カリキュラムシート

分類番号

訓練分野	電気・電子系	訓練コース	ＩｏＴ導入にかかる情報セキュリティ対策
訓練対象者	製造現場のシステム管理業務に従事する技能・技術者等であって、指導的・中核的な役割を担う者又はその候補者		
訓練目標	製造現場へのＩｏＴ導入に係る情報セキュリティ対策の適正化をめざして、ＩｏＴ導入の有用性及び情報セキュリティに関するリスク等を理解すると同時に、現場におけるセキュリティリスクチェック及び必要な対策等について習得する。		

教科の細目	内　　容	訓練時間	うち実習・まとめ
		(H)	(H)
１．コース概要	（１）コースの概要及び専門的能力の確認	1.0	
	（２）ＩｏＴ導入の背景について		
	（３）利便性と危険性について		
２．ＩｏＴ導入	（１）Ｉｎｔｅｒｎｅｔ接続の方法	2.0	1.5
	（２）ネットワークの利用方法		
	（３）クラウドの活用方法		
３．情報セキュリティ	（１）ファイアーウォールによる防衛	5.0	4.0
	（２）パスワード解読によるアカウント乗っ取りと防衛		
	（３）ウィルスによる攻撃とアンチウィルスソフト		
	（４）ＤｏＳやＤＤｏＳ攻撃と防衛法		
	（５）システムの冗長性による障害対策		
４．セキュリティリスクチェック	（１）リスクの洗い出し方法	3.0	2.5
	（２）各種ログの活用方法		
	（３）パケットモニタ利用のすすめ		
５．まとめ	（１）実習の全体的な講評および確認・評価	1.0	1.0
		12.0	9.0

使用器具等	パソコン、ネットワーク、組込み端末
養成する能力	生産性の向上を実現できる能力

訓練コースの関連情報

			分類番号	
コース名		IoT導入にかかる情報セキュリティ対策	レベル	3
習得する技術要素及び到達目標（教科の構成要素）		IoT導入による情報セキュリティに関するリスクを理解する。		
		セキュリティリスクチェックを行い、担当技術者への対策指示方法を習得する。		
受講の条件等				
受講前に必要知識（受講の前提条件）		製造現場でコンピュータを扱う業務に携わっている方、 コンピュータのキーボード操作やマウス操作に精通していること		
受講時の持参品・服装等		筆記用具		
使用教材等				
訓練用テキスト市販図書名等		参考文献（テキストではなく、あくまで参考として「IoT時代のセキュリティ脅威と対策」 中野学著　http://sec.ipa.go.jp/users/seminar/seminar_tokyo_20150330-03.pdf）		
訓練の進め方				
導入部	「教科の細目」名	概要		
	主となる内容	IoTの現状を紹介し、その利点を理解してもらう。		
	進め方のポイント	危険性を紹介する前に、まず利便性を納得してもらう。		
提示部	「教科の細目」名	IoT導入		
	主となる内容	ネットワークの接続方法と利用方法、さらにクラウドの活用方法を体験し、理解する。		
	進め方のポイント	体験することで、感覚的にも理解をすすめる。		
	情報収集先（事例・例題等）			
	「教科の細目」名	情報セキュリティ		
	主となる内容	パスワード解読、ウィルス攻撃、DoS攻撃を体験（ウィルスに関しては疑似）する。		
	進め方のポイント	パスワード解読ソフトやパケット送信ソフトなどソフトウェアを操作することで、簡単なパスワードは解読されたりDDoS攻撃でコンピュータが反応しなくなることを体験する。ただし、危険性を体験するだけでなく原因（攻撃）と結果を結び付けて経験する。		
	情報収集先（事例・例題等）			
	「教科の細目」名	セキュリティリスクチェック		
	主となる内容	セキュリティリスクの洗い出しを演習する。リスクチェックに欠かせない各種ログを確認方法を習得し、パケットモニターソフトの利用を経験する。		
	進め方のポイント	リスクの洗い出しはグループでのディスカッション形式で行う。各種ログの確認やパケットモニターの利用は基本的なものにする。		
	情報収集先（事例・例題等）			
実習部	安全面で注意すべき点	VDT作業を行うため、適宜休憩をとる		
	「教科の細目」名	実習課題		
	主となる実習内容	ネットワークに接続しクラウドを活用、セキュリティソフトの利用、パケットモニタの使い方など		
	進め方のポイント	物理的なネットワーク接続から各種ソフトの使い方まで、まず、概要を説明し、基本動作（操作）、応用動作（操作）を進める。		
	使用する機器等	パソコン、ネットワーク、組込み端末		
まとめ	進め方のポイント	IoT導入の有用性及び情報セキュリティに関するリスク等について理解できているか確認する		