パターンフィルタの設定方法

SYNESIS　Ver. 7.0

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“GET”を含む行を選択。
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ため、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]

重要度	No.	チャネル	時間	デルタ時間	送信元	送信先	プロトコル	長さ	サマリ
	999	ip-172-31	13:42:03.3672	0.000167(	192.168.202.1	192.168.27.1	TCP	66	38425 → 22306 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PE
	1000	ip-172-31	13:42:03.3674	0.000166(	192.168.202.1	192.168.21.20	HTTP	722	GET /phpmyadmin/index.php?token=e600db693d72c0fe308633e286
	1001	ip-172-31	13:42:03.3675	0.000169(	192.168.202.1	192.168.27.1	TCP	66	15200 → 22359 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PE

[詳細]

▼Hypertext Transfer Protocol

▶ **GET /phpmyadmin/index.php?token=e600db693d72c0fe308633e28611b835 HTTP/1.1\r\n**

Host: 192.168.21.203\r\n

Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1\r\n

Accept-Language: en\r\n

[HEX]

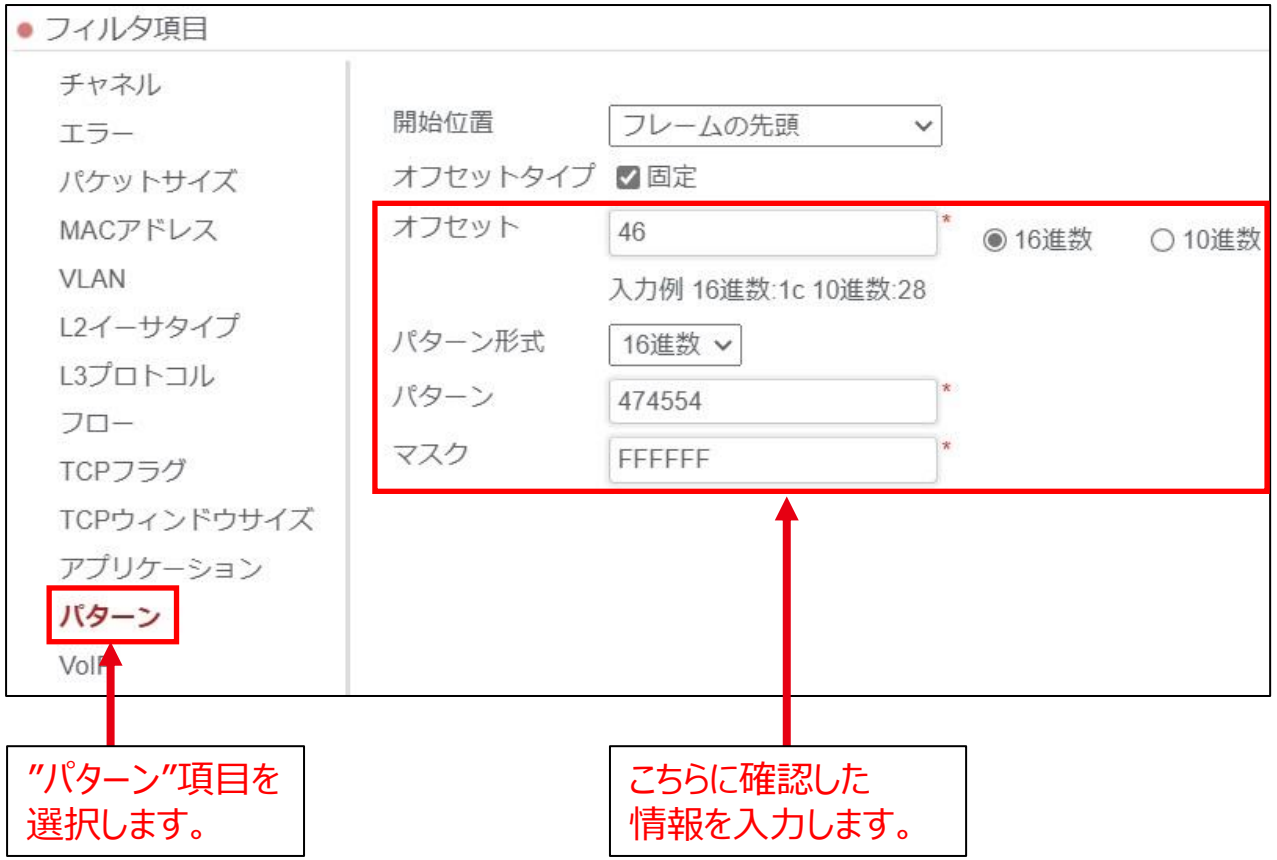
アドレス	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0020	CA	8A	C0	A8	15	CB	89	88	00	50	F2	DF	90	51	21	D4
0030	7E	E7	80	18	03	91	29	9B	00	00	01	01	08	0A	00	51
0040	00	3C	00	0A	05	F5	**47**	**45**	**54**	**20**	**2F**	**70**	**68**	**70**	**6D**	**79**

・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:0x46
マスク　　:0xFF FF FF
パターン :0x47 45 54(ASCIIで”GET”)

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



項目	説明	
開始場所	パターンの一致を判定する位置を指定する際、パケットのどの位置を "0" とするかを選択します。選択項目は以下の 3 種類です。	
	フレームの先頭	フレームの先頭を起点とします。
	IP ヘッダ	IP ヘッダの先頭を起点とします。
	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(L4 ヘッダの終端)を起点とします。
オフセットタイプ	「固定」にチェックを入れると、パターンの一致を判定する位置を固定します。無効の場合は、指定した位置以降のすべてのバイト列が対象となります。	
	「固定」が無効	「開始場所」と「オフセット」で指定された「以降のすべてのバイト列」でパターン一致を判定します。
	「固定」が有効	「開始場所」と「オフセット」で指定されたバイト列のみでパターンの一致を判定します。
オフセット	「開始場所」で指定された位置を起点として、パターンの一致を判定する位置をバイトで指定します。「16 進数」または「10 進数」で選択することができます。	
パターン形式	パターン文字列の表示形式を指定します。「ASCII」 または 「16 進数」 で選択することができます。	
パターン	パターンを「ASCII」または「16 進数」で指定します。	
マスク	「マスク」のパターンを 16 進数で指定します。パターン形式が「16 進数」の場合のみ有効で、「ASCII」を指定した場合は選択できません。	