L3 および L4 フィルタを持つ Ethernet 用セキュリティスイッチ

4 December 2020

更新履歴

版数	日付	内容
0.5	2020.12.04	初版

目次

1. 概要

L2/L3/L4 フィルターによる高いセキュリティと FPGA ハードウェア処理による低消費電力および高速処理を特徴としたセキュリティスイッチ用 IP である。

低消費電力・高性能のファイアウォール機能を実現するためにハッシュ計算をベースとしたホワイトリストテーブルを FPGA 内部メモリと論理回路で実現しており、ユーザが L2/L3/L4 ヘッダの組み合わせから成るフィルタ条件を設定することができる。また、受信パケットや送信パケットを対象としたポートミラー機能によりユーザのトラフィック監視や解析をサポートしており、最大で 1GbE x 4 ポートの Ethernet スイッチ性能を持つ。IoT(Internet of Things)や車載ゲートウェイとしての応用に適した低コストスイッチを実現可能である。

1.1. ハードウェア諸元

ポリシースイッチ(セキュリティスイッチ)用 IP は NetFPGA などの FPGA に実装されることでハードウェアによる高速スイッチング機能を提供する。ベースとなる NetFPGA のハードウェア諸元を表 1-1 に示す。

表 1-1 ポリシースイッチハードウェア仕様

項番	項目	内容	備考
1	ボード型名	NetFPGA-1G-CML	
2	ネットワークインタフェース	10/100/1000Base-T	
3	LAN ポート	RJ-45 4 ポート	
4	レイヤ2フレーム形式	Ethernet V2	
5	レイヤ3フレーム形式	IPv4 オプション無し	
6	フロー制御	未サポート	
7	VLAN	未サポート	
8	最大フレーム長	1518Byte(FCS 含む)	
9	電源入力	DC12V 5A	
9	電源コネクタ	ATX 電源の 6 ピン PCIe 電源コネクタ	

NetFPGA のハーウェア仕様については、下記 URL に詳細が記載されている。
https://netfpga.org/site/#/systems/2netfpga-1g-cml/details/

1.2. 電源投入・切断

ポリシースイッチの電源コネクタに ATX 電源の 6 ピン PCIe 電源コネクタを接続し、電源スイッチを ON にする事で外部不揮発メモリから FPGA への回路情報(ビットストリームデータ)の転送が自動的に開始される。その後、ビットストリームデータの転送が完了次第、FPGA がポリシースイッチとして動作することになる。

