平成17年度　ネットワークセキュリティ担当者研修カリキュラム

日程	時間	項目	含まれるキーワード	実習内容	使用ソフト
1日目	9:30 12:30	IPsecによるVPN構築 ・IPsec概要 ・AH概要 ・ESP概要 ・IKE概要	IPsec、IP-VPN	IPsecによるVPN環境構築	Windows2000
	13:30 17:30	TCP/IPアプリケーションの弱点 ・TCPコネクションの問題点 ・DNS、SMTP、HTTP、FTP、Telnet、SNMP、ICMPの問題点	IPspoofing、SYNflood クロスサイトスクリプティング、Unicodeバグ、PASV FTP、Smurf攻撃	Windows、UNIXを利用した脆弱性の確認 Unicodeバグを利用したIISの改ざん	Windows2000、Linux
2日目	9:30 12:30	・無線LANの問題点 ・Windowsネットワークの問題点	WEP		
	13:30 17:30	ハッキング技術 ・情報収集 ・権限取得（パスワード推測、バッファオーバフロー 等） ・不正実行（TCP/IPアプリケーションの弱点に含む） ・事後処理（トロイの木馬、ファイルの隠蔽 等　ログ消去はログ分析に含む）		 バッファオーバフロー SUトロイ、ファイルの隠蔽 等	
3日目	9:30 12:30	ログ分析 ・不正アクセスの兆候 ・複数システム間での時刻同期 ・Windows/Unixのログ ・Webサーバのログ	不正検知　発見, 分析, フットプリン	ログ設定、発生するログ内容等の確認	Windows2000、Linux
	13:30 16:00	・ルータ、ファイアウォールのログ セキュリティ診断、監視 ・セキュリティ診断ツールの利用 ・IDSによる不正侵入の監視 ・侵入発見後の処理の流れ（不正アクセスを受けた場合のとりくみ）	対処　インシデントレスポンス, 原因調査など		 Nessus Snort