アルテリア・ネットワークス社「クロスパス」を利用するための設定例

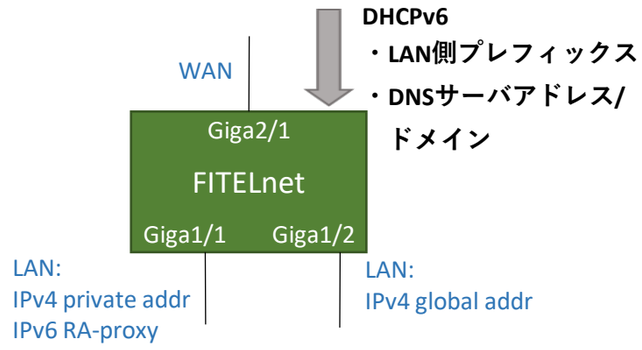
対象装置：FITELnet F70/F71/F220/F221/F225/F310/F220 EX/F221 EX

固定IP8/IP16

・WANからLANへのIPv6プレフィクス
　配布にDHCPv6-PDを利用

※本設定例は、「固定IP8」を使用する場合の例です。
「固定IP16」では、Giga 1/2 (Port-channel 12) に
マスク長28を設定かつ access-list 100 のエントリを
必要に応じて追加してください。

○：対応する構成
HGWあり/ひかり電話あり
HGWあり/ひかり電話なし
○ HGWなし/ひかり電話あり
HGWなし/ひかり電話なし



	設定例	補足
1	access-list 100 permit ip any host ##固定IP8アドレス-2##	IPv4アクセスリスト（グローバルアドレス宛の通信を許可） ★お客様の環境に合わせて設定してください。
2	access-list 100 permit ip any host ##固定IP8アドレス-3##	IPv4アクセスリスト（グローバルアドレス宛の通信を許可） ★お客様の環境に合わせて設定してください。
3	access-list 100 permit ip any host ##固定IP8アドレス-4##	IPv4アクセスリスト（グローバルアドレス宛の通信を許可） ★お客様の環境に合わせて設定してください。
4	access-list 100 permit ip any host ##固定IP8アドレス-5##	IPv4アクセスリスト（グローバルアドレス宛の通信を許可） ★お客様の環境に合わせて設定してください。
5	access-list 111 deny udp any eq 135 any	UDPポート135（MS DCOM / RPC）からの全てのトラフィックを拒否します。
6	access-list 111 deny udp any any eq 135	UDPポート135（MS DCOM / RPC）への全てのトラフィックを拒否します。
7	access-list 111 deny tcp any eq 135 any	TCPポート135（MS DCOM / RPC）からの全てのトラフィックを拒否します。
8	access-list 111 deny tcp any any eq 135	TCPポート135（MS DCOM / RPC）への全てのトラフィックを拒否します。
9	access-list 111 deny udp any range 137 139 any	UDPポート137-139（NetBIOS関連）からの全てのトラフィックを拒否します。
10	access-list 111 deny udp any any range 137 139	UDPポート137-139（NetBIOS関連）への全てのトラフィックを拒否します。
11	access-list 111 deny tcp any range 137 139 any	TCPポート137-139（NetBIOS関連）からの全てのトラフィックを拒否します。
12	access-list 111 deny tcp any any range 137 139	TCPポート137-139（NetBIOS関連）への全てのトラフィックを拒否します。
13	access-list 111 deny udp any eq 445 any	UDPポート445（Microsoft-DS / SMB）からの全てのトラフィックを拒否します。
14	access-list 111 deny udp any any eq 445	UDPポート445（Microsoft-DS / SMB）への全てのトラフィックを拒否します。
15	access-list 111 deny tcp any eq 445 any	TCPポート445（Microsoft-DS / SMB）からの全てのトラフィックを拒否します。
16	access-list 111 deny tcp any any eq 445	TCPポート445（Microsoft-DS / SMB）への全てのトラフィックを拒否します。
17	access-list 112 deny ip 192.168.100.0 0.0.0.255 any	IPアドレス範囲192.168.100.0/24からの全てのトラフィックを拒否します。
18	access-list 112 permit icmp any 192.168.100.0 0.0.0.255	192.168.100.0/24へのICMPトラフィックを許可します。
19	access-list 113 spi tcp any any eq ftp	TCPポート21（FTP）への全てのトラフィックを許可します。応答パケットも許可されます。