一方、電源スイッチを OFF にすることで電源が遮断されスイッチ動作が停止する。

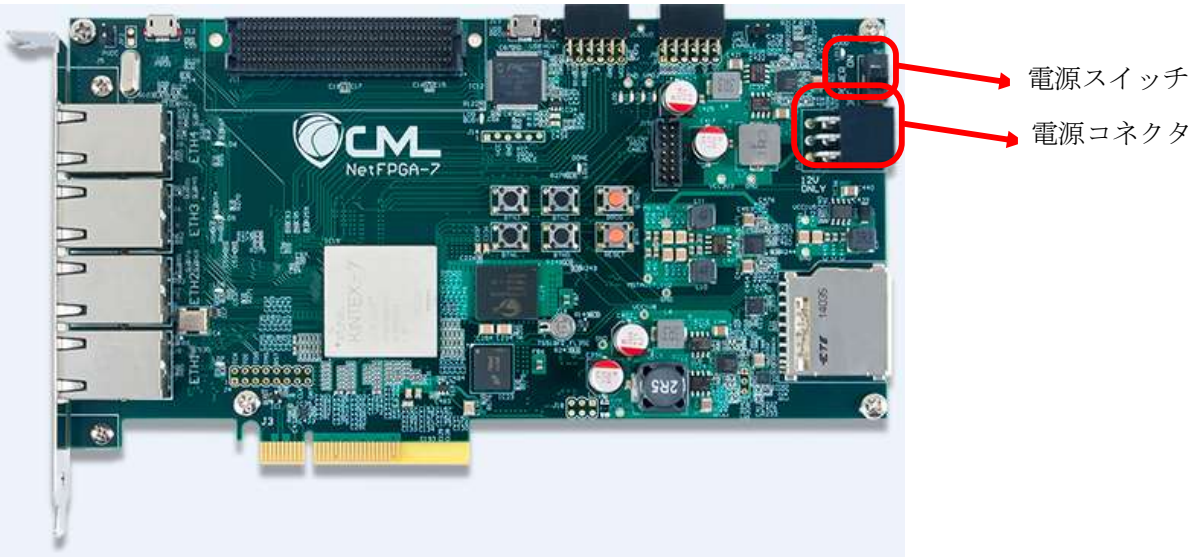

図 1-1 NetFPGA-1G-CML の電源スイッチ

1.3. ステータス LED

ステータス LED は NetFPGA の部品面(表側)に実装されている。

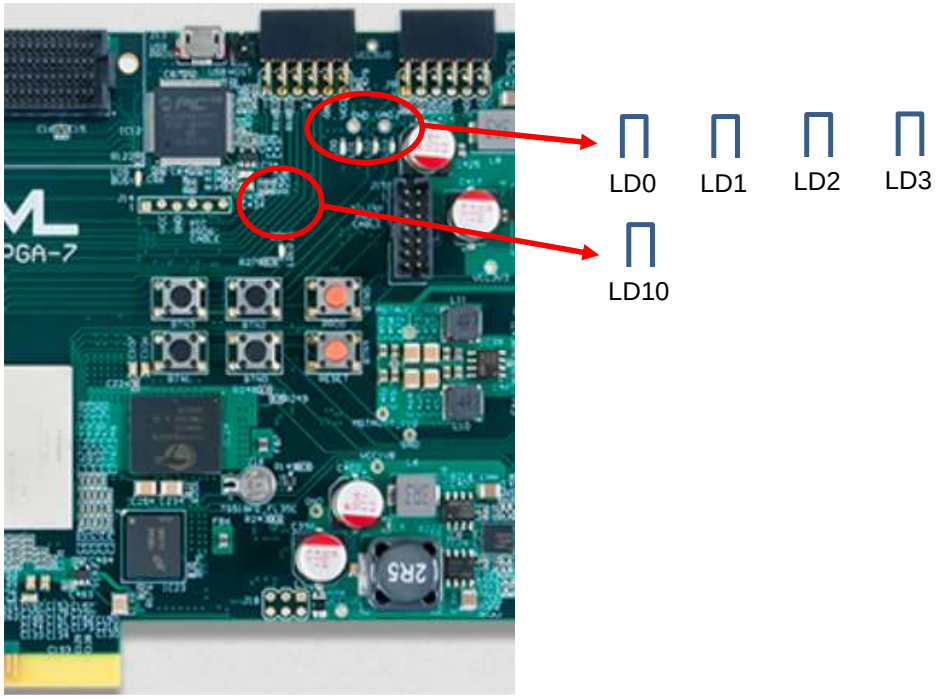

図 1-2 NetFPGA-1G-CML のステータス LED の配置

1.3.1. FPGA コンフィグレーション (LD10)

FPGA のコンフィグレーションが正常に終了した事を示す。

表 1-2 FPGA コンフィグレーション LED

項番	LED	説明	備考
1	LD10	コンフィグレーション動作結果 緑点灯：正常　消灯：失敗	

1.3.2. FPGA バージョン (LD0 - LD3)

FPGA のバージョンを表示する。

表 1-3 FPGA コンフィグレーション LED

項番	LED	説明	備考
1	LD0	FPGA のバージョンを示す	
2	LD1		
3	LD2		
4	LD3		

2. ルーティング機能

ポリシースイッチは 4 ポートある物理 LAN ポートに対し、ポート 1 とポート 2 をグループ A として、ポート 4 とポート 2 をグループ B として、そしてポート 1 とポート 4 をグループ C としてグループ分けしており、グループ内でフレームを転送する。物理 LAN ポート 3 は後述するポートミラーリング専用のポートとして割り当てられており、ポートミラーリング以外の用途で使用することはできない。

