

科目	カリキュラム		概要	研修スタイル
モバイルセキュリティ				
	0.確認テスト 9:30～10:00			机上テスト
	1.モバイルコンピューティング			講義
	10:00～11:00	1.1 モバイルコンピューティング普及の背景		
		1.2 モバイルコンピューティングのメリット・リスク		
		1.3 無線ネットワーク	1.3.1 短距離無線 1.3.2 無線PAN 1.3.3 無線MAN 1.3.4 無線WAN	
		1.4 無線LAN	1.4.1 無線LANのメリット 1.4.2 無線LANのリスク 1.4.3 無線LANが使用できる周波数帯 1.4.4 無線LANの構成	
		1.5 標準化動向	1.5.1 無線LAN標準規格の歴史 1.5.2 無線LAN規格の概要 1.5.3 新しい技術 1.5.4 業界団体	
	2.無線LAN環境の構成			講義 + 演習
	11:15～12:30 13:30～14:00	2.1 構成装置	2.1.1 無線LANアダプタ 2.1.2 アクセスポイント 2.1.3 その他の機器 2.1.4 方式による構成の違い	
		2.2 無線LAN制御のしくみ	2.2.1 各層で使用される規格 2.2.2 変調のしくみ 2.2.3 FHSSのしくみ 2.2.4 DSSSのしくみ 2.2.5 OFDMのしくみ 2.2.6 スキャン 2.2.7 CAMA/GA	
		2.3 基本的な設定手順	2.3.1 アクセスポイントへの初期設定 2.3.2 無線LANアダプタの取り付けと設定 2.3.3 接続状況の確認	
		2.4 設定方法	2.4.1 アクセスポイントの初期設定 2.4.2 無線LANアダプタの初期設定 参考A OSI参照モデル	
	14:00～14:30	2.5 演習	現状の無線LAN機器の設定を確認し、接続確認を行う	
	3.無線LANの危険性			講義 + 演習
	14:45～16:00 16:15～16:50	3.1 無線LAN環境をとりまく脅威	3.1.1 盗聴(通信内容の傍受) 3.1.2 不正アクセス 3.1.3 アクセスポイントのなりすまし 3.1.4 脅威に対するセキュリティ機能	
		3.2 ESS-ID漏洩		
		3.3 MACアドレス認証の脆弱性		
		3.4 WEPの脆弱性	3.4.1 WEPによる暗号化 3.4.2 WEPの脆弱性	
		3.5 設定方法	3.5.1 ESS-IDの設定 3.5.2 ANY接続・WEPの設定 3.5.3 MACアドレス認証	
	16:50～17:30	3.6 演習	基本的なセキュリティ(ESS-ID、MACアドレス設定、WEP設定)設定と確認	
	4.無線LANセキュリティ対策			講義 + 演習
	9:40～11:00	4.1 無線LANセキュリティの概要		
		4.2 無線LANにおける暗号化	4.2.1 暗号方式 4.2.2 暗号化アルゴリズム 4.2.3 認証機能と暗号化	
		4.3 無線LANにおける認証	4.3.1 IEEE802.1xのプロトコルスタック 4.3.2 IEEE802.1x認証の種類	
		4.4 無線LANにおける検疫システム	4.4.1 検疫システムの機能 4.4.2 検疫システムの方式	
		4.5 IPsecによるセキュア無線LAN		
		4.6 設定方法	4.6.1 TKIPの設定 4.6.2 AESの設定 4.6.3 EAPモードの設定	
	11:15～12:00	4.7 演習	WPAの設定などの実装を行わせる実機演習とする。(※最大1グループ5名のグループ演習となります) ・WPA-PSKを設定し、コンシューマ向けのセキュリティ対策を実施	
	5.無線LAN実習			講義 + 演習
	12:00～12:30 13:30～14:30	5.1 設計要素	5.1.1 アクセスポイントを設置する上での考慮点 5.1.2 無線LAN規格の選定 5.1.3 電波干渉 5.1.4 アクセスポイントの負荷分散 5.1.5 無線LANのセキュリティ機能選定	
		5.2 無線LAN導入の注意事項	5.2.1 企業における無線LAN導入時のポイント 5.2.2 学校における無線LAN導入時のポイント 5.2.3 病院における無線LAN導入時のポイント	
	14:45～17:00 (途中休憩含む)	演習	机上設計演習(導入事例・設計要素を元に顧客条件に対して設計) 実機演習(構築事例に基づいて構築を行う) (※最大1グループ5名のグループ演習となります) ・ある企業の構築例に沿って既存のRadiusサーバの機材と連携するアクセスポイント、無線PCカードを設定する	
	6.確認テスト 17:00～17:30			机上テスト