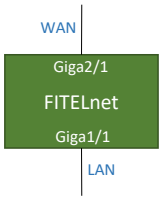
HB46PPによる国内標準方式を利用するための設定例

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

HGWあり/ひかり電話あり、HGWなし/ひかり電話なし、どちらも利用可



	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サーバ設定（自装置をサーバに設定）
40	!	
41	ip dhcp client-profile DHCPv4_client	WAN側DHCPv4クライアント設定
42	retries infinity	DHCPメッセージの応答があるまで再送する設定
43	exit	
44	!	
45	ip dhcp server-profile DHCPv4_server	LAN側DHCPv4サーバ設定
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	NAT+変換にて全ポート番号を変換対象とする設定
54	!	
55	ipv6 dhcp client-profile DHCPv6_client	WAN側DHCPv6クライアント設定
56	option-request dns-server	DNSサーバ要求設定
57	option-request dns-server-domain	DNSサーバドメイン要求設定
58	option-request sntp-server	SNTPサーバ要求設定
59	retries infinity	DHCPメッセージの応答があるまで再送する設定
60	exit	
61	!	

	設定例	補足
62	ipv6 dhcp server-profile DHCPv6_server	LAN側DHCPv6サーバ設定
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 46PP	IPinIPトンネルプロファイル
68	profile-mode 46pp	トンネルのプロファイルモードを指定（46pp：HB46PPに対応）
69	ipinip fragment pre	プリフラグメント指定
70	set 46pp capability ipip	プロビジョニングサーバに送信するcapabilityを指定（IPIPトンネル）
71	set 46pp username ##ユーザ名## password ##パスワード##	ユーザ名、パスワードを設定 ★ユーザ名とパスワードはVNE各社の指定に合わせて設定してください。 VNEによっては、本設定は不要です。
72	exit	
73	!	
74	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。
75	!	
76	aaa authentication login default local login	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）
77	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）
78	!	
79	sntp server dhcp port-channel 2	NTPサーバもしくはSNTPサーバを指定 ※お客様の環境に合わせて設定してください。本設定例ではDHCPで取得した SNTPサーバを指定しています。 NTPサーバ指定の場合は ntp server コマンドを設定ください。
80	!	
81	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
82	!	
83	hostname FITELnet	hostname設定
84	!	
85	interface GigaEthernet 1/1	物理インターフェース（LAN側）
86	vlan-id 1	vlan-id設定（ポートVLAN）
87	bridge-group 1	ブリッジグループ設定
88	channel-group 1	LAN側論理インタフェース（Port-channel）と紐付け
89	policy-route input DNS-POLICY	LAN側ポリシールーティング設定
90	exit	
91	!	
92	interface GigaEthernet 2/1	物理インターフェース（WAN側）
93	vlan-id 2	vlan-id設定（ポートVLAN）
94	bridge-group 2	ブリッジグループ設定
95	channel-group 2	WAN側論理インタフェース（Port-channel）と紐付け
96	ip access-group 100 in	IPアクセスリスト紐付け（DHCPv4）
97	ip access-group 111 out	IPv4アクセスリスト紐づけ
98	ip access-group 112 in	IPv4アクセスリスト紐づけ
99	ip access-group 113 out	IPv4アクセスリスト紐づけ
100	ip access-group 114 out	IPv4アクセスリスト紐づけ
101	ip access-group 115 in	IPv4アクセスリスト紐づけ
102	ip access-group spi ftp-data enable	学習フィルタ追加
103	ipv6 access-group 4000 in	IPv6アクセスリスト紐付け（NS/NA/RA/DHCPv6）
104	ipv6 access-group 4009 in	IPv6アクセスリスト紐付け（deny）
105	ipv6 access-group 4010 out	IPv6アクセスリスト紐付け（SPI）
106	exit	
107	!	
108	interface Port-channel 1	論理インターフェース（LAN側）
109	ip dhcp service server	DHCPv4サーバ設定
110	ip dhcp server-profile DHCPv4_server	DHCPv4サーバプロファイル紐付け
111	ip address 192.168.100.1 255.255.255.0	IPv4アドレス設定
112	ipv6 enable	IPv6リンクローカルアドレス設定
113	ipv6 address autoconfig	IPv6アドレス設定（RAからアドレス生成）
114	ipv6 address autoconfig-46pp 46PP	IPv6アドレス設定（RAからHB46PP用アドレス生成）
115	ipv6 nd other-config-flag	RA Oフラグセット
116	ipv6 nd send-ra	RA送信設定
117	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。デフォルトでは、サービス否認攻撃回避のため、2時間よりも短い値はlifetimeに反映しません。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。 ※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。
118	ipv6 dhcp service server	DHCPv6サーバ設定
119	ipv6 dhcp server-profile DHCPv6_server	DHCPv6サーバプロファイル紐付け
120	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 ＊装置起動時にリンクダウンしているとMAPルール取得に失敗するため、本設定を推奨します。
121	exit	