20	access-list 113 spi tcp any any eq ftp-data	TCPポート20（FTPデータ）への全てのトラフィックを許可します。応答パケットも許可されます。
21	access-list 113 spi tcp any any eq www	TCPポート80（HTTP）への全てのトラフィックを許可します。応答パケットも許可されます。
22	access-list 113 spi udp any any eq domain	UDPポート53（DNS）への全てのトラフィックを許可します。応答パケットも許可されます。
23	access-list 113 spi tcp any any eq smtp	TCPポート25（SMTP）への全てのトラフィックを許可します。応答パケットも許可されます。
24	access-list 113 spi tcp any any eq pop3	TCPポート110（POP3）への全てのトラフィックを許可します。応答パケットも許可されます。
25	access-list 113 spi tcp any any eq 587	TCPポート587（SMTPサブミッション）への全てのトラフィックを許可します。応答パケットも許可されます。
26	access-list 113 spi tcp any any	全てのTCPトラフィックを許可します。応答パケットも許可されます。
27	access-list 113 spi udp any any	全てのUDPトラフィックを許可します。応答パケットも許可されます。
28	access-list 114 permit ip any any	全てのIPトラフィックを許可します。
29	access-list 115 deny ip any any	全てのIPトラフィックを拒否します。
30	access-list 4000 permit icmp6 any any neighbor-advertisement	IPv6アクセスリスト（NA許可）
31	access-list 4000 permit icmp6 any any neighbor-solicitation	IPv6アクセスリスト（NS許可）
32	access-list 4000 permit icmp6 any any router-advertisement	IPv6アクセスリスト（RA許可）
33	access-list 4000 permit udp any any eq 546	IPv6アクセスリスト（DHCPv6許可）
34	access-list 4009 deny ipv6 any any	IPv6アクセスリスト（access-list 4000と学習フィルタ以外を拒否）
35	access-list 4010 spi ipv6 any any	IPv6アクセスリスト（学習フィルタ）
36	!	
37	ip route 0.0.0.0 0.0.0.0 tunnel 1	IPv4 default経路設定（デフォルトルートをIPv4overIPv6トンネルに設定）
38	ip name-server ::1	DNSサーバー設定（自装置をサーバーに設定）
39	!	
40	ip dhcp server-profile LAN	DHCPv4サーバープロファイル
41	address 192.168.0.2 192.168.0.254	配布アドレス設定
42	lease-time 28800	DHCPリース期間設定
43	dns 192.168.0.1	配布DNSサーバーアドレス設定
44	gateway 192.168.0.1	配布Gatewayアドレス設定
45	exit	
46	!	
47	ip nat list 1 192.168.0.0 0.0.0.255	NAT変換対象アドレス設定（LAN側 192.168.0.0/24）
48	ip nat default action pass	NAT対象外のパケットを中継する設定 ※送信元アドレス「192.0.2.2-192.0.2.6」を中継するために設定します。
49	!	
50	ipv6 route ::/0 dhcp port-channel 1	IPv6 default経路設定（デフォルトルートをDHCPv6サーバとする設定）
51	!	
52	ipv6 dhcp client-profile NGN	DHCPv6クライアントプロファイル
53	option-request prefix-delegation	アドレスプレフィックス要求設定
54	option-request dns-server	DNSサーバの情報取得要求の設定
55	retries infinity	DHCPメッセージの返信があるまで再送する設定
56	exit	
57	!	
58	ipv6 dhcp server-profile LANv6	DHCPv6サーバープロファイル
59	dns port-channel 1	DHCPv6クライアント機能で取得したDNSサーバアドレスを配布する設定
60	exit	
61	!	

