2023/7/29 Ver.2.0

●IoTデバイス脆弱性診断士

			定義
ジョブディスクリプション			**IoTデバイスの脆弱性診断を実施** ・IoT機器のファームウェアやハードウェアの脆弱性やセキュリティ機能の調査 ・脆弱性診断の報告書の作成と説明、対策の提言
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デバイス脆弱性診断業務（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プロトコルに対するファジング** -製品に実装されたプロトコルを把握し、対象となるプロトコルに対するファジングや脆弱性調査(通信内容解析、ポートスキャン、中間者攻撃など)を実施できる **⑧実装基板から主要部品を特定し、その特性を悪用して攻撃を行うスキル** -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等の部品を特定し、部品の機能や特性を悪用した攻撃(デバッグ機能の悪用など)の検討および実施できる
	知識	管理	**④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 **⑨CVSSの目的や概要の知識、ゼロデイ情報の取り扱い** -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
		技術	**①コンピュータサイエンス/IT基礎** -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 **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 **⑤IoTデバイスの脆弱性に関する知識**

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。）