●IoT脅威分析士

2023/7/29 Ver.1.0

			定義
ジョブディスクリプション			**IoTデバイスを含むIoTシステムの脅威分析し、想定脅威に対する脆弱性の報告や対策の提言** ・IoTデバイスおよび構成するIoTシステムに対して脅威を想定しリスクを特定 ・設計・開発段階において考慮すべきリスクの優先度とその対策を提言 ・判明したリスクを報告・提案
エントリー	業務遂行能力	管理	上位のサポートにより以下を部分的に実施できる： **⑩IoTデバイス脅威分析業務（情報収集・報告書作成・リスク評価）** -脆弱性に関する公開情報(NVD、JVNなど)を収集できる -報告書に記載すべき内容について知っていて、報告書を作成できる -リスク評価基準に則ってリスク評価ができる
		技術	上位のサポートにより以下を部分的に実施できる： **⑥製品設計書、仕様書、マニュアル等の読み解き** -製品設計書・仕様書から製品の構成要素や実装を読み解く -マニュアルから製品の持つ機能要素を推測する -製品の設計書、仕様書、フローチャート、データシートを読み解く **⑦実装基板から主要部品を特定し、その特性を悪用してリスクを特定** -対象となる製品の実装基板上に実装されている主要なICなどの部品を特定し、部品の機能や特性を悪用した攻撃リスク(FWの更新による悪用方法など)の指摘および対策の提案ができる
	知識	管理	**⑤関連法、標準に関する知識** -法律または罪状に関する基礎的な知識や、典型的な事例の知識 -診断をする際の守秘義務を理解している -必要な情報の正しい取得方法を理解している **⑧CVSSの目的や概要の知識およびゼロデイ情報の取り扱いに関する知識** -ゼロデイ情報の適切な扱い方を理解している -脆弱性関連情報の届け出制度を理解している -脆弱性診断業務に関連するセキュリティに関する基準の概要を理解している **⑨リスク評価と特定の手法に関する知識** -リスク評価の手法に対する目的や概要の知識(CVSS, DREADなど) -リスク特定の手法に対する目的な概要の知識(STRIDE/CCDS-STRIDE, EVITA, Attack Treeなど)
		技術	**①コンピュータサイエンス/ITに関する基礎知識** -コンピュータの基本構成、動作原理、コンピュータサイエンスに関する基礎的な知識 -ソフトウェア開発、言語、特性などソフトウェアエンジニアリングに関する基礎的な知識 -ネットワーク構成、プロトコル、機能、特性などネットワークに関する基礎的な知識 -OSやディストリビューションなどOSに関する基礎的な知識 -通信における認証方式に関する知識 **②IoTデバイス・ハードウェアに関する知識** -基本的な電子部品・回路設計に関する知識 -デバイスデータシートの読み方の知識 -CPU、メモリ、SoCに関する知識 -デバッグ機能に関する知識 **③セキュリティに関する基礎知識** -セキュリティにおける基本的概念 -サイバー攻撃における共通的な手法、主要な手法に関する知識 -データ保護に関する知識 **④IoTデバイスのセキュリティに関する基礎知識** -基盤の保護方法に関する知識 -ファームウェアの更新方法に関する知識 -セキュアブートに関する知識　-通信プロトコルに関する知識(CAN, MOSTなど) -IoTデバイスに用いられるOSの知識

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。）