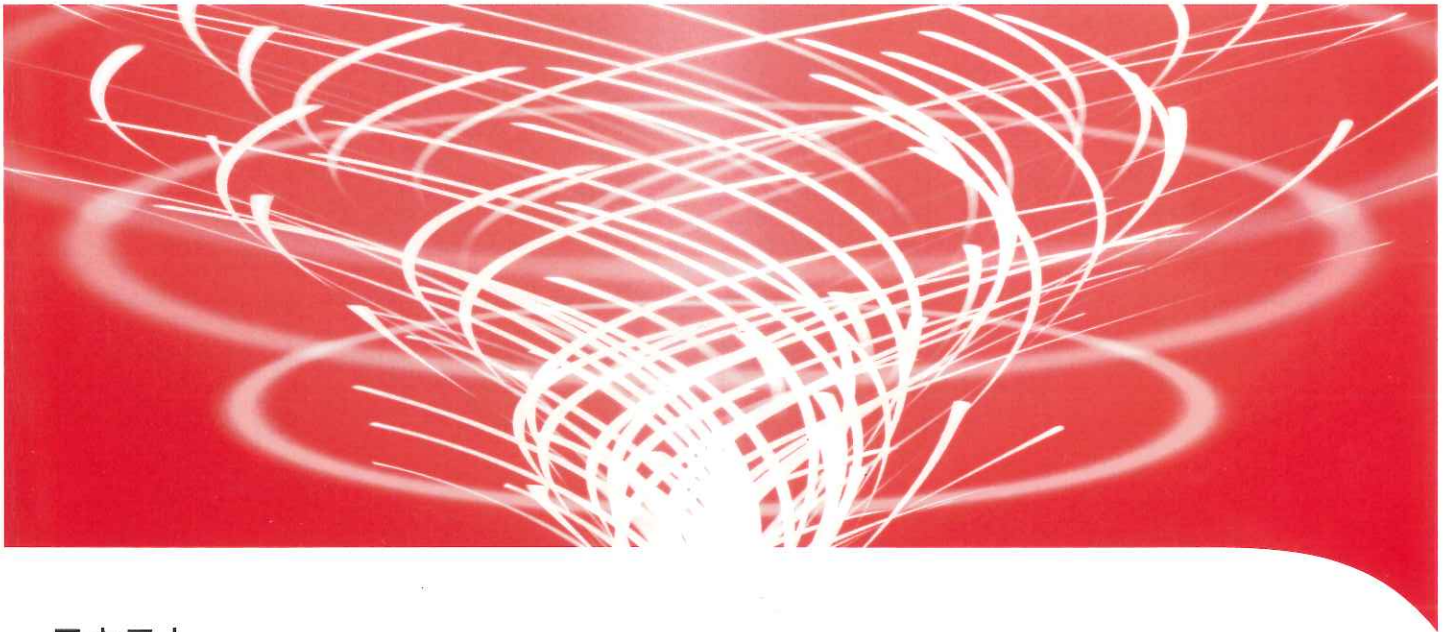


FUJITSU 人材育成・研修サービス
ネットワークの基礎ステップアップ運用編
～ 通信解析&ログ監視 ～



テキスト

UJE84L1N-03

目次

第1章 ネットワークの運用管理	
1.1 ICTシステムにおける運用管理の役割	15
1.2 ネットワークにおける運用管理	16
<演習1> ネットワークのトラブルについて考える	17
1.3 ネットワークの運用管理～正常時～	18
1.3.1 主な4項目	18
1.3.2 構成管理	19
<参考> 物理構成図	20
<参考> 論理構成図	21
<参考> アドレス一覧表	22
<参考> 装置一覧表	23
<参考> パラメーターシート	24
<参考> 構成定義	25
1.3.3 性能管理	26
<参考> 性能監視で確認する項目	27
1.3.4 障害管理	28
<参考> コンティンジェンシープラン	29
<参考> 障害管理表(例:障害報告書、障害一覧表)	30
1.3.5 セキュリティ管理	31
1.4 ネットワークの運用管理～異常時～	32
1.4.1 トラブル発生時の影響	32
1.4.2 トラブル発生時の対応	33
1.5 ネットワークの運用管理手法	34
第2章 通信解析	
2.1 ネットワークの通信解析の役割と目的	39
2.2 通信解析の進め方	40
2.3 パケットキャプチャー	41
2.3.1 パケットキャプチャーのツール	41
2.3.2 パケットキャプチャーの方法	42
2.4 Wireshark	43
2.4.1 Wiresharkの概要	43
2.4.2 Wiresharkの基本操作～キャプチャーの開始～	44
2.4.3 Wiresharkの基本操作～ディスプレイの読み方～	45