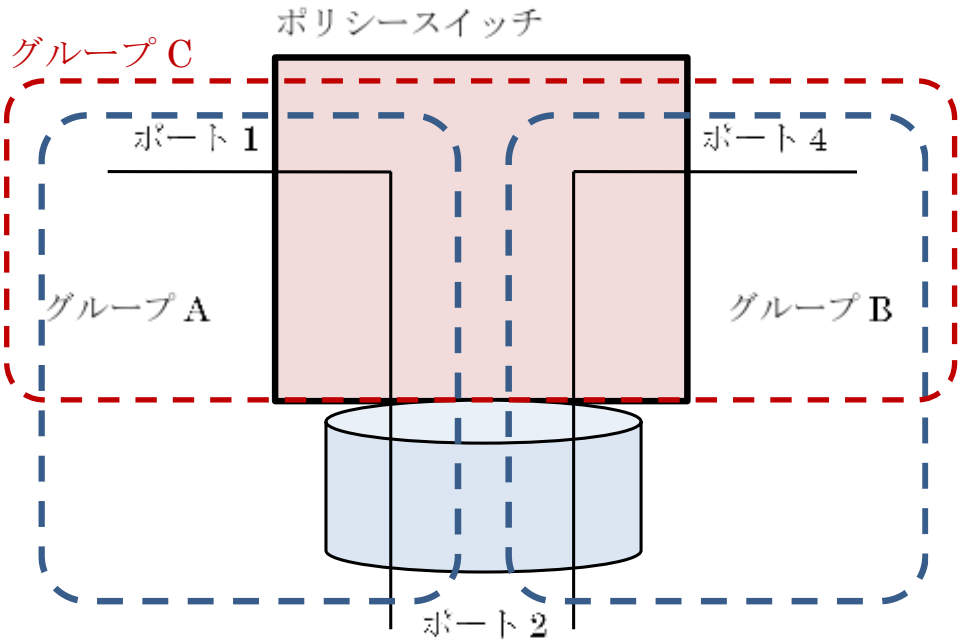

図 2-1 ポリシースイッチのルーティング機能

ポート 2 の物理インタフェースはグループ A とグループ B で共有されるが、ポリシースイッチはポート 2 から受信したフレームをそれぞれグループ A, グループ B に振り分けて転送する。振り分けの決定条件としては、高いセキュリティ機能を提供する SMAC、SIP によるルーティング動作モード、通常の DMAC、DIP によるルーテ

ィング動作モードの合計 4 つの動作モードがある。

表 2-1 ポリシースイッチのポート 2 宛先選択モード

モード	受信ポート	ヘッダ情報	転送先ポート	備考
1	SMAC がグループ A に所属	-	ポート 1	デフォルト動作
	SMAC がグループ B に所属	-	ポート 4	
2	SIP がグループ A に所属	-	ポート 1	
	SIP がグループ B に所属	-	ポート 4	
3	-	DMAC による	ポート 1 or 4	
4	-	DIP による	ポート 1 or 4	

2.1. ポートミラー機能

ポリシースイッチは受信ポートミラー機能を有する。ミラーポートにポート 3 を割り当て、ポート 1,4 から受信したフレーム、及びポート 2 から受信してポート 1,4 に転送するフレームをポート 3 にミラーリングする。なお、ミラー先のポートで合計帯域が回線容量を超える場合、ポリシースイッチ内でフレーム廃棄が発生することに注意する必要がある。

