カリキュラム

機構施設名： 静岡職業能力開発促進センター
実施機関名： **株式会社パワートレイン**
25-22-12-021-013

A. バックオフィス	クラウド・IoT導入	021IoT導入に係る情報セキュリティ

コースのねらい	情報セキュリティ対策の適正化を目指して、IoT導入の有用性及び情報セキュリティに関するリスク及びセキュリティチェック等の必要な対策についての知識及び技術を習得する。

		「基本項目」		「主な内容」	訓練時間（H）	日程 月日	日程 時刻
講義内容	1	IoT（Internet of Things）導入	（1）IoTの基礎と最新動向 ・IoTの基本概念（クラウド、SaaS、AI、ビッグデータなど関連情報も含む） ・IoTの事例（スマート工場、遠隔監視など） ・最近の導入事例と利便性（例：中小企業の在庫管理自動化） ・IoTを取り巻く最新の脅威（デバイス乗っ取り、データ漏洩など）	1.5	令和7年 11月20日（木）	9:30～16:30 昼休憩 12:00～13:00
	2	情報セキュリティ	（1）IoTセキュリティの基本方針と最新トレンド ・経営層の関与とセキュリティ方針の策定 ・クラウド（SaaS）を使用するための基本的な考え方の徹底 ・ゼロトラストセキュリティモデルの概要と適用例（例：社内ネットワークでの毎回認証） ・内部不正や人的ミスへの備え ・物理的・ネットワーク的リスクの違い ・物理的リスクの例（泥棒や火事、紛失、破損など） ・ネットワークのリスク（漏洩、感染、侵入など） ・最近の攻撃事例から学ぶ（例：カメラ乗っ取り事件）	1.5		
			（2）IoTリスクへの対策設計とリスク評価【演習あり】 ・リスク評価の基本的な考え方 ・自社で使う可能性のあるIoT機器（例：センサー、カメラ）とそのリスクを考える	1.0		
			（3）ネットワークとデバイスの最新セキュリティ対策 ・クラウドベースのソリューション（AWS IoT、Azure IoT）の概要とメリット（例：リアルタイム監視の実現） ・安全なデータ送信の課題と対策を考える（例：暗号化、認証） ・AIを活用したセキュリティ監視の仕組みと事例（例：異常検知で不正アクセスを検出）	1.0		
			（4）高度なセキュリティ技術の活用【演習あり】 ・自社環境のセキュリティレベルの「アセスメント（自己採点）」 ・ブロックチェーン技術を使ったデータ保護の概要と適用例（例：データ送信記録の改ざん防止） ・多要素認証（MFA）の導入とその効果（例：デバイス管理アプリにMFA導入）	1.0		
				合計時間	6時間		

カリキュラム作成のポイント

このカリキュラムにて参加者はIoTの基本概念から最新のセキュリティ対策まで幅広く学ぶことができます。特に、実際の事例や演習を通じて、理論だけでなく実践的なスキルも身につけられます。また、最新の脅威やリスクに対する対策を学ぶことで、企業のセキュリティレベルを向上させることができます。カリキュラムは、経営層から現場担当者まで幅広い層に対応しており、具体的な導入事例や演習を取り入れることで、実践的かつ効果的な学びを提供します。