2023/7/29 Ver.2.0

●インシデントハンドラー

			定義
ジョブディスクリプション			**インシデント発生から調査完了までの技術的な知見をベースにした上位層への報告、専門職への指示を含む各種マネジメント** ・対応状況の把握とプライオリティの決定 ・上位層、セキュリティ責任者、事業責任者、必要者への報告・共有 ・専門家（外部ベンダ含む）への作業依頼 ・経過報告、最終報告など必要資料の作成、とりまとめ（含む広報対応支援） ・初動対応、復旧措置、暫定対応、再発防止策の立案、とりまとめ（原則として、実装完了までは追跡しない）
エントリー	業務遂行能力	管理	上位者のサポートにより、以下を部分的に実施できる： **⑧インシデント対応時の情報連携と記録管理活動** - インシデントハンドリングに伴う守秘義務、業務委託時のNDA等を理解遂行する - インシデント報告を受け付け、知るべき部署などに連携する - 一連の対応について記録を残す
		技術	上位者のサポートにより、以下を部分的に実施できる： **⑦インシデント対応の初期対応活動** - PCやサーバ、通信機器などのシステムからのログ収集作業 - ログなどの簡易調査（文字列調査、パケット調査 等） - セキュリティパッチ適用やパッチの確認作業 **⑨システム隔離作業**（VLAN切り替え、LAN切り離し、サービス停止 等） **⑩システム復旧作業**（VLAN切り替え、LAN接続、サービス再開 等） **⑪システム復旧後のログ等の確認作業** - 期間を定めた検知機構のシグネチャ検証やログ等の確認作業 **⑫検知機構に対するシグネチャ登録作業**
	知識	管理	**④セキュリティに関連する法令、制度等の理解** - 不正アクセス禁止法、個人情報保護保護法 等 - ISO/IEC 27001、PCIDSS 等 - 外部組織との情報連携や脆弱性情報等の取扱い(TLP) **⑥組織におけるセキュリティ活動の理解** - 組織内におけるポリシーなどの理解 - 組織内における重要システム、資産等の把握 - 組織内におけるシステム構成や課題等の理解
		技術	**①一般的なOS/アプリケーションのテクノロジーやセキュリティ機能の理解** - OSの基本的な設定項目 - GUIやシェルの基本的な操作 **②ネットワークテクノロジーやプロトコルの理解** - ネットワークセキュリティの基本的な仕組み - セキュリティ管理や検知・防御システムの理解 **③代表的な脆弱性の発生メカニズムと緩和方法の理解** - 各脆弱性の発生要因と対策 - 脅威動向の把握や脆弱性情報の取り扱い方法 **⑤運用面に対する課題の理解** - バックアップや一般的なパッチ適用、アップデートサイクル - 相互に連携したシステムの理解

アプローチ

（習得の順番を表しています。下から順番に習得するのが推奨です。）