22s. ネットワーク管理者のための
ネットワークセキュリティ（New）

1. 研修要領

・募集定員	16名
・研修会場	NISA研修室（確定）
・講　　師	福岡ソフトウェアセンター（FSC)講師：山田 篤彦 氏
・開催月日（希望日を記入）	H29年 12月 06・07・08日（水)・(木)・(金)
・実施時間・日数	9:30 ～ 17:30（7時間/日）・3日間（21時間）
・受 講 料（税別）	78,800円
・教 材 料（税別）	5,000円

2. 対象者

ネットワーク運用管理者の方、ネットワーク設計者の方

3. カリキュラムの概要

企業のネットワークシステムにとって脅威となる、**不正アクセス攻撃、情報漏えい、コンピュータウィルス被害**など、その技**術的な手法や動作などを理解し対策する方法**について学習します。
FWの実機を使用して、FW、メールサーバ、Webサーバ、DNSサーバのセキュリティ対策および**ネットワーク監視**について知識を深め、演習を通してセキュリティ設計知識を身につけます。

4. カリキュラムの詳細　　3日間（21時間）

※改善のためカリキュラムは予告なく変更させていただくことがあります。

科目	時間	科目の内容
1.最新セキュリティ事情	2.0h	1.セキュリティとは 2.最新セキュリティ事情
2.不正アクセス攻撃	2.0h	1.プロファイリング（ポートスキャン、バナー） 2.侵入（ウィルス、バッファオーバーフロー） 3.DoS 4.標的型サイバー攻撃
3.ネットワーク基礎知識と確認ツール	3.0h	1.OSI参照モデル 2.Ethernet、IP、ARP、ICMP、TCP/UDP 3.HTTP、SMTP、POP、DNS 4.ipconfig、netstat、ping、nslookup、tracert、arp、telnet
4.ファイアウォール	3.0h	1.ルール設計 2.ルール設定演習【実機　NetScreen 204】

5.ネットワーク監視	2.0h	1.SNMP ・MIB 2.ログ 3.SNMPによる監視【実機】
6.暗号技術／ 認証技術基礎知識	3.0h	1.暗号方式 （共通鍵暗号、公開鍵暗号、ハイブリッド暗号） 2.利用者認証 （パスワード認証、公開鍵認証、 ワンタイムパスワード認証、生体認証） 3.デジタル署名 4.第三者認証
7.Webサーバの セキュリティ	3.0h	1.バージョン情報取得 2.ファイル一覧表示 3.プログラムの実行 4.セッションハイジャック 5.フィッシング詐欺／ファーミング詐欺 6.SSL技術 7.セキュリティ対策【実機】
8.メールサーバの セキュリティ	2.0h	1.第三者中継問題 2.アカウントのなりすまし 3.パスワードの漏えい 4.メールの盗聴 5.OP25B 6.SSL技術応用 7.S/MIME 8.SPF 9.DKIM 10.セキュリティ対策【実機】
9.DNSサーバの セキュリティ	1.0h	1.バージョン情報取得 2.DNSスプーフィング／キャッシュポイゾニング 3.DNSSEC 4.TSIG
計	21.0Hr	

５．使用教材

オリジナルテキスト、ファイアフォール（4～5名につき一台）

PC１人１台

６．到達目標

本コース修了後、次の事項ができることを目標としています。

・不正アクセス攻撃、情報漏えいの仕組み／原因について理解する。
・各種ネットワーク機器やサーバによるセキュリティ対策を実施できる。
・ネットワーク機器の監視技術の知識を身につける。
・ネットワークのセキュリティ設計技術を身につける。