2.4.4	Wireshark の基本操作～アイコンと機能～	46	<実習 2>	ARP の通信を確認する	85
2.4.5	Wireshark の基本操作～キャプチャーのオプション設定～	47	3.7	IP アドレスを使用した通信の状態確認	86
2.4.6	Wireshark の基本操作～キャプチャーフィルターの適用～	48	3.7.1	ICMP プロトコル	86
2.4.7	Wireshark の基本操作～キャプチャーフィルターの作成・管理～	49	3.7.2	ping の通信	87
2.4.8	Wireshark の基本操作～表示フィルターの直接定義～	50	3.7.3	ICMP Echo Request/Echo Reply メッセージ	88
2.4.9	Wireshark の基本操作～パケットから表示フィルターを作成～	51	3.7.4	ICMP Destination Unreachable メッセージ	89
2.4.10	Wireshark の基本操作～キャプチャーデータの保存～	52	3.7.5	Time Exceeded メッセージ	90
			<参考>	Traceroute	91
			<実習 3>	ICMP の通信を確認する	92
第 3 章	TCP/IP 通信とパケット		3.8	IP アドレス自動設定のための通信	93
3.1	TCP/IP 通信の概要	57	3.8.1	DHCP の通信	93
<参考>	OSI 参照モデル	58	3.8.2	DHCP メッセージ	94
<参考>	OSI 参照モデルの各層の役割	59	<実習 4>	DHCP の通信を確認する	96
3.2	パケットとヘッダー	60	3.9	トランスポート層の通信制御	97
3.3	ネットワークインターフェイス層の通信制御	61	3.9.1	TCP/UDP の通信	97
3.3.1	Ethernet の通信	61	3.9.2	ポート番号	98
3.3.2	MAC アドレス	62	3.9.3	TCP ヘッダー	99
3.3.3	Ethernet ヘッダー	63	3.9.4	TCP の機能	100
3.3.4	スイッチング	64	3.9.5	コネクション制御	101
<参考>	MAC アドレステーブル	65	<参考>	TCP 通信の状態遷移	102
3.4	インターネット層の通信制御	66	<参考>	コネクションのリセット	103
3.4.1	IP の通信	66	3.9.6	確認応答	104
3.4.2	IP アドレス	67	<参考>	ACK の通知	105
<参考>	サブネットマスク	68	3.9.7	UDP ヘッダー	106
3.4.3	ブロードキャストアドレス	69	3.10	ファイル転送の通信～FTP と TFTP～	107
3.4.4	IPv4 ヘッダー	70	3.10.1	ファイル転送通信の仕組み	107
<実習 1>	Ethernet と IP のヘッダーを確認する	72	3.10.2	FTP の通信	108
<参考>	IPv6 アドレス	73	3.10.3	TFTP の通信	109
<参考>	IPv6 標準ヘッダー	74	3.10.4	FTP メッセージ	110
3.4.5	ルーティング	75	<参考>	FTP メッセージコード①	112
<参考>	ルーティングテーブル	76	<参考>	FTP メッセージコード②	113
<参考>	経路制御装置の種類と違い	77	<実習 5>	FTP の通信を確認する	114
3.4.6	IP で行う通信制御	78	3.11	FQDN と IP アドレス～DNS～	116
3.4.7	フィルタリング	79	3.11.1	DNS の仕組み	116
3.4.8	アドレス変換	80	3.11.2	DNS の通信	118
3.5	アドレスの解決	81	3.11.3	DNS メッセージ	119
3.6	IP アドレスと MAC アドレス～ARP～	82	3.11.4	Question section	121
3.6.1	ARP の仕組み	82	3.11.5	Answer section	122
3.6.2	ARP のやりとり	83	<実習 6>	DNS の通信を確認する	124
3.6.3	ARP メッセージ	84	3.12	FQDN を使用した通信	125
			3.12.1	WWW の通信	125

3.12.2 HTTP の通信	126
3.12.3 HTTP パケット~リクエストメッセージ~	127
3.12.4 HTTP パケット~レスポンスメッセージ~	128
<参考> HTTP/1.1 の主なメソッド.....	129
<参考> HTTP/1.1 のステータスコード.....	130
<参考> Cookie(クッキー)	131
3.12.5 HTTPSの通信	132
<参考> SSLとTLS.....	133
<実習 7> HTTP/HTTPS の通信を確認する	134
<参考> ブラウザーを利用したメールやファイルの閲覧	135
3.13 遠隔操作の通信	136
3.13.1 遠隔操作通信の仕組み	136
3.13.2 Telnetの通信	137
3.13.3 SSHの通信	138
3.13.4 Telnet メッセージ.....	139
<参考> Telnet のネゴシエート.....	140
<実習 8> Telnet/SSH の通信を確認する	141
<参考> Telnet での接続方法.....	142
<参考> SSH での接続方法	143
第4章 ログ監視	147
4.1 ログ監視の目的と役割	147
<参考> ログの種類	148
4.2 ログ監視の手順.....	149
<参考> SNMP による機器の監視	150
4.3 ログ取得の方法.....	151
<参考> Syslog と Syslog メッセージ.....	152
<参考> Facility と Severity.....	153
<演習 2> Syslog を読んでみよう	154
総合実習	157
<総合実習> Web アクセスを行い、通信の流れを確認する	157