パケットモニター(Wireshark)の使い方

<u>1. Wireshark とは</u>

ネットワーク上(LAN ケーブルに流れている)のパケットを取得して、その中の情報を画面に表示するソフトウェア(LAN アナライザーまたはパケットモニター)の1つに Wireshark がある。Wireshark は、非常に高機能なオープンソース(ソース コードが公開されている)の LAN アナライザで、誰でも自由にコンピュータにインストールして利用することができる。(公 式サイト http://www.wireshark.org)

<主な利用目的>

- ネットワーク管理者がネットワークのトラブルを解決するため
- セキュリティ技術者がセキュリティの問題を解決するため
- 開発技術者がプロトコルの実装についてデバッグ(誤り確認)するため
- ネットワークプロトコルの内部について学習するため

<主な機能>

- ネットワークインタフェースから送出されるパケットをキャプチャ(取得する)する
- パケットの内容を詳細表示する
- パケットキャプチャしたデータを開いたり保存したりできる。
- 他の LAN アナライザが取得したキャプチャデータを変換して読み込み、書き出しができる
- さまざまな条件でパケットを絞り込んで検索できる
- 特定のパケットのみ色づけできる
- さまざまな統計情報を作成できる

<u>2. ユーザインタフェース</u>

Wireshark は、パケットをキャプチャするための様々なメニューやツールバーで構成されている。また、右クリックで呼び 出したサブメニューで、オプションなどを指定することができる。ここでは、キャプチャしたパケットを解析するために必要 な Wireshark の画面構成などについて述べる。



<画面構成と各部の名称>

[メインメニュー]

Wireshark の様々な機能を呼び出すために使用され、以下の項目がある。

項目名	主 な 機 能	
File	ファイルの開閉・保存・結合・印刷など	
Edit	パケット検索・強調表示	
View	ツールバーや画面表示、パケットの色分け	
Go	特定パケットの表示	
Capture	キャプチャの開始・終了、キャプチャフィルタ(キャプチャ時の絞り込み)の編集	
Analyze	Analyze 表示フィルタ(絞り込み表示)の作成・編集、パケット解析	
Statistics	itistics パケット数の一覧やプロトコル分布などの統計情報の表示	
Help	ヘルプ機能	

ペーンアーエー ひねって 工体能	メイ	インメニ	<u>л—</u> с)項目	と主	巻 能
------------------	----	------	-------------	-----	----	------------

[ツールバー]

よく使う機能をボタン化してある

[フィルタツールバー]

パケットを絞り込む(フィルタ機能)ときに使用する

[パケット一覧部]

キャプチャしたパケットを一覧にして表示する。1つのパケットを1行で表示し、簡単な説明(info)がつけられる。ここで クリックして選択した1つのパケットの詳細な内容が、[パケット詳細部]に表示される。

項目名	内容
No.	キャプチャした順番を示す番号
Time	キャプチャした時刻
Source	送信元アドレス
Destination	宛先アドレス
Protocol	プロトコルの名称
info	パケットの概要

パケット一覧部・表示内容

[パケット詳細部]

[パケットー覧部]で選択したパケットの詳細内容(解析内容)を表示する。また、ヘッダやレイヤに付けられている+ 印をクリックすると、詳細な解析内容が表示される。

[パケットデータ部]

[パケットー覧部]で選択したパケットの内容を、16 進数や ASCII コードなどで表示する。より細かく解析する時に利用 する。

[ステータスバー]

現在のプログラムの状態やパケットキャプチャに関する情報が表示される。通常、左側には現在のWiresharkの状態 及びキャプチャファイルや選択したフィールドの内容が、右側には現在選択しているパケットの番号が表示されてい る。

キャプチャ画面

3. キャプチャ操作とパケット表示

ここでは、web サーバー(PC1)からサンプルホームページをダウンロードするときにやり取りされるパケットを例に取って、 キャプチャの操作手順とパケットの表示と確認方法を説明する。