	設定例	補足
122	!	
123	interface Port-channel 2	論理インターフェース（WAN側）
124	ip dhcp service client	DHCPv4クライアント設定
125	ip dhcp client-profile DHCPv4_client	DHCPv4クライアントプロファイル紐付け
126	ipv6 enable	IPv6リンクローカルアドレス設定
127	ipv6 nd receive-ra prefix-delegation port-channel 1	RA-proxy設定
128	ipv6 router-lifetime-receive-enable	RA default経路登録設定
129	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。
130	ipv6 dhcp service client	DHCPv6クライアント設定
131	ipv6 dhcp client-profile DHCPv6_client	DHCPv6クライアントプロファイル紐付け
132	exit	
133	!	
134	interface Tunnel 1	HB46PPトンネルインターフェース
135	ip access-group 111 out	IPv4アクセスリスト紐づけ
136	ip access-group 112 in	IPv4アクセスリスト紐づけ
137	ip access-group 113 out	IPv4アクセスリスト紐づけ
138	ip access-group 114 out	IPv4アクセスリスト紐づけ
139	ip access-group 115 in	IPv4アクセスリスト紐づけ
140	ip access-group spi ftp-data enable	学習フィルタ追加
141	ip nat inside source list 1 46pp overload	HB46PP用NAT+設定
142	tunnel mode ipinip tunnel-profile 46PP	IPinIPトンネルプロファイル（46PP）と紐付け
143	exit	
144	!	
145	line console	Consoleアクセス設定 ※本設定モードは、お客様の環境に合わせて設定ください。
146	exec-timeout 0	自動ログアウト時間(分) ＊"0"指定時は自動ログアウトしません。
147	authorization exec default local	Consoleログイン時の許可方式を指定 local: usernameコマンドで設定した特権レベルでログイン許可
148	exit	
149	!	
150	line telnet	SSH/TELNETアクセス設定 ※本設定モードは、お客様の環境に合わせて設定ください。
151	exec-timeout 0	自動ログアウト時間(分) ＊"0"指定時は自動ログアウトしません。
152	exit	
153	!	
154	class-map DNS6	ポリシールーティング用class-map
155	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）
156	exit	
157	!	
158	class-map DNS6_LO	ポリシールーティング用class-map
159	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）
160	exit	
161	!	
162	policy-route-map DNS-POLICY	ポリシールーティング用のポリシー設定
163	!	
164	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）
165	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）
166	count	クラスにマッチしたパケット数をカウントする設定
167	action nexthop 2001:db8::1	クラスにマッチしたパケットのnexthopを設定（2001:db8::1）： ★IPv6 Documentation Prefixの範囲（2001:db8::/32）のアドレスを指定してください。 ※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。このため、IPv6デフォルトルートに包含されるアドレスを指定する必要があります。
168	exit	
169	!	
170	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）
171	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）
172	count	クラスにマッチしたパケット数をカウントする設定
173	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
174	exit	
175	!	
176	exit	
177	!	
178	local policy-route DNS-POLICY	自発パケットのポリシールーティング設定
179	!	
180	dns-server ip enable	DNSv4サーバ設定
181	dns-server ipv6 enable	DNSv6サーバ設定
182	!	
183	proxydns domain 1 any * any dhcp ipv6 port-channel 2 source-interface port-channel 1	proxyDNS 順引き設定（IPv6 DNS / any）
184	proxydns address 1 any dhcp ipv6 port-channel 2 source-interface port-channel 1	proxyDNS 逆引き設定（IPv6 DNS / any）
185	!	
186	end	