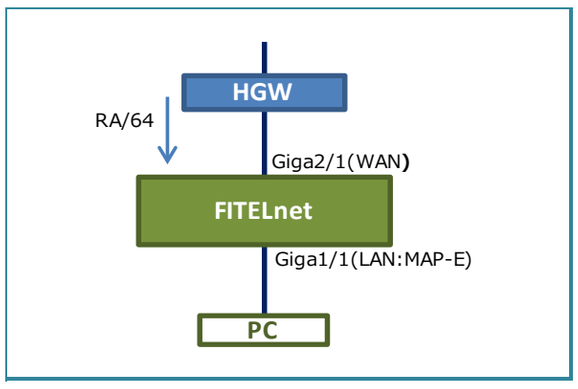
JPIX社「v6プラス」を利用するための設定例（MAP-E方式）

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

パターン2：HGWあり/ひかり電話なし	
受信IPv6 prefix	RA/64
WAN側 IPv6アドレス	linklocal
LAN側 IPv6アドレス	RA/64から生成
LAN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 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 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	access-list 4100 permit tcp any any eq 53	IPv6アクセスリスト（IPv6 TCP DNS／ポリシールーティング用）
34	access-list 4100 permit udp any any eq 53	IPv6アクセスリスト（IPv6 UDP DNS／ポリシールーティング用）
35	access-list 4101 permit tcp any ::1/128	IPv6アクセスリスト（IPv6 TCP loopback／ポリシールーティング用）
36	access-list 4101 permit udp any ::1/128	IPv6アクセスリスト（IPv6 UDP loopback／ポリシールーティング用）
37	!	
38	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）
39	ip name-server ::1	DNSサーバー設定（自装置をサーバーに設定）
40	!	
41	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。
42	!	
43	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）
44	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）
45	!	
46	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
47	!	
48	hostname FITELnet_MAPCE	hostname設定
49	!	
50	ip dhcp client-profile DHCPv4_client	DHCPv4クライアントプロファイル
51	retries infinity	DHCPメッセージの返信があるまで再送する設定
52	exit	
53	!	
54	ip dhcp server-profile DHCPv4_server	DHCPv4サーバープロファイル
55	address 192.168.100.2 192.168.100.254	配布アドレス設定
56	lease-time 259200	DHCPリース期間設定
57	dns 192.168.100.1	配布DNSサーバーアドレス設定
58	gateway 192.168.100.1	配布Gatewayアドレス設定
59	exit	
60	!	
61	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）
62	ip nat wellknown 1 1 65535 off	全ポートをNAT+変換する設定
63	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。
64	!	