受信ポートミラーでは、フィルタ機能の適用前の受信フレーム、適用後の受信フレームのどちらかを選択してミラーする事が出来る。

3. フィルタ機能

3.1. 受信フレームのチェックフィールド

ポート 2 で受信するフレームでモード 1 のチェックフィールドを示す。

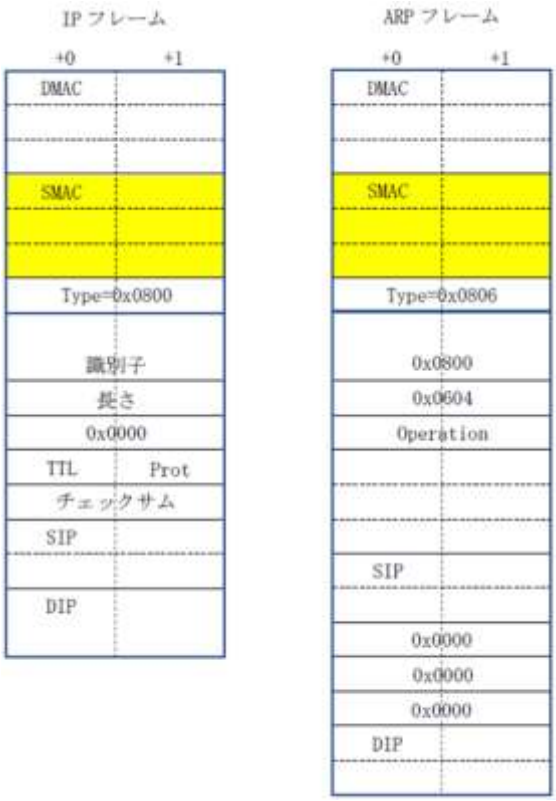

図 3-1 受信フレームのチェックフィールド(SMAC)

ポート 2 で受信するフレームでモード 2 のチェックフィールドを示す。

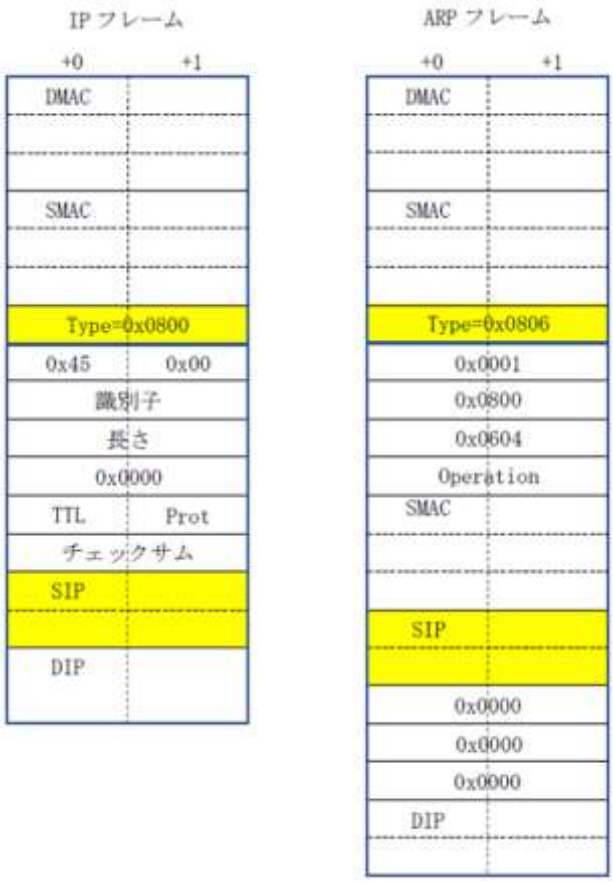

図 3-2 受信フレームのチェックフィールド(SIP)

3.2. ホワイトリスト機能

ポリシースイッチはホワイトリストによる受信フレームのフィルタを行い、該当するフレームのみを通過させる機能を有する。ホワイトリストはグループ A,B,C の全てで使用される。

表 3-1 フィルタ仕様

項番	項目	説明	備考
1	対象フレーム	EthernetV2＋ARP EthernetV2＋IPv4 　IP オプション無し EthernetV2＋IPv4＋TCP 　IP,TCP オプション無し	
2	フィルタ挙動	フレーム通過	
3	エントリ数	テーブル種類毎に 256	
4	ワイルドカードマスク	未サポート(ビット完全一致)	
5	テーブル書き換え	任意に可能 電源 OFF/ON でデフォルト値に戻る	

ホワイトリストは 6 種類のテーブルフォーマットがある。それぞれ、通過させる受信フレームの SMAC,DMAC,SIP,DIP 等の条件をホワイトリストに登録する。

