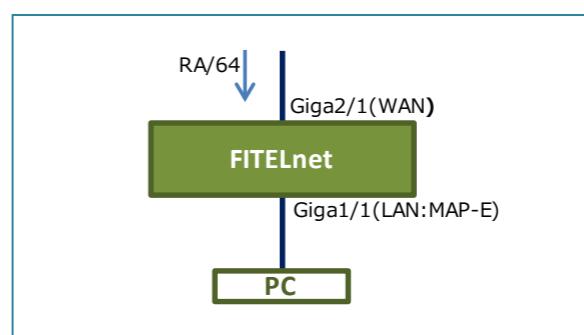


JPIX社「v6プラス」を利用するための設定例 (MAP-E方式)

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

パターン3 : HGWなし/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 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。
2 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。
3 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。
4 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。
5 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。
6 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。
7 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。
8 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。
9 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。
10 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。
11 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。
12 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。
13 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。
14 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。
15 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。
16 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。
17 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。
18 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。
19 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。
20 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。
21 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。
22 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。
23 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。
24 access-list 114 permit ip any any	全てのIPトラフィックを許可します。
25 access-list 115 deny ip any any	全てのIPトラフィックを拒否します。
26 access-list 4000 permit icmp6 any any neighbor-advertisement	IPv6アクセリスト (NA許可)
27 access-list 4000 permit icmp6 any any neighbor-solicitation	IPv6アクセリスト (NS許可)
28 access-list 4000 permit icmp6 any any router-advertisement	IPv6アクセリスト (RA許可)
29 access-list 4000 permit udp any any eq 546	IPv6アクセリスト (DHCPv6許可)
30 access-list 4009 deny ipv6 any any	IPv6アクセリスト (全拒否)
31 access-list 4010 spi ipv6 any any	IPv6アクセリスト (SPI)
32 !	
33 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)
34 ip name-server ::1	DNSサーバー設定 (自装置をサーバーに設定)
35 !	
36 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。
37 !	
38 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)
39 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)
40 !	
41 username guest password guest-secret	ログインユーザID名 (guest) とパスワード (guest-secret) の登録
42 !	
43 hostname FITELnet_MAPCE	hostname設定
44 !	
45 ip dhcp server-profile DHCPv4_server	DHCPv4サーバープロファイル
46 address 192.168.100.2 192.168.100.254	配布アドレス設定
47 lease-time 259200	DHCPリース期間設定
48 dns 192.168.100.1	配布DNSサーバーアドレス設定
49 gateway 192.168.100.1	配布Gatewayアドレス設定
50 exit	
51 !	
52 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)
53 ip nat wellknown 1 1 65535 off	全ポートをNAT+変換する設定
54 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。
55 !	
56 ipv6 dhcp client-profile DHCPv6_client	DHCPv6クライアントプロファイル
57 option-request dns-server	DNSサーバー要求設定
58 option-request dns-server-domain	DNSサーバードメイン要求設定
59 retries infinity	DHCPメッセージの返信があるまで再送する設定
60 exit	
61 !	
62 ipv6 dhcp server-profile DHCPv6_server	DHCPv6サーバープロファイル
63 dns port-channel 2	WAN側で受信したDNSサーバを配布する設定
64 domain port-channel 2	WAN側で受信したドメイン名を配布する設定
65 exit	
66 !	
67 ipinip tunnel-profile MAPCE	MAPトンネルプロファイル
68 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
69 map rule-get	v6プラスのサービスを利用する設定
70 ipinip fragment pre	プリフラグメント設定
71 exit	
72 !	
73 interface GigaEthernet 1/1	物理インターフェース (LAN側)
74 vlan-id 1	vlan-id設定 (ポートVLAN)
75 bridge-group 1	ブリッジグループ設定
76 channel-group 1	LAN側論理インターフェース (Port-channel) と紐付け
77 exit	

	設定例	補足
78 !		
79 interface GigaEthernet 2/1	物理インターフェース (WAN側)	
80 vlan-id 2	vlan-id設定 (ポートVLAN)	
81 bridge-group 2	ブリッジグループ設定	
82 channel-group 2	WAN側論理インターフェース (Port-channel) と紐付け	
83 ipv6 access-group 4000 in	IPv6アクセリスト紐付け (NS/NA/RA/DHCPv6)	
84 ipv6 access-group 4009 in	IPv6アクセリスト紐付け (deny)	
85 ipv6 access-group 4010 out	IPv6アクセリスト紐付け (SPI)	
86 exit		
87 !		
88 interface Port-channel 1	論理インターフェース (LAN側)	
89 ip dhcp service server	DHCPv4サーバー設定	
90 ip dhcp server-profile DHCPv4_server	DHCPv4サーバープロファイル紐付け	
91 ip address 192.168.100.1 255.255.255.0	IPv4アドレス設定	
92 ipv6 enable	IPv6リンクローカルアドレス設定	
93 ipv6 address autoconfig	IPv6アドレス設定 (RAからアドレス生成)	
94 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)	
95 ipv6 nd other-config-flag	RAフラグセット	
96 ipv6 nd send-ra	RA送信設定	
97 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いと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ー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。	
98 ipv6 dhcp service server	DHCPv6サーバー設定	
99 ipv6 dhcp server-profile DHCPv6_server	DHCPv6サーバープロファイル紐付け	
100 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。)	
101 exit		
102 !		
103 interface Port-channel 2	論理インターフェース (WAN側)	
104 ipv6 enable	IPv6リンクローカルアドレス設定	
105 ipv6 nd receive-ra prefix-delegation port-channel 1	RA-proxy設定	
106 ipv6 router-lifetime-receive-enable	RA default経路登録設定	
107 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 * 論理インターフェース (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ー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。	
108 ipv6 dhcp service client	DHCPv6クライアント設定	
109 ipv6 dhcp client-profile DHCPv6_client	DHCPv6クライアントプロファイル紐付け	
110 exit		
111 !		
112 interface Tunnel 1	MAPトンネルインターフェース	
113 ip access-group 111 out	IPv4アクセリスト紐づけ	
114 ip access-group 112 in	IPv4アクセリスト紐づけ	
115 ip access-group 113 out	IPv4アクセリスト紐づけ	
116 ip access-group 114 out	IPv4アクセリスト紐づけ	
117 ip access-group 115 in	IPv4アクセリスト紐づけ	
118 ip access-group spi ftp-data enable	学習フィルタ追加	
119 ip nat inside source list 1 map-encap overload	MAP用NAT+設定	
120 tunnel mode ipinip tunnel-profile MAPCE	MAP用プロファイルと紐付け	
121 exit		
122 !		
123 dns-server ip enable	DNSv4サーバー設定	
124 dns-server ipv6 enable	DNSv6サーバー設定	
125 !		
126 proxydns domain 1 any * any dhcp ipv6 port-channel 2 source-interface port-channel 1	proxyDNS 順引き設定 (any)	
127 proxydns address 1 any dhcp ipv6 port-channel 2 source-interface port-channel 1	proxyDNS 逆引き設定 (any)	
128 !		
129 end		