	設定例	補足
65	ipv6 dhcp client-profile DHCPv6_client	DHCPv6クライアントプロファイル
66	option-request dns-server	DNSサーバー要求設定
67	option-request dns-server-domain	DNSサーバードメイン要求設定
68	retries infinity	DHCPメッセージの返信があるまで再送する設定
69	exit	
70	!	
71	ipv6 dhcp server-profile DHCPv6_server	DHCPv6サーバープロファイル
72	dns port-channel 2	WAN側で受信したDNSサーバを配布する設定
73	domain port-channel 2	WAN側で受信したドメイン名を配布する設定
74	exit	
75	!	
76	ipinip tunnel-profile MAPCE	MAPトンネルプロファイル
77	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
78	map rule-get	v6プラスのサービスを利用する設定
79	ipinip fragment pre	プリフラグメント設定
80	exit	
81	!	
82	interface GigaEthernet 1/1	物理インターフェース（LAN側）
83	vlan-id 1	vlan-id設定（ポートVLAN）
84	bridge-group 1	ブリッジグループ設定
85	channel-group 1	LAN側論理インタフェース（Port-channel）と紐付け
86	policy-route input DNS-POLICY	LAN側ポリシールーティング設定
87	exit	
88	!	
89	interface GigaEthernet 2/1	物理インターフェース（WAN側）
90	vlan-id 2	vlan-id設定（ポートVLAN）
91	bridge-group 2	ブリッジグループ設定
92	channel-group 2	WAN側論理インタフェース（Port-channel）と紐付け
93	ip access-group 100 in	IPv4アクセスリスト紐付け（DHCPv4）
94	ip access-group 111 out	IPv4アクセスリスト紐づけ
95	ip access-group 112 in	IPv4アクセスリスト紐づけ
96	ip access-group 113 out	IPv4アクセスリスト紐づけ
97	ip access-group 114 out	IPv4アクセスリスト紐づけ
98	ip access-group 115 in	IPv4アクセスリスト紐づけ
99	ip access-group spi ftp-data enable	学習フィルタ追加
100	ipv6 access-group 4000 in	IPv6アクセスリスト紐付け（NS/NA/RA/DHCPv6）
101	ipv6 access-group 4009 in	IPv6アクセスリスト紐付け（deny）
102	ipv6 access-group 4010 out	IPv6アクセスリスト紐付け（SPI）
103	exit	
104	!	
105	interface Port-channel 1	論理インターフェース（LAN側）
106	ip dhcp service server	DHCPv4サーバー設定
107	ip dhcp server-profile DHCPv4_server	DHCPv4サーバープロファイル紐付け
108	ip address 192.168.100.1 255.255.255.0	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 autoconfig	IPv6アドレス設定（RAからアドレス生成）
111	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）
112	ipv6 nd other-config-flag	RA Oフラグセット
113	ipv6 nd send-ra	RA送信設定
114	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 ＊RA送信側でプレフィックスの削除(lifetime=0)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、2時間よりも短い値はlifetimeに反映しません。 ※本設定はLAN側/WAN側の両方の論理インタフェースにて必要です。 ※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。
115	ipv6 dhcp service server	DHCPv6サーバー設定
116	ipv6 dhcp server-profile DHCPv6_server	DHCPv6サーバープロファイル紐付け
117	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。）
118	exit	
119	!	
120	interface Port-channel 2	論理インターフェース（WAN側）
121	ip dhcp service client	DHCPv4クライアント設定
122	ip dhcp client-profile DHCPv4_client	DHCPv4クライアントプロファイル紐付け
123	ipv6 enable	IPv6リンクローカルアドレス設定
124	ipv6 nd receive-ra prefix-delegation port-channel 1	RA-proxy設定
125	ipv6 router-lifetime-receive-enable	RA default経路登録設定
126	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 ＊論理インタフェース（LAN側）の補足欄に記載の通り、本設定を推奨します。 ※本設定はLAN側/WAN側の両方の論理インタフェースにて必要です。 ※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。
127	ipv6 dhcp service client	DHCPv6クライアント設定
128	ipv6 dhcp client-profile DHCPv6_client	DHCPv6クライアントプロファイル紐付け
129	exit	
130	!	
131	interface Tunnel 1	MAPトンネルインターフェース
132	ip access-group 109 in	IPv4アクセスリスト紐付け（deny）
133	ip access-group 110 out	IPv4アクセスリスト紐付け（SPI）
134	ip nat inside source list 1 map-encap overload	MAP用NAT+設定
135	tunnel mode ipinip tunnel-profile MAPCE	MAP用プロファイルと紐付け
136	exit	
137	!	

	設定例	補足
138	class-map DNS6	ポリシールーティング用class-map
139	match ipv6 access-group 4100	IPv6アクセスリスト紐付け（宛先ポート番号53：DNSサーバ宛）
140	exit	
141	!	
142	class-map DNS6_LO	ポリシールーティング用class-map
143	match ipv6 access-group 4101	IPv6アクセスリスト紐付け（宛先アドレス[::1/128]：自装置のloopback宛）
144	exit	
145	!	
146	policy-route-map DNS-POLICY	ポリシールーティング用のポリシー設定
147	!	
148	class DNS6	ポリシールーティング用のクラス設定（IPv6 DNSアクセス）
149	search-sequence 10	クラスの検索優先度を10に設定（DNS6_LOより検索優先度が低い）
150	count	クラスにマッチしたパケット数をカウントする設定
151	action nexthop ##ネクストホップアドレス(IPv6)##	クラスにマッチしたパケットのnexthopを設定：HGWでproxyDNSが動作している場合など、DNSサーバアドレスがRAで受信したプレフィックスに包含されるような場合に、本装置が送信するDNSサーバ宛パケットがLAN方向に送信されて、名前解決が行われなくなることを防ぐための設定です。 ※IPv6デフォルトルートに包含されるアドレスを設定してください。show ipv6 routeで表示される、デフォルトルート以外のプレフィックス（LAN側ネットワークアドレスなど）に包含されないアドレスであれば、問題ありません。
152	exit	
153	!	
154	class DNS6_LO	ポリシールーティング用のクラス設定（IPv6 loopbackアクセス）
155	search-sequence 1	クラスの検索優先度を1に設定（DNS6より検索優先度が高い）
156	count	クラスにマッチしたパケット数をカウントする設定
157	action transmit	クラスにマッチしたパケットを経路表に従って送信する設定
158	exit	
159	!	
160	exit	
161	!	
162	local policy-route DNS-POLICY	自発パケットのポリシールーティング設定
163	!	
164	dns-server ip enable	DNSv4サーバー設定
165	dns-server ipv6 enable	DNSv6サーバー設定
166	!	
167	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）
168	proxydns domain 2 any * any dhcp ipv6 port-channel 2 source-interface port-channel 1	proxyDNS 順引き設定（IPv6 DNS / any）
169	proxydns address 1 any dhcp ipv6 port-channel 2 source-interface port-channel 1	proxyDNS 逆引き設定（IPv6 DNS / any）
170	!	
171	end	