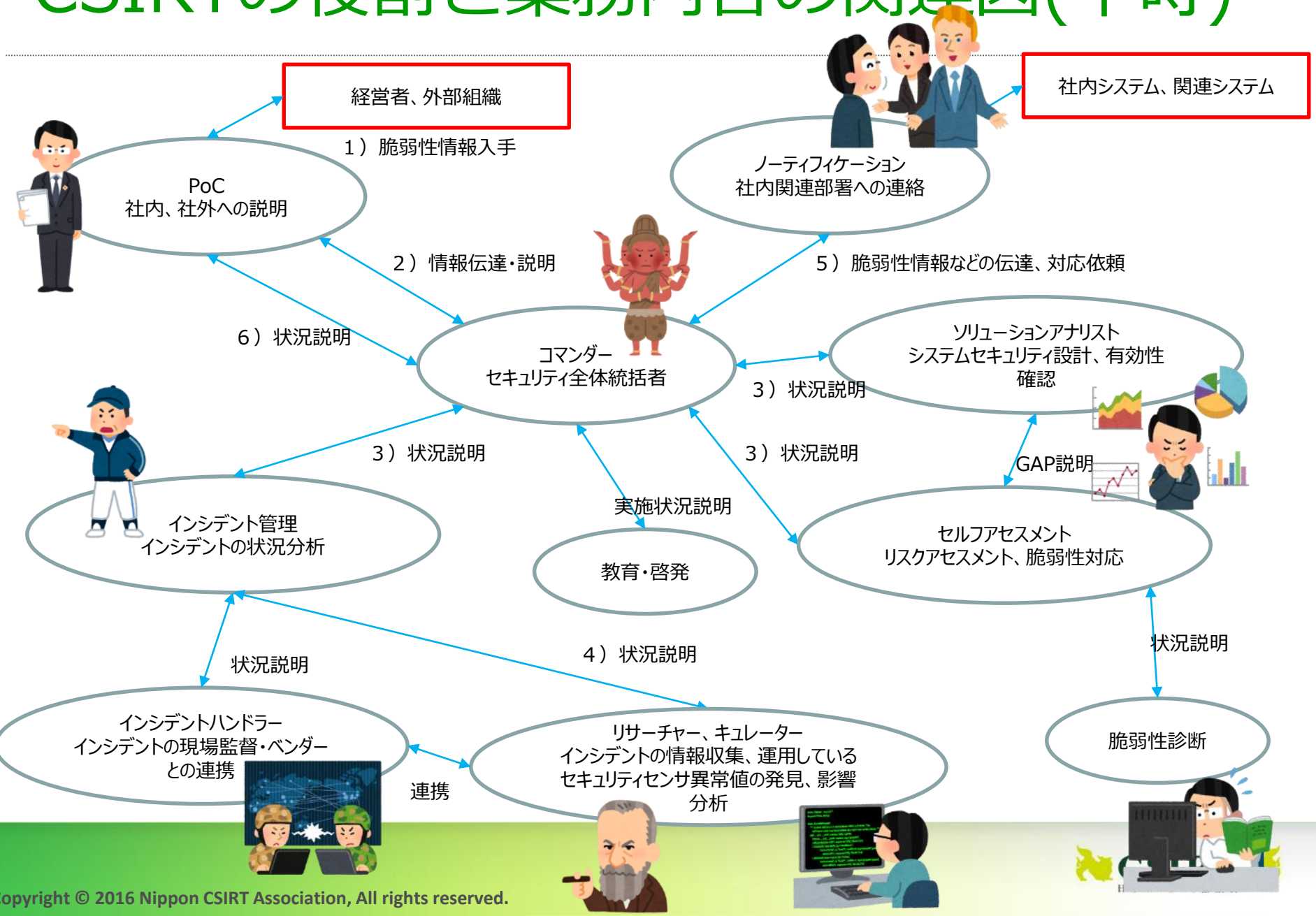
フォレンジックエンジニア

- 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

インベスティゲーター

- 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
  - 自社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

CSIRTの役割と業務内容の関連図(平時)



CSIRTの役割と業務内容の関連図(有事)