

科目	カリキュラム		概要	研修スタイル
情報セキュリティ総括基礎				
	0.確認テスト 9:30～10:00			机上テスト
	1.情報セキュリティとインターネット概論			講義 + 演習
	10:00～11:00 11:15～11:40	1.1 情報セキュリティと情報セキュリティ対策	1.1.1 情報セキュリティとは 1.1.2 情報セキュリティ対策の必要性	
		1.2 情報資産をとりまく利便性とリスク		
		1.3 情報資産に対する脅威と脆弱性	1.3.1 脅威の分類 1.3.2 脆弱性の分類	
		1.4 インターネット概要	1.4.1 インターネットに潜む脆弱性 1.4.2 インターネットのサービス形態	
		1.5 TCP/IP通信	1.5.1 インターネットにおけるTCP/IP通信 1.5.2 主なTCP/IPプロトコル 1.5.3 TCP/IP通信におけるポートの役割 1.5.4 3Way Hand Shake	
		1.6 TCP/IPのアプリケーション	1.6.1 Webのしくみ 1.6.2 電子メールのしくみ 1.6.3 TCP/IP通信に関する留意点 参考A OSI参照モデルとTCP/IPプロトコル群 参考B ネットマスク 参考C 情報資産を脅かす攻撃者	
	11:40～12:00	1.7 演習	・机上演習(TCP/IP通信、一般的なセキュリティに関する演習) ・マシン演習(リモートデスクトップ)	
	2.セキュリティ侵害と攻撃			講義 + 演習
	12:00～12:30	2.1 情報セキュリティの動向	2.1.1 情報セキュリティに関連する主な法律 2.1.2 情報漏洩、サイバー犯罪の例	
		2.2 攻撃手順の例	2.2.1 情報収集 2.2.2 攻撃・侵入 2.2.3 後作業	
	13:30～14:30 14:45～15:10	2.3 代表的な攻撃	2.3.1 脆弱性(セキュリティホール)とは 2.3.2 サービス妨害 2.3.3 盗聴 2.3.4 パスワードクラック 2.3.5 バッファオーバーフロー	
		2.4 攻撃の動向	2.4.1 rootkit 2.4.2 ウィルス、ワーム、トロイの木馬 2.4.3 スパイウェア 2.4.4 ボット、ボットネット	
		2.5 Webアプリケーションに対する攻撃	2.5.1 検索エンジンハッキング 2.5.2 SQLインジェクション、コマンドインジェクション 2.5.3 クロスサイトスクリプティング	
		2.6 その他の攻撃	2.6.1 スпамメール 2.6.2 フィッシング、ファームング 2.6.3 Winny、Antinnyによる情報漏洩	
	15:10～15:45	2.7 演習	・実機演習(アドレス調査・ポートスキャン・バナー調査、ツールによるパスワード解析、暗号化されていないパスワードのキャプチャ)	
	3.情報セキュリティマネジメント			講義 + 演習
	16:00～17:30 (途中休憩含む)	3.1 情報セキュリティマネジメントの重要性	3.1.1 情報セキュリティ事件・事故 3.1.2 情報セキュリティマネジメントとは 3.1.3 リスク管理	
		3.2 ISMS(情報セキュリティマネジメントシステム)	3.2.1 ISMS適合性評価制度 3.2.2 ISMS認証基準 3.2.3 PDCAモデルによる情報セキュリティの確保	
		3.3 情報セキュリティポリシー導入と運用	3.3.1 情報セキュリティポリシーとは 3.3.2 情報セキュリティポリシー策定の流れ 3.3.3 情報セキュリティポリシーの運用 3.3.4 情報セキュリティ監査制度とISMS適合性評価制度 3.3.5 情報セキュリティ教育	
	9:40～9:55	3.4 個人情報保護	3.4.1 個人情報保護法の概要 3.4.2 プライバシーマーク制度 3.4.3 JIS Q 15001	
	9:55～10:15	3.5 演習	机上演習(仮想企業においてセキュリティポリシー運用上の問題点を分析し、改善策を考察・記述するような演習)	
	4.情報セキュリティ対策			講義 + 演習
	10:15～11:00 11:15～12:30	4.1 暗号化	4.1.1 暗号化の概要 4.1.2 公開鍵基盤(PKI) 4.1.3 デジタル署名 4.1.4 通信の暗号化 4.1.5 ディスクとファイルの暗号化 4.1.6 暗号化の導入の留意点	
		4.2 認証	4.2.1 認証技術 4.2.2 パスワードによる認証 4.2.3 強固なパスワードの設定	
		4.3 アクセス制御	4.3.1 OSにおけるアクセス制御 4.3.2 Webサイトにおけるアクセス制御	
		4.4 ファイアウォールと侵入検知	4.4.1 ファイアウォールとは 4.4.2 ファイアウォールの種類 4.4.3 侵入検知と侵入防御 4.4.4 ファイアウォールや侵入検知・防御システム導入時の考慮点	
	13:30～14:30 14:45～15:45	4.5 不正プログラム対策	4.5.1 ウィルス対策ソフトの導入 4.5.2 スパイウェア、rootkit、ボットネット対策 4.5.3 検疫システム	
		4.6 侵入・攻撃への対処・復旧・予防	4.6.1 侵入・攻撃の検知と対応 4.6.2 システムの復旧 4.6.3 ホストの要塞化	
		4.7 クライアントセキュリティ	4.7.1 修正プログラムの適用 4.7.2 ウィルス対策ソフトの導入 4.7.3 モバイルコードへの対応 4.7.4 パーソナルファイアウォール 4.7.5 コンピュータのロック 4.7.6 ネットワーク利用時の留意点 4.7.7 モバイル環境における留意点	
		4.8 Webアプリケーションのセキュリティ対策	4.8.1 セキュアプログラミング 4.8.2 Webアプリケーションファイアウォールの導入	
		4.9 セキュアなネットワークシステム	4.8.1 セキュアなネットワークシステムの構築 4.8.3 構築・運用時のチェックと確認	
	16:00～16:30	4.9 演習	実機演習(不正プログラム対策、ファイルの暗号化、アクセス権の設定・変更など)	
	5.セキュリティインシデント			机上テスト
	16:30～17:00	5.1 コンピュータセキュリティインシデント	5.1.1 コンピュータセキュリティインシデントとは 5.1.2 インシデントの種類 5.1.3 インシデントの例	
		5.2 インシデントレスポンス	5.2.1 事前の対応 5.2.2 インシデントの発見と対応 5.2.3 インシデントからの復旧 5.2.4 復旧後の対応	
		5.3 インシデントマネジメント	5.3.1 インシデントマネジメントの必要性	
	0.確認テスト 17:00～17:30			机上テスト