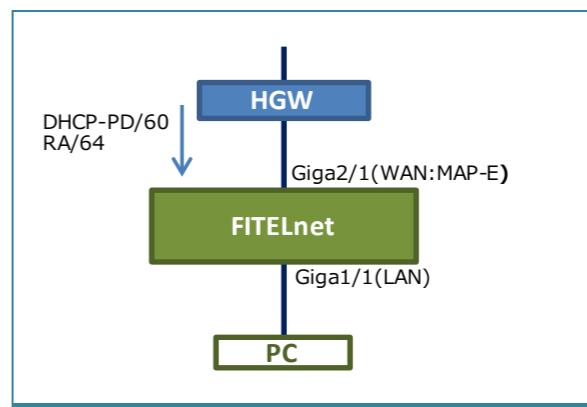


JPIX社「v6プラス」を利用するための設定例 (MAP-E方式)

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

パターン1 : HGWあり/ひかり電話あり	
受信IPv6 prefix	DHCPv6-PD/60 RA/64
WAN側 IPv6アドレス	RA/64から生成
WAN側 MAP-Eアドレス	RA/64から該当ルールを検索して生成
LAN側 IPv6アドレス	DHCPv6-PD/64に拡張(61-64bit:ALL1)してから生成
LAN側 PC配布 IPv6 prefix	RA/64



設定例	補足
1 access-list 100 permit udp any eq 67 any eq 68	IPv4アクセスリスト (DHCPv4許可)
2 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。
3 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。
4 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。
5 access-list 111 deny tcp 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。
6 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。
7 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。
8 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。
9 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。
10 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。
11 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。
12 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。
13 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。
14 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。
15 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。
16 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。
17 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。
18 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。
19 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。
20 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。
21 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。
22 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。
23 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。
24 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。
25 access-list 114 permit ip any any	全てのIPトラフィックを許可します。
26 access-list 115 deny ip any any	全てのIPトラフィックを拒否します。
27 access-list 4000 permit icmp6 any any neighbor-advertisement	IPv6アクセスリスト (NA許可)
28 access-list 4000 permit icmp6 any any neighbor-solicitation	IPv6アクセスリスト (NS許可)
29 access-list 4000 permit icmp6 any any router-advertisement	IPv6アクセスリスト (RA許可)
30 access-list 4000 permit udp any any eq 546	IPv6アクセスリスト (DHCPv6許可)
31 access-list 4009 deny ipv6 any any	IPv6アクセスリスト (全拒否)
32 access-list 4010 spi ipv6 any any	IPv6アクセスリスト (SPI)
33 !	
34 ip route 0.0.0.0 0.0.0.0 tunnel 1	IPv4デフォルトルート設定 (デフォルトルートをMAPトンネルに設定)
35 ip name-server ::1	DNSサーバー設定 (自装置をサーバーに設定)
36 !	
37 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。
38 !	
39 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)
40 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)
41 !	
42 username guest password guest-secret	ログインユーザ名 (guest) と、パスワード (guest-secret) の登録
43 !	
44 hostname FITELnet_MAPCE	hostname設定
45 !	
46 ip dhcp client-profile DHCPv4_client	DHCPv4クライアントプロファイル
47 retries infinity	DHCPメッセージの返信があるまで再送する設定
48 exit	
49 !	
50 ip dhcp server-profile DHCPv4_server	DHCPv4サーバープロファイル
51 address 192.168.100.2 192.168.100.254	配布アドレス設定
52 lease-time 259200	DHCPリース期間設定
53 dns 192.168.100.1	配布DNSサーバーアドレス設定
54 gateway 192.168.100.1	配布Gatewayアドレス設定
55 exit	
56 !	
57 ip nat list 1 192.168.100.0 0.0.0.255	NAT変換対象アドレス設定 (LAN側 192.168.100.0/24)
58 ip nat wellknown 1 1 65535 off	全ポートをNAT+変換する設定
59 ip nat port-sharing enable	NATポートシェアリング設定 *宛先アドレス/ポートの異なる複数のトラフィックに対して同一のNATエントリを適用して、NATのリソースを節約します。 ※F70/F71は初版から、F220/F221はV01.02(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。
60 !	
61 ipv6 dhcp client-profile DHCPv6_client	DHCPv6クライアントプロファイル
62 option-request prefix-delegation	アドレスプレフィックス要求設定
63 option-request dns-server	DNSサーバー要求設定
64 option-request dns-server-domain	DNSサーバードメイン要求設定
65 retries infinity	DHCPメッセージの返信があるまで再送する設定
66 exit	