くキャプチャ操作手順>

① デスクトップの下に示すアイコンをダブルクリックして Wireshark を起動する。



Wireshark Wiresharkのアイコン

- ② ツールバーの[interfaces]ボタン(一番左にあるボタン)を押して、キャプチャインタフェース画面を表示させる。
- ③ 使用している通信アダプタ(LAN カード)を選択して[Start]ボタンを押す。この時点でキャプチャが開始されるので、何 らかのパケットが表示される

Description	IP	Packets	Packets/s		Stop	
. Intel(R) PRO/1000 PL Networ	k Connection 192.168.0.3	15	0	Start	ptions	Details
. Microsoft	0.0.0.0	0	0	Start	Options	Details
. MS Tunnel Interface Driver	unknown	0	0	Start	Options	Details

 ④ ブラウザを起動させ、web サーバー(PC1)のアドレスを指定して、ホームページを表示させる。ホームページのダウン ロードが終了したら、ツールバーの[Stop]ボタン(左から4番目のボタン)を押す。

<パケットの表示>

キャプチャ終了直後は、目的以外のパケットが表示されているので、表示フィルタを使って絞り込みを行う。今回は、 http プロトコルのみを表示するために、以下の通りにフィルタツールバーのボックスに http を入力する。

Filter: http Expression... Clear Apply

```
フィルタ入力画面
```

http を入力し終わるとボックスが緑色に変わるので、Enter キーを押すとパケット一覧部に、以下のように http プロトコルのみが表示される。

<パケット(各ヘッダ)の確認>

ここでは、表示されたパケットヘッダの構成を確認する方法について、1つのパケットを例に挙げて説明する。

The second secon	
Energine procession and an and a second and	
SUZAT Channel Wineless Setun	gs Decryption Reys
No., Time Source Destination Protocol Info 4 0.000398 192.168.1.1 192.168.1.6 HTTP GET / HTTP/1.1	n
7 0.129562 192.168.1.6 192.168.1.1 HTTP HTTP/1.1 200 Document follows 8 0.193130 192.168.1.1 192.168.1.6 HTTP GET /favicon.ico HTTP/1.1	(text/html)
11 0.330772 192.168.1.6 192.168.1.1 HTTP HTTP/1.1 404 Not Found (text/	html)
	▶ フィルタ結果
フィル友結甲で書くまテキれたパケットの内部	
ノイルグ和木で自て衣小されたパンプリンパー	(http パケット)
⊕ Frame 4 (258 bytes on wire, 258 bytes captured) ⊕ Ethernet II, Src: Intel_25:4f:b3 (00:19:d1:25:4f:b3), Dst: Intel_56:83:7b (00:19:d1:56:83:7b)	
∃ Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.6 (192.168.1.6) Transmission Control Protocol, Src Port: termant (2027), Dst Port: http://doi.org/10.1000/000000000000000000000000000000	14
B Hypertext Transfer Protocol	
0010 00 f4 ab da 40 00 80 06 ca d1 c0 a8 01 01 c0 a8	
0030 ff ff f6 21 00 00 47 45 54 20 2F 20 48 54 54 50GE T / HTTP 0040 2F 31 2e 31 0d 0a 41 63 63 65 70 74 3a 20 2a 2F /1.1Ac cept: */	E
0050 2a 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 *Accep t-Langua 0060 67 65 3a 20 6a 61 0d 0a 55 41 2d 43 50 55 3a 20 ge: jaUA-CPU:	
00/0 /8 38 30 00 0a 41 63 63 65 /0 /4 20 45 66 65 66 6c ding; gg ip, defl	
00a0 20 4d 6f 7a 69 6c 6c 61 2f 34 2e 30 20 28 63 6f Mozilla /4.0 (co	T
File: F:#shonan#インダーネットフロト Packets: 15 Displayed: 4 Marked: 0	Pronie: Default

2019.5 第1版

表示されているパケットで[info]の列で GET /http/1.1 と表示されているパケットを選び、パケット詳細部の表示内容を確認する。

⊕ Frame 4 (258 bytes on wire, 258 bytes capture	ed)	🗩 Ethernet II ヘッ
Ethernet II, Src: Intel_25:4f:b3 (00:19:d1:25	5:4f:b3), Dst: Intel_56:83:7b (00:19:d1:56:83:7b)	IP へぃゟ
Internet Protocol, SrC: 192.108.1.1 (192.108.	nagt (2077), Dst Port: http (80), Seq: 1, Ack: 1, Len	: 204
Hypertext Transfer Protocol	K	
http ヘッダ	パケット内部 TCP /	ヽッダ