	設定例	補足
62	ipinip tunnel-profile IPIP1	IPinIPトンネルプロファイル
63	profile-mode ipip	プロファイルモードをIPinIPに設定
64	source ipv6 port-channel 11	Outerの送信元アドレス：Port-channel11のIPv6アドレスを指定
65	destination address ##トンネル終端装置 IPv6アドレス##	Outerの宛先アドレス：トンネル終端装置のアドレスを設定 ★アルテリア・ネットワークス社の指定に合わせて設定ください。 例）destination address 2001:db8::1
66	ipinip fragment pre	プリフラグメント設定
67	exit	
68	!	
69	logging buffer level informational	装置内部バッファへ出力するログレベル（informational）を指定：指定したレベル名称以上（レベル番号以下）のログ情報を出力します。
70	!	
71	aaa authentication login default local	本装置にログインする□場合の認証方式を指定（username コマンドで登録したID/パスワードとする）
72	aaa authorization exec default local	本装置でコマンド実行を許可するかどうかの□許可方式を指定（username コマンドで登録した特権レベルとする）
73	!	
74	username test privilege 15 password 2 1LAruCQ4A$T3O69MOhXaiNub6xoHNsG1	ログインユーザ□□名（guest）とパスワード□□(guest-secret）の登録
75	!	
76	hostname FITELnet	hostname設定
77	!	
78	interface GigaEthernet 1/1	物理インターフェース（LAN側）
79	vlan-id 11	
80	bridge-group 11	
81	channel-group 11	LAN側論理インタフェース（Port-channel）と紐付け
82	exit	
83	!	
84	interface GigaEthernet 1/2	物理インターフェース（LAN側）
85	vlan-id 12	
86	bridge-group 12	
87	channel-group 12	LAN側論理インタフェース（Port-channel）と紐付け
88	exit	
89	!	
90	interface GigaEthernet 2/1	物理インターフェース（WAN側）
91	vlan-id 1	
92	bridge-group 1	
93	channel-group 1	WAN側論理インタフェース（Port-channel）と紐付け
94	ipv6 access-group 4000 in	IPv6アクセスリスト紐づけ（NS/NA/RA/DHCPv6）
95	ipv6 access-group 4009 in	IPv6アクセスリスト紐づけ（deny）
96	ipv6 access-group 4010 out	IPv6アクセスリスト紐づけ（学習フィルタ）
97	exit	
98	!	
99	interface Port-channel 1	論理インターフェース（WAN側）
100	ipv6 enable	IPv6リンクローカルアドレス設定
101	ipv6 dhcp service client	DHCPv6クライアント設定
102	ipv6 dhcp client-profile NGN	DHCPv6クライアントプロファイル紐付け
103	exit	
104	!	
105	interface Port-channel 11	論理インターフェース（LAN側） IPv4：プライベートアドレスを設定 IPv6：RAで受信したプレフィックスを本IFに割り当て（RA-proxy機能） ※RA-proxy機能にて、RAで受信したプレフィックスを複数のLAN側 Port-channelに割り当てることはできません。
106	ip dhcp service server	DHCPv4サーバー設定
107	ip dhcp server-profile LAN	DHCPv4サーバープロファイル紐付け
108	ip address 192.168.0.1 255.255.255.0	IPv4アドレス設定
109	ipv6 enable	IPv6リンクローカルアドレス設定
110	ipv6 address dhcp port-channel 1 ##インタフェースID##/64	IPv6アドレス設定（RAから上位64bit＋インタフェースIDから下位64bitによりアドレス生成） ★インタフェースIDはお客様の環境に合わせて設定してください。 例）ipv6 address dhcp port-channel 1 ::11/64
111	ipv6 nd other-config-flag	RA Oフラグセット
112	ipv6 nd send-ra	RA送信設定
113	ipv6 trust-ra-prefix-lifetime	RA prefix lifetime 0 を送信する設定 ＊プレフィックスの削除が行われた場合に、端末側に即時反映させるための設定です。 端末側のプレフィックス残留により通信ができなくなるケースを回避するために、本設定を推奨します。デフォルトでは、サービス否認攻撃を受ける環境を想定して、prefix lifetime 0 を送信しません。 ※F70/F71はV01.02(00)以降、F220/F221はV01.04(00)以降のファームウェアにてサポートするコマンドです。
114	ipv6 dhcp service server	DHCPv6サーバー設定
115	ipv6 dhcp server-profile LANv6	DHCPv6サーバープロファイル紐付け
116	mss 1420	MSS設定（1420byte：Tunnel 1から送信するIPv4overIPv6パケットのinner最大長に合わせた値です。）
117	link-state always-up	本論理インタフェースを常にリンクアップさせる設定
118	ddns-client address ipv6 action http-client 1 delay 10 interval 600	ダイナミックDNSクライアント設定
119	exit	
120	!	
121	interface Port-channel 12	論理インターフェース（LAN側） IPv4：固定IP8のグローバルアドレスを設定
122	ip address ##固定IP8アドレス-6## 255.255.255.248	IPv4グローバルアドレス設定 ★アルテリア・ネットワークス社より割り当てられた固定IP8アドレスをお客様の環境に合わせて設定してください。
123	mss 1420	MSS設定（1420byte：Tunnel 1から送信するIPv4overIPv6パケットのinner最大長に合わせた値です。）
124	exit	
125	!	