	設定例	補足
67 !		
68 ipv6 dhcp server-profile DHCPv6_server	DHCPv6サーバープロファイル	
69 dns port-channel 2	WAN側で受信したDNSサーバを配布する設定	
70 domain port-channel 2	WAN側で受信したドメイン名を配布する設定	
71 exit		
72 !		
73 ipinip tunnel-profile MAPCE	MAPトンネルプロファイル	
74 profile-mode map-encap option-a	トンネルのプロファイルモードをMAP (v6プラス) に設定	
75 map rule-get	v6プラスのサービスを利用する設定	
76 ipinip fragment pre	プリフラグメント設定	
77 exit		
78 !		
79 interface GigaEthernet 1/1	物理インターフェース (LAN側)	
80 vlan-id 1	vlan-id設定 (ポートVLAN)	
81 bridge-group 1	ブリッジグループ設定	
82 channel-group 1	LAN側論理インターフェース (Port-channel) と紐付け	
83 exit		
84 !		
85 interface GigaEthernet 2/1	物理インターフェース (WAN側)	
86 vlan-id 2	vlan-id設定 (ポートVLAN)	
87 bridge-group 2	ブリッジグループ設定	
88 channel-group 2	WAN側論理インターフェース (Port-channel) と紐付け	
89 ip access-group 100 in	IPv4アクセリスト紐付け (DHCPv4)	
90 ip access-group 111 out	IPv4アクセリスト紐づけ	
91 ip access-group 112 in	IPv4アクセリスト紐づけ	
92 ip access-group 113 out	IPv4アクセリスト紐づけ	
93 ip access-group 114 out	IPv4アクセリスト紐づけ	
94 ip access-group 115 in	IPv4アクセリスト紐づけ	
95 ip access-group spi ftp-data enable	学習フィルタ追加	
96 ipv6 access-group 4000 in	IPv6アクセリスト紐付け (NS/NA/RA/DHCPv6)	
97 ipv6 access-group 4009 in	IPv6アクセリスト紐付け (deny)	
98 ipv6 access-group 4010 out	IPv6アクセリスト紐付け (SPI)	
99 exit		
100 !		
101 interface Port-channel 1	論理インターフェース (LAN側)	
102 ip dhcp service server	DHCPv4サーバー設定	
103 ip dhcp server-profile DHCPv4_server	DHCPv4サーバープロファイル紐付け	
104 ip address 192.168.100.1 255.255.255.0	IPv4アドレス設定	
105 ipv6 enable	IPv6リンクローカルアドレス設定	
106 ipv6 address dhcp port-channel 2 ::f:0:0:0:1/64	IPv6アドレス設定 (DHCPv6-PDから上位64bit+下位64bitアドレス生成)	
107 ipv6 nd other-config-flag	RAフラグセット	
108 ipv6 nd send-ra	RA送信設定	
109 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、末端側に即時反映させるための設定です。末端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。	
110 ipv6 dhcp service server	DHCPv6サーバー設定	
111 ipv6 dhcp server-profile DHCPv6_server	DHCPv6サーバープロファイル紐付け	
112 mss 1420	MSS設定 (1420byte : MAPトンネルから送信するIPv4overIPv6パケットのinner最大長に合わせた値です。)	
113 exit		
114 !		
115 interface Port-channel 2	論理インターフェース (WAN側)	
116 ip dhcp service client	DHCPv4クライアント設定	
117 ip dhcp client-profile DHCPv4_client	DHCPv4クライアントプロファイル紐付け	
118 ipv6 enable	IPv6リンクローカルアドレス設定	
119 ipv6 address autoconfig	IPv6アドレス設定 (RAからアドレス生成)	
120 ipv6 address autoconfig-map-encap MAPCE	IPv6アドレス設定 (RAからMAP-E用アドレス生成)	
121 ipv6 nd receive-ra	RA受信設定	
122 ipv6 router-lifetime-receive-enable	RA default経路登録設定	
123 ipv6 trust-ra-prefix-lifetime	RAで通知されたprefix valid lifetimeをそのままアドレスのlifetimeに反映する設定 * 本インターフェースアドレスとMAP-Eアドレスに、2時間よりも短いlifetimeを反映するための設定です。lifetime 0 が反映された場合はアドレスを削除します。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、2時間よりも短い値はlifetimeに反映しません。 ※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。	
124 ipv6 dhcp service client	DHCPv6クライアント設定	
125 ipv6 dhcp client-profile DHCPv6_client	DHCPv6クライアントプロファイル紐付け	
126 exit		
127 !		
128 interface Tunnel 1	MAPトンネルインターフェース	
129 ip access-group 111 out	IPv4アクセリスト紐づけ	
130 ip access-group 112 in	IPv4アクセリスト紐づけ	
131 ip access-group 113 out	IPv4アクセリスト紐づけ	
132 ip access-group 114 out	IPv4アクセリスト紐づけ	
133 ip access-group 115 in	IPv4アクセリスト紐づけ	
134 ip access-group spi ftp-data enable	学習フィルタ追加	
135 ip nat inside source list 1 map-encap overload	MAP用NAT+設定	
136 tunnel mode ipinip tunnel-profile MAPCE	MAP用プロファイルと紐付け	
137 exit		
138 !		
139 dns-server ip enable	DNSv4サーバー設定	
140 dns-server ipv6 enable	DNSv6サーバー設定	
141 !		
142 proxydns domain 1 any ntt.setup ::1/128 dhcp-no-skip ipv4 port-channel 2	proxyDNS 順引き設定 (IPv4 DNS / 自装置からHGWへ"ntt.setup"ドメインの問い合わせ)	
143 proxydns domain 2 any * any dhcp ipv6 port-channel 2	proxyDNS 順引き設定 (IPv6 DNS / any)	
144 proxydns address 1 any dhcp ipv6 port-channel 2	proxyDNS 逆引き設定 (IPv6 DNS / any)	
145 !		
146 end		