

# パターンフィルタの設定方法

Synesis Ver. 3.x

# パターンフィルタ

- /// パターンフィルタはパケット中のフラグや文字列などSynesisのフィルタ項目にない特定のパターンをフィルタリングします。
- /// パターンフィルタは、“キャプチャフィルタ(\*1)” または“保存フィルタ”より作成できます。

\*1)キャプチャフィルタでは全てのパケットのキャプチャを実現させるため複数のフィルタを組み合わせて(and/or)使用することはできません。

# 例. HTTPのGETメソッドがあるパケットフィルタの作成

## フィルタの作成手順

1. HTTPのGETパケットを含むトレースファイルを開く。
2. トレースファイルのサマリ画面より、“GET”を含むパケットを選択。
3. 詳細画面から “Request Method:GET” の行を選択。
4. 詳細画面で選択した箇所がHEX画面上で赤く表示されるので、その値をメモしておく
5. パターンフィルタ作成
  - キャプチャフィルタの画面遷移  
[エージェント] > [Default Agent] > [概要] > [オプション] > [キャプチャフィルタ]
  - 保存フィルタの画面遷移  
[構成] > [保存フィルタ]

# 必要情報の確認方法

[サマリ]

No.	時間	Delta Time	ソース	送信先	プロトコル	長さ	サマリー
286	14:11:48.002092	0.000001	192.168.43.212	192.168.1.4	TCP	64	58941->80 [ACK] Seq=1 Ack=1 Win=32768 Len=0
287	14:11:48.002093	0.000001	192.168.43.131	192.168.1.9	HTTP	129	GET /index.html HTTP/1.1
288	14:11:48.002094	0.000001	192.168.43.212	192.168.1.4	HTTP	129	GET /index.html HTTP/1.1
289	14:11:48.002106	0.000012	192.168.1.1	192.168.43.5	TCP	1,518	[TCP segment of a reassembled PDU]

[詳細]

```

▼ GET /index.html HTTP/1.1\r\n
  ▼ Expert Info (Chat/Sequence): GET /index.html HTTP/1.1\r\n
    GET /index.html HTTP/1.1\r\n
    Severity level: Chat
    Group: Sequence
    Request Method: GET
    Request URI: /index.html
    
```

[HEX]

0000	00 15 17 A1 BA E4 00 15 17 A1 BA E3 08 00 45 00
0010	00 6F D0 A8 00 00 80 06 BC 03 C0 A8 2B 83 C0 A8
0020	01 09 F5 45 00 50 36 7E F4 3E 36 7E F4 92 50 18
0030	80 00 17 76 00 00 <b>47 45 54</b> 20 2F 69 6E 64 65 78
0040	2E 68 74 6D 6C 20 48 54 54 50 2F 31 2E 31 0D 0A
0050	48 6F 73 74 3A 20 31 39 32 2E 31 36 38 2E 31 2E
0060	39 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 4B
0070	65 65 70 2D 41 6C 69 76 65 0D 0A 0D 0A 8A 8E E2

オフセット分

## ・オフセット/マスク/パターン設定

GETメソッドの例

オフセット: 0x0036

マスク : FF FF FF

パターン : 47 45 54

オフセット: フレームの先頭からパターンが始まる一[byte]を設定

マスク : 文字列のパターンマスクを設定

パターン : フィルタする文字列のパターンを設定

# パターンフィルタ設定画面

● パターン

開始位置

オフセットタイプ  固定

オフセット   16進数  10進数  
(例: 16進数 0x6000 または 10進数 10000)

パターン形式

マスク

パターン

項目	説明
開始場所	パケット中でパターンの一致を判定する場所を指定します。下記の中から選択します。 「フレームの先頭」：フレームの先頭から判定します (プリアンブル除く)。 「IP ヘッダ」：IP ヘッダの先頭から判定します。 「アプリケーションヘッダ」：アプリケーションヘッダの先頭から判定します。
オフセットタイプ	「固定」チェックがオフの場合：入力したオフセット値「以降のバイト列」からパターン一致を判定します。 「固定」チェックがオンの場合：入力したオフセット値「のみ」からパターン一致判定します。
オフセット	開始場所を 0 としたオフセットバイト数を指定します。形式は 16 進数と 10 進数のどちらかを右側のラジオボタンから選択できます。
パターン形式	「ASCII」または「Hex」から選択します。
マスク	パターン形式が「HEX」の場合のみ有効です。マスクパターンを HEX 文字列で指定します。
パターン	一致文字列を ASCII または HEX の文字列で指定します。