

18j. ネットワークトラブルの原因分析技術 ～パケットキャプチャリングとトラフィック解析～

1. 研修要領

・募集定員	16名
・研修会場	NISA研修室(確定)
・講師	富士通九州システムズ(FJQS)講師:太田 伸一郎氏
・開催月日	平成28年10月19日(水)～21日(金)《3日間》
・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

ネットワーク技術者で高度のセキュリティ対策を担当している方。

3. カリキュラムの概要

TCP/IPプロトコルのヘッダフォーマットについて学習し、Wireshark(キャプチャツール)を利用したパケットキャプチャリング技術を習得し、キャプチャリングした情報を解析し各プロトコルのシーケンスを学習します。またネットワークトラブルにおける原因調査をWiresharkでパケットキャプチャリングした情報を解析して行います。また、総合演習では実務を想定したネットワークトラブルを実際に発生させ、パケットキャプチャリング技術を用いたトラブルの原因分析を実際に行います。こうすることで、実践的なネットワークトラブルの対応が可能となります。

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
1. TCP/IPの概要	1.5 Hr	<ul style="list-style-type: none"> ・TCP/IPの起源 ・RFC ・TCP/IPプロトコルに関連する組織 ・TCP/IPプロトコル体系
2. IP	5.5 Hr	<ul style="list-style-type: none"> ・IPの概要 ・IPヘッダフォーマット ・IPアドレス ・Fragmentation/Reassembly ・アドレス解決(ARP) ・ProxyARP ・Wiresharkの使い方 ・【実習1】パケットキャプチャによるIPヘッダフォーマットの確認
3. ICMP	2.0 Hr	<ul style="list-style-type: none"> ・ICMPの動作原理 ・メッセージ種別 ・【実習2】パケットキャプチャによるICMPのメッセージ確認
4. TCP	3.5 Hr	<ul style="list-style-type: none"> ・TCPの概要 ・パケットフォーマット ・ポート番号 ・フローシーケンス ・PSHフラグとURGフラグ ・TCPオプション ・Silly Window Syndrome ・【実習3】パケットキャプチャによるTCPシーケンス確認
5. UDP	3.5 Hr	<ul style="list-style-type: none"> ・UDPの概要 ・パケットフォーマット ・【実習4】パケットキャプチャによるUDPフォーマットの確認 ・【実習5】パケットキャプチャによる上位プロトコル解析(HTTP/HTTPS/SMTP/DNS)

6. ネットワークトラブル分析 総合演習	5.0 Hr	・務を想定したネットワークトラブルを実際に発生させ、パケットキャプチャリング技術とトラフィック解決技術を用いたネットワークトラブルの原因分析を実際に行います。
計	21.0 Hr	

5. 使用教材

インターネットプロトコル解説(富士通ラーニングメディア)
FJQS補足資料
FJQS総合演習

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。

1. TCP/IPの動作を説明することができる。
2. IP、TCP、UDPのヘッダフォーマットについて説明することができる。
3. TCPやICMPなどのプロトコル情報からネットワークの問題点を説明することができる。
4. Wireshark(キャプチャツール)を使用したパケット分析を行うことができる。
5. Wireshark(キャプチャツール)を使用し、ネットワークトラブルの原因究明を行うことができる。
6. 実務を想定した環境でトラブルが発生したときに、キャプチャリング技術、トラフィック解析技術を使用してネットワークトラブル分析、対応ができる。

7. レベル

ITSS:ITスペシャリスト育成 - [*]要素技術【レベル: 2】
ITSS:ITサービスマネジメント育成 - [*]セキュリティ管理基礎【レベル: 2】
ITSS:ソフトウェア開発育成 - [*]要素技術基礎【レベル: 2】

[*] ITスキル標準研修ロードマップにおけるコース群名