06s ルータを中心に学ぶネットワーク基礎とセキュリティ ～最新動向と対策の基本～

1. 研修要領

・募集定員	16名
・研修会場	出島交流会館(住所:〒850-0862 長崎市出島町2-11)
・講　師	福岡ソフトウェアセンター(FSC)講師:山田 篤彦
・開催月日	2023年8月23日(水)・24日(木)・25(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

入社2、3年目までのエンジニアで、システム構築においてシステム全体的な提案・営業活動等に携わる方

3. カリキュラムの概要

ネットワーク技術者が知っているべきネットワーク基礎知識とセキュリティ基礎知識を実機を使いながら学習します。
IP／TCP／UDPなどネットワーク基礎知識、暗号技術／認証技術に関する基本から認証局までネットワークを利用する上で押さえておかなければならない基礎知識を演習を通して身につけます。演習ではネットワークシュミレータ(GNS3)を使用して基本を理解し、ルータ実機(YAMAHA)を使用してネットワーク構築とトラブルシューティングを経験しながら実践に役立つスキルを習得します。

4. カリキュラムの詳細　　3日間(21時間)

	科目	時間	科目の内容
8月23日	1. ネットワークとは	1.5h	・OSI参照モデル P.3 ・Webの通信からネットワークを解剖する P4～5 ・TCP/IPって何？ P4～P5 ・WireSharkでパケット解析、ネットワークの流れを調査する 【講義・演習】
	2. セキュリティとは	2.0h	・最新セキュリティ事情 P8～P12 ・ポートスキャン(nmapとWireSharkでパケット解析) P.13 演習 ・DoS攻撃／DDoS攻撃 P.14 ・バッファオーバーフロー攻撃 P.15 ・中間者攻撃 P.85～P86 P34～P35 ・標的型サイバー攻撃 P.16 【講義・演習】
	3. ネットワーク層プロトコルとセキュリティ	3.5h	・IP(Internet Protocol)… IPアドレスとサブネットマスク、TTL、ネットワークアドレスとブロードキャストアドレス、デフォルトゲートウェイ P17 ・ipconfigコマンドで情報確認 P25～演習 ・IPアドレスとサブネットマスク P17～P19 ・ルーティングと経路情報テーブルとrouteコマンド P48～49 ・ネットワークシュミレータでルーティング ・プライベートIPアドレス、アドレス変換技術(NAT、IPマスカレード) P50～51 ・ICMP(Internet Control Message Protocol) pingコマンドのパケット解析 P30.31 tracertコマンとのパケット解析 P32 ネットワークトラブルのパケット解析(宛先到達不能、ルーティングループ) P30.演習 ・ICMP経路変更通知による中間者攻撃とは P32 【講義・演習】

	科目	時間	科目の内容
8月24日	4. ネットワーク構築演習	3.0h	実機ルータを使った課題演習とトラブルシューティング 【演習】
	5. ネットワーク層プロトコル2	0.5h	・ARP(Address Resolution Protocol) … ARPとarpキャッシュ 【講義】 p33
	6. データリンク層プロトコルとセキュリティ	1.5h	・Ethernet …MACアドレス p36 ・ARPの動作をWireSharkでキャプチャ ;演習 p33 ・スイッチングハブ … MACアドレステーブル、フラッディング、ブロードキャストストーム ・arpスプーフィングによる中間者攻撃とは p34~35 ・VLANとは p40 ・ネットワークシュミレータでVLAN 【講義・演習】
	7. トランスポート層プロトコル	1.5h	・TCP(Transmission Control Protocol)ポート番号、フラグ、TCPの状態遷移、シーケンス番号、ACK番号、ウィンドウサイズ p38~42 ・TCPの状態遷移のパケット解析とnetstatコマンド p41 ;演習 ・UDP(User Datagram Protocol)、TCPの動作 ;演習 【講義・演習】 p43
	8. 暗号技術基礎	0.5h	・共通鍵暗号方式と公開鍵暗号方式 p52~p54 ・ハイブリッド暗号方式 p55 【講義】
8月25日	9. 認証技術基礎	2.0h	・パスワード認証(チャレンジ&レスポンス認証) p56~57 ・公開鍵認証 p58 ・ワンタイムパスワード認証 p59 ・バイオメトリクス認証 p59 ・二要素認証と二段階認証 p59 ・デジタル署名 p60 ・第三者認証(認証局とPKI) p61~64 ・TLS/SSL 【講義】 p65
	10. アプリケーション層プロトコルとセキュリティ	p.74 5.0h p83 ← p78-81 p84 p85	・DNS(Domain Name System) p66~67 リゾルバ、hostsファイル、nslookupコマンド、リゾルバキャッシュ ・DNSキャッシュ汚染攻撃とDNSSEC p66 ・HTTP(Hyper Text Transfer Protocol)…, ﾒｿｯﾄﾞ、ｽﾃｰﾀｽｺｰﾄﾞ、HTTPヘッダ、curlコマンド p67~p71 ・XSS攻撃、CSRF攻撃、Web通信の盗聴、Webサーバーのなりすまし ・SMTP(Simple Mail Transfer Protocol)…MUA、MTA、SMTPコマンド、応答コード p77 ・POP3(Post Office Protocol version 3) p82 ・メールの盗聴対策(SMTPS、POP3S、STARTTLS、S/MIMEとPGP) ・SPAMメールと対策(第三者中継とRBL,、OP25B、SMTP_AUTH、送信ドメイン認証) ・DHCP(Dynamic Host Configuration Protocol) ・DHCPスプーフィングによる中間者攻撃と偽サイトへの誘導 【講義】
	計	21.0Hr	

※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。

5. 使用教材

オリジナルテキスト

6. 到達目標

①ネットワークの基本的知識を習得しネットワークの設計ができるようになる
②ネットワーク利用者のセキュリティリスクを認識する
③ネットワークトラブルの原因を解析できるようになる
④セキュリティを保つための技術を習得し、行動と心構えを身につける

7. ITSSレベル

4