領域	セキュリティ領域												
専門分野	情報リスクストラテジ	情報セキュリティデザイン	セキュア開発管理	脆弱性診断	情報セキュリティアドミニストレーション	情報セキュリティアナリシス	CSIRTキュレーション	CSIRTリエゾン	CSIRTコマンド	インシデントハンドリング	デジタルフォレンジクス	情報セキュリティインベスティゲーション	情報セキュリティ監査
レベル7													
レベル6													
レベル5													
レベル4													
レベル3													
レベル2													
レベル1													
登録ｾｷｽﾍﾟ想定業務	経営課題	設計・開発		運用・保守				緊急対応					監査

専門分野	説明
情報リスクストラテジ	自組織または受託先における業務遂行の妨げとなる情報リスクを認識し、その影響を抑制するための、組織体制の整備や各種ルール整備等を含む情報セキュリティ戦略やポリシーの策定等を推進する。自組織または受託先内の情報セキュリティ対策関連業務全体を俯瞰し、アウトソース等を含むリソース配分の判断・決定を行う。
情報セキュリティデザイン	「セキュリティバイデザイン」の観点から情報システムのセキュリティを担保するためのアーキテクチャやポリシーの設計を行うとともに、これを実現するために必要な組織、ルール、プロセス等の整備・構築を支援する。
セキュア開発管理	情報システムや製品に関するリスク対応の観点に基づき、機能安全を含む情報セキュリティの側面から、企画・開発・製造・保守などにわたる情報セキュリティライフサイクルを統括し、対策の実施に関する責任をもつ。
脆弱性診断	ネットワーク、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。
情報セキュリティ アドミニストレーション	組織としての情報セキュリティ戦略やポリシーを具体的な計画や手順に落とし込むとともに、対策の立案や実施（指示・統括）、その見直し等を通じて、自組織または受託先における情報セキュリティ対策の具体化や実施を統括する。また、利用者に対する情報セキュリティ啓発や教育の計画を立案・推進する。
情報セキュリティアナリシス	情報セキュリティ対策の現状に関するアセスメントを実施し、あるべき姿とのギャップ分析をもとにリスクを評価した上で、自組織または受託先の事業計画に合わせて導入すべきソリューションを検討する。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。
CSIRTキュレーション	情報セキュリティインシデントへの対策検討を目的として、セキュリティイベント、脅威や脆弱性情報、攻撃者のプロファイル、国際情勢、メディア動向等に関する情報を収集し、自組織または受託先に適用すべきかの選定を行う。
CSIRTリエゾン	自組織外の関係機関、自組織内の法務、渉外、IT部門、広報、各事業部等との連絡窓口となり、情報セキュリティインシデントに係る情報連携及び情報発信を行う。必要に応じてIT部門とCSIRTの間での調整の役割を担う。
CSIRTコマンド	自組織で起きている情報セキュリティインシデントの全体統制を行うとともに、事象に対する対応における優先順位を決定する。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。
インシデントハンドリング	自組織または受託先におけるセキュリティインシデント発生直後の初動対応（被害拡大防止策の実施）や被害からの復旧に関する処理を行う。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する。情報セキュリティインシデントへの対応状況を管理し、CSIRTコマンドのタスクを担当する者へ報告する。
デジタルフォレンジクス	悪意をもつ者による情報システムやネットワークにを対象とした活動の証拠保全を行うとともに、消されたデータを復元したり、痕跡を追跡したりするためのシステム的な鑑識、精密検査、解析、報告を行う。
情報セキュリティ インベスティゲーション	情報セキュリティインシデントを対象として、外部からの犯罪、内部犯罪を捜査する。犯罪行為に関する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の絞り込みを行う。
情報セキュリティ監査	情報セキュリティに係るリスクのマネジメントが効果的に実施されるよう、リスクアセスメントに基づく適切な管理策の整備、運用状況について、基準に従って検証又は評価し、もって保証を与えあるいは助言を行う。