表 3-2 ホワイトリストのテーブル種類(IP)

#	ポート番号	L2 ヘッダ EthernetV2			L3 ヘッダ IPv4			L4 ヘッダ TCP		
	受信	SMAC	DMAC	Type	SIP	DIP	Protcol	SPort	DPort	Session flag(6bit)
1	○	○	○	○	○	○	○			
2	○	○	○	○	○	○	○			○
3	○			○	○	○	○			
4	○			○	○	○	○			○

表 3-3 ホワイトリストのテーブル種類(ARP)

#	ポート番号	L2 ヘッダ EthernetV2			ARP		
	受信	SMAC	DMAC	Type	Operation	SIP	DIP
1	○	○		○	○	○	○
2	○			○	○	○	○

3.2.1. ホワイトリストのデフォルト値

ポリシースイッチにおけるホワイトリストのデフォルト値を示す。表 3-4 と表 3-5 は IP パケット転送時に適用されるデフォルトのホワイトリストテーブルを示している。

表 3-4 グループ A(IP)

	L2				L3			L4
#	ポート番号(IN)	SMAC	DMAC	Tpye	Protcol	SIP	DIP	session flg(6b)
1	1	*	*	0x0800	0x06	192.168.20.10	192.168.20.20	*
2	1	*	*	0x0800	0x06	192.168.20.40	192.168.20.20	*
3	1	*	*	0x0800	0x06	192.168.20.50	192.168.20.20	*
4	1	*	*	0x0800	0x06	192.168.20.60	192.168.20.20	*
5	2	*	*	0x0800	0x06	192.168.20.20	192.168.20.10	*
6	2	*	*	0x0800	0x06	192.168.20.20	192.168.20.40	*
7	2	*	*	0x0800	0x06	192.168.20.20	192.168.20.50	*
8	2	*	*	0x0800	0x06	192.168.20.20	192.168.20.60	*
9	2	*	*	0x0800	0x11	192.168.20.20	192.168.20.60	
10	2	*	*	0x0800	0x11	192.168.20.20	192.168.20.255	
11	1	*	*	0x0800	0x01	192.168.20.50	192.168.20.20	
12	2	*	*	0x0800	0x01	192.168.20.20	192.168.20.50	
13	1	*	*	0x0800	0x11	192.168.20.60	192.168.20.20	
14	1	*	*	0x0800	0x11	192.168.20.60	192.168.20.255	

表 3-5 グループ B(IP)

	L2				L3			L4
#	ポート番号(IN)	SMAC	DMAC	Type	Protcol	SIP	DIP	session flg(6b)
1	4	*	*	0x0800	0x11	192.168.10.10	192.168.10.40	*
2	4	*	*	0x0800	0x11	192.168.10.30	192.168.10.40	*
3	2	*	*	0x0800	0x11	192.168.10.40	192.168.10.10	*
4	2	*	*	0x0800	0x11	192.168.10.40	192.168.10.30	*

一方で、表 3-6 と表 3-7 は ARP(ICMP)パケット転送時に適用されるホワイトリストテーブルのデフォルト値を示している。

表 3-6 グループ A(ARP)

	L2				ARP		
#	ポート番号 (IN)	SMAC	DMAC	Tpye	Oprration	SIP	DIP
1	1	*	*	0x0806	0x0001	192.168.20.10	192.168.20.20
2	1	*	*	0x0806	0x0002	192.168.20.10	192.168.20.20
3	1	*	*	0x0806	0x0001	192.168.20.40	192.168.20.20
4	1	*	*	0x0806	0x0002	192.168.20.40	192.168.20.20
5	1	*	*	0x0806	0x0001	192.168.20.50	192.168.20.20
6	1	*	*	0x0806	0x0002	192.168.20.50	192.168.20.20
7	1	*	*	0x0806	0x0001	192.168.20.60	192.168.20.20
8	1	*	*	0x0806	0x0002	192.168.20.60	192.168.20.20
9	2	*	*	0x0806	0x0001	192.168.20.20	192.168.20.10
10	2	*	*	0x0806	0x0002	192.168.20.20	192.168.20.10
11	2	*	*	0x0806	0x0001	192.168.20.20	192.168.20.40
12	2	*	*	0x0806	0x0002	192.168.20.20	192.168.20.40
13	2	*	*	0x0806	0x0001	192.168.20.20	192.168.20.50
14	2	*	*	0x0806	0x0002	192.168.20.20	192.168.20.50
15	2	*	*	0x0806	0x0001	192.168.20.20	192.168.20.60
16	2	*	*	0x0806	0x0002	192.168.20.20	192.168.20.60