上図(パケット内部)の[Ethernet II][Internet Protocol][Transmission Control Protocol][Hypertext Transfer Protocol]は、 パケットの<u>ヘッダ</u>と呼ぶ部分で複数の要素から構成されており、重要な役割を果たしている。また、最上部の[Frame]は、 フレーム情報(プロトコルの構成やサイズなど)を表している。

* Ethernet II ヘッダ(※行頭のプラス印+をクリックするとヘッダ情報が表示する)

3	Ethernet II, Src: Intel_25:4f:b3 (00:19:d1:25:4f:b	<pre>>3), Dst: Intel_56:83:7b (00:19:d1:56:83:7b)</pre>
1]
		▲ ヘッダ情報
	Type: IP (0x0800)	

<u>Ethernet II ヘッダ情報</u>

EthernetIIヘッダの主要素と内容

Destination	宛先 LAN カードの MAC アドレス
Source	送信元 LAN カードの MAC アドレス
Туре	上位プロトコルタイプ(ヘッダ形式)

* IP ヘッダ(※行頭のプラス印+をクリックするとヘッダ情報が表示する)

<pre>Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.6 (1 Version: 4</pre>	192.168.1.6)
Header length: 20 bytes	
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00) Total Length: 244	
Identification: Oxabda (43994)	
Image: Ox04 (Don't Fragment)	
Fragment offset: 0	▲ ヘッダ情報
Time to live: 128	
Protocol: TCP (0x06)	
Header checksum: 0xcad1 [correct]	
Source: 192.168.1.1 (192.168.1.1)	
Destination: 192.168.1.6 (192.168.1.6))

<u>IP ヘッダ情報</u>

IP ヘッダの主要素と内容

Vertion	バージョン(通常は 4)
Header length	ヘッダサイズ(通常は 20 パイト)
Differentiated Service Field	パケット優先度(プロトコル優先度)
Total Length	IP パケットサイズ(単位:バイト)
Identification	パケット識別情報
Flags	パケット分割識別子
Fragment offset	パケット分割位置
Time to live	パケットの寿命
Protocol	上位プロトコルタイプ
Header checksum	パケット破損確認情報
Source	送信元 IP アドレス
Destination	宛先 IP アドレス

* TCP ヘッダ(※行頭のプラス印十をクリックするとヘッダ情報が表示する)

Transmission Control Protocol	, Src Port: tsrmagt	(2077), Dst	Port: http	(80), Seq:	1, Ack:	1, Len:	204
Source port: tsrmagt (2077) Destination port: http (80) Sequence number: 1 (rela [Next sequence number: 205 Acknowledgement number: 1 Header length: 20 bytes Flags: 0x18 (PSH, ACK) Window size: 65535 Checksum: 0xf621 [correct]	tive sequence number (relative sequen (relative ack num)	r) ce number)] ber)	- ^	ッダ情報			

<u>TCP ヘッダ情報</u>

Source port	送信元ポート番号
Destination port	宛先ポート番号
Sequence number	順序番号(パケットの順番)
Acknowledgement number	応答確認番号(受け取ったパケットの順番)
Header length	ヘッダサイズ(通常 20 バイト)
Flages	TCP 通信制御のための識別子
Windows size	受信バッファサイズ(単位:バイト)
Checksum	パケット破損確認情報

TCP ヘッダの主要素と内容

* http ヘッダ(※行頭のプラス印+をクリックするとヘッダ情報が表示する)



<u>httpヘッダ情報</u>

TCP ヘッダの主要素と内容

GET	要求メソッド(Web ページ取得)
Accept	Web ブラウザの書式
Accept-Language	Web ブラウザの利用言語
UA-CPU	使用 CPU(コード形式)
Accept-Encoding	Web ブラウザのデータ形式
User-Agent	Web ブラウザの種類やバージョン
Host	Web サーバーの情報(IP アドレス)
Connection	Web サーバーの接続情報