	設定例	補足
126	interface Tunnel 1	トンネルインタフェース設定
127	ip address ##固定IP8アドレス-1## 255.255.255.255	IPv4グローバルアドレス設定 ★アルテリア・ネットワークス社より割り当てられた固定IP8アドレスを お客様の環境に合わせて設定してください。
128	ip access-group 100 in	IPv4アクセスリスト紐づけ（permit）
129	ip access-group 111 out	IPv4アクセスリスト紐づけ
130	ip access-group 112 in	IPv4アクセスリスト紐づけ
131	ip access-group 113 out	IPv4アクセスリスト紐づけ
132	ip access-group 114 out	IPv4アクセスリスト紐づけ
133	ip access-group 115 in	IPv4アクセスリスト紐づけ
134	ip access-group spi ftp-data enable	学習フィルタ追加
135	ip nat inside source list 1 interface	NAT+設定（送信元アドレスをLAN側アドレスからグローバルアドレスに変換）
136	tunnel mode ipinip tunnel-profile IPIP1	トンネルプロファイル紐づけ
137	exit	
138	!	
139	line console	
140	exec-timeout 0	
141	authorization exec default local	
142	exit	
143	!	
144	line telnet	
145	exec-timeout 0	
146	exit	
147	!	
148	dns-server ip enable	DNSサーバ機能およびProxyDNS機能を有効化（IPv4）
149	dns-server ipv6 enable	DNSサーバ機能およびProxyDNS機能を有効化（IPv6）
150	!	
151	proxydns domain 1 any * any dhcp ipv6 port-channel 1 source-interface port-channel 11	ProxyDNSの正引き動作条件を指定（DHCPクライアントが取得したDNSサーバアドレスをリレー先に指定）
152	proxydns address 1 any dhcp ipv6 port-channel 1 source-interface port-channel 11	ProxyDNSの逆引き動作条件を指定（DHCPクライアントが取得したDNSサーバアドレスをリレー先に指定）
153	!	
154	http-client 1	ダイナミックDNSのHTTPクライアント設定
155	request-timeout 10 retry 5	登録要求メッセージの応答受信待ち許容時間とリトライ回数を設定
156	method 1 get url https://##Basic認証ID##:##Basic認証パスワード##@##アップデートサーバURL## d ##FQDN## p ##DDNSパスワード## u ##DDNS_ID## a $i6	HTTPSのRequest-Lineの設定 ★Basic認証ID、Basic認証パスワード、アップデートサーバURL、DDNS_ID、 DDNSパスワード、FQDNはアルテリア・ネットワークス社の指定に合わせて 設定ください。 例）method 1 get url https://BID:diAC/Lag5iPe6@www.example.net d example.com p DPASS u DID a $i6 ※HTTPS指定は、F70/F71はV01.03(00)以降、F220/F221はV01.05(00)以降の ファームウェアにてサポートしています。
157	reference-interface port-channel 11	methodコマンドで参照するインタフェースを指定
158	source-interface port-channel 11	登録要求メッセージの送信元アドレスを指定
159	logging on	HTTPクライアントのログ出力を行う設定
160	exit	
161	!	
162	end	