表 3-7 グループ B(ARP)

	L2				ARP		
#	ポート番号(IN)	SMAC	DMAC	Type	Opreration	SIP	DIP
1	4	*	*	0x0806	0x0001	192.168.10.10	192.168.10.40
2	4	*	*	0x0806	0x0002	192.168.10.10	192.168.10.40
3	4	*	*	0x0806	0x0001	192.168.10.30	192.168.10.40
4	4	*	*	0x0806	0x0002	192.168.10.30	192.168.10.40
5	2	*	*	0x0806	0x0001	192.168.10.40	192.168.10.10
6	2	*	*	0x0806	0x0002	192.168.10.40	192.168.10.10

7	2	*	*	0x0806	0x0001	192.168.10.40	192.168.10.30
8	2	*	*	0x0806	0x0002	192.168.10.40	192.168.10.30

4. コンフィギュレーション

4.1. コンフィグレーション設定

ポリシースイッチは専用インタフェースを介して、以下の設定を行う事が可能である。

・ポート 2 から受信してポート 1,4 にフレームを振り分ける SMAC,SIP の設定
・フィルタ機能の ON/OFF を選択
・ポート毎にポートミラーON/OFF を選択
・ポートミラーでミラーするフレームでフィルタ機能の適用前/後を選択

なお、ポリシースイッチのの電源を OFF/ON すると、デフォルトのコンフィグレーション設定に戻ることに注意する必要がある。
コンフィギュレーション設定の際は、CSV 書式のファイルを使用する。

```
# set sip/smac
switch_mode,sip
# set ip address
out_sip,192.168.20.20
in_sip,192.168.10.40
# set mac address
out_smac,00-20-7F-80-00-02
in_smac,00-20-7F-80-00-03
# set on/off
port_mirror1,on
port_mirror4,off
port_mirror-2out,off
port_mirror-2in,off
# set before/after
port_mirror-whitelist,before
```

図 4-1 コンフィギュレーション設定ファイルの例

表 4-1 コンフィグレーション設定ファイルの書式

項番	項目	説明
1	ファイルタイプ	ASCII
2	形式	CSV
3	使用文字	半角英数字,半角記号
4	区切り文字	「,」（カンマ）

表 4-2 パラメータ設定値

項番	パラメータ	説明	設定値
1	switch_mode	ポート 2 のフレーム振り分けを SMAC/SIP のどちらかで行うか選択	smac,sip
2	out_sip	ポート 2 からポート 1 宛の SIP	XX.XX.XX.XX (*1)
3	in_sip	ポート 2 からポート 4 宛の SIP	XX.XX.XX.XX (*1)
4	out_smac	ポート 2 からポート 1 宛の SMAC	XX-XX-XX-XX-XX-XX (*2)
5	in_smac	ポート 2 からポート 4 宛の SMAC	XX-XX-XX-XX-XX-XX (*2)
6	port_mirror1	ポート 1 のミラーON/OFF を選択	on,off
7	port_mirror4	ポート 4 のミラーON/OFF を選択	on,off
8	port_mirror-2out	ポート 2 からポート 1 宛てのミラー ON/OFF を選択	on,off
9	port_mirror-2in	ポート 2 からポート 4 宛てのミラー ON/OFF を選択	on,off
10	port_mirror-whitelist	ポートミラーでフィルタ適用前(before)/後(after)を選択	before,after
11	#	先頭文字が#の場合、コメント行	

(*1)10 進数表記
(*2)ゼロパディングした 16 進数 2 文字

4.2. ホワイトリスト設定

ポリシースイッチは専用インタフェースを介して、フィルタで使用するホワイトリストの書き換えが可能である。
なお、ポリシースイッチのの電源を OFF/ON すると、デフォルトのホワイトリストに戻る。

設定には CSV 書式のファイルを使用する。

```
#En,InPort,OutPort,SMAC,DMAC,Type,Prot,SIP,DIP,SPort,DPort,U,A,P,R,S,F,Operation
#table-1 #1
1,1,2,60-61-62-63-64-65,70-71-72-73-74-75,0x0800,0x06,192.168.20.70,192.168.20.20,-,-,-,-,-,-,-,-
1,2,1,60-61-62-63-64-65,70-71-72-73-74-75,0x0800,0x06,192.168.20.20,192.168.20.70,-,-,-,-,-,-,-,-
#table-1 #2
1,1,2,60-61-62-63-64-65,70-71-72-73-74-75,0x0800,0x06,192.168.20.80,192.168.20.20,-,-,0,1,0,0,0,0
1,1,2,60-61-62-63-64-65,70-71-72-73-74-75,0x0800,0x06,192.168.20.80,192.168.20.20,-,-,0,0,0,0,1,0
#table-1 #3
1,1,2,*,*,0x0800,0x06,192.168.20.90,192.168.20.20,-,-,-,-,-,-,-,-
1,2,1,*,*,0x0800,0x06,192.168.20.20,192.168.20.90,-,-,-,-,-,-,-,-
#table-1 #4
1,1,2,*,*,0x0800,0x06,192.168.20.100,192.168.20.20,-,-,0,1,0,0,0,0
1,1,2,*,*,0x0800,0x06,192.168.20.100,192.168.20.20,-,-,0,0,0,0,1,0
#table-1 #5
1,1,2,60-61-62-63-64-65,*,0x0806,*,192.168.20.110,192.168.20.20,-,-,-,-,-,-,-,-,0x0001
#table-1 #6
1,2,1,*,*,0x0806,*,192.168.20.20,192.168.20.110,-,-,-,-,-,-,-,-,0x0002
```

図 4-2 ホワイトリスト設定ファイルの例

表 4-3 ホワイトリスト設定ファイルの書式

項番	項目	説明
1	ファイルタイプ	ASCII
2	形式	CSV
3	使用文字	半角英数字,半角記号
4	区切り文字	「,」（カンマ）

表 4-4 パラメータ設定値

Column	記号	説明	設定値
1	#En	行のコメント(#)/無効(0)/有効(1)	#
			1
			0
2	InPort	受信ポート番号	1,2,4
3	OutPort	送信ポート番号	1,2,4
4	SMAC	Ethernet ヘッダの SMAC	XX-XX-XX-XX-XX-XX (*1)
5	DMAC	Ethernet ヘッダの DMAC	XX-XX-XX-XX-XX-XX (*1)
6	Type	Ethernet ヘッダの Type	0xXXXX (*2)
7	Port	IP ヘッダの Port	0xXX (*3)
8	SIP	IP ヘッダの SIP	XX.XX.XX.XX (*4)
9	DIP	IP ヘッダの DIP	XX.XX.XX.XX (*4)
10	SPort	Reserved(TCP ヘッダの SPort)	
11	DPort	Reserved(TCP ヘッダの DPort)	
12	U	TCP ヘッダの URG	0,1
13	A	TCP ヘッダの ACK	0,1
14	P	TCP ヘッダの PSH	0,1
15	R	TCP ヘッダの RST	0,1
16	S	TCP ヘッダの SYN	0,1
17	F	TCP ヘッダの FIN	0,1
18	Operation	ARP ヘッダの Operation	0xXXXX (*2)

(*1)ゼロパディングした 16 進数 2 文字
(*2)ゼロパディングした 16 進数 4 文字。0x は 16 進数を示す
(*3)ゼロパディングした 16 進数 2 文字。0x は 16 進数を示す
(*4)10 進数表記