

## NTTコミュニケーションズ社「OCNバーチャルコネクタサービス（IPoE）」を利用するための設定例

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

## ケース3：固定IP8



※ログインID/Passwordは“test”/“test”です。

設定例	補足
1 access-list 100 permit ip any host 192.0.2.2	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 192.0.2.3	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 192.0.2.4	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 192.0.2.5	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（全拒否）
35 access-list 4010 spi ipv6 any any	IPv6アクセスリスト（SPI）
36 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）
37 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）
38 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）
39 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）
40 !	
41 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）
42 ip name-server ::1	DNSサーバ設定（自装置をサーバに設定）
43 !	
44 ip dhcp server-profile DHCPv4_server	LAN側DHCPv4サーバ設定（プライベートアドレスをLANに配布）
45 address 192.168.100.2 192.168.100.254	配布アドレス設定
46 lease-time 259200	DHCPリース期間設定
47 dns 192.168.100.1	配布DNSサーバアドレス設定
48 gateway 192.168.100.1	配布Gatewayアドレス設定
49 exit	
50 !	
51 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）
52 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
53 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。
54 !	

	設定例	補足
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	retries infinity	DHCPメッセージの応答があるまで再送する設定
59	exit	
60	!	
61	ipv6 dhcp server-profile DHCPv6_server	LAN側DHCPv6サーバ設定
62	dns port-channel 20	WAN側で受信したDNSサーバを配布する設定
63	domain port-channel 20	WAN側で受信したドメイン名を配布する設定
64	exit	
65	!	
66	event-action 1	イベントアクション設定 (HGWのSPIフィルタエントリ対策用)
67	event-condition match-all	イベント発生判定のマッチタイプを設定 * 本設定モードのイベントがすべて発生したときにアクションを実施します。
68	event interface tunnel 1 up	イベント監視 (interface tunnel 1 up)
69	event timer countdown 180 replay	イベント監視 (180秒毎のカウントダウンタイマー)
70	action 1.1 cli exec command ping ##宛先IPアドレス## source 192.168.100.1 repeat 1	イベント発生時のアクション設定: HGWのSPIエントリの消去を防ぐための設定 * BRから送信されたパケットのHGWでの破棄を防ぐために、本設定を推奨します。 * interface tunnel 1がupしている場合、180秒に1回、##宛先IPアドレス##に対して、192.168.100.1 (LAN側インタフェースのアドレス)を送信元アドレスとしてPingを送信します。 ※##宛先IPアドレス##はお客様の環境に合わせて設定ください。
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-c	トンネルのプロファイルモードを指定
75	map rule-get	MAPルール取得設定
76	ipinip fragment pre	ブリフラグメント指定
77	exit	
78	!	
79	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。
80	!	
81	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)
82	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口許可方式を指定 (username コマンドで登録した特権レベルとする)
83	!	
84	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
85	!	
86	hostname FTELnet	hostname設定
87	!	
88	interface GigaEthernet 1/1	物理インターフェース (LAN側)
89	vlan-id 11	vlan-id設定 (ポートVLAN)
90	bridge-group 11	ブリッジグループ設定
91	channel-group 11	LAN側論理インタフェース (Port-channel) と紐付け
92	policy-route input DNS-POLICY	LAN側ポリシールーティング設定
93	exit	
94	!	
95	interface GigaEthernet 1/2	物理インターフェース (LAN側)
96	vlan-id 12	vlan-id設定 (ポートVLAN)
97	bridge-group 12	ブリッジグループ設定
98	channel-group 12	LAN側論理インタフェース (Port-channel) と紐付け
99	exit	
100	!	
101	interface GigaEthernet 2/1	物理インターフェース (WAN側)
102	vlan-id 20	vlan-id設定 (ポートVLAN)
103	bridge-group 20	ブリッジグループ設定
104	channel-group 20	WAN側論理インタフェース (Port-channel) と紐付け
105	ipv6 access-group 4000 in	IPv6アクセスリスト紐付け (NS/NA/RA/DHCPv6)
106	ipv6 access-group 4009 in	IPv6アクセスリスト紐付け (deny)
107	ipv6 access-group 4010 out	IPv6アクセスリスト紐付け (SPI)
108	ipv6 access-group spi ftp-data enable	ダイナミックフィルタリング (FTP)
109	exit	
110	!	

	設定例	補足
111	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に割り当ててはできません。
112	ip dhcp service server	DHCPv4サーバ設定
113	ip dhcp server-profile DHCPv4_server	DHCPv4サーバプロファイル紐付け
114	ip address 192.168.100.1 255.255.255.0	IPv4アドレス設定
115	ipv6 enable	IPv6リンクローカルアドレス設定
116	ipv6 address autoconfig	IPv6アドレス設定（RAからアドレス生成）
117	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）
118	ipv6 nd other-config-flag	RA 0フラグセット
119	ipv6 nd send-ra	RA送信設定
120	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ーフェースにて必要です。
121	ipv6 dhcp service server	DHCPv6サーバ設定
122	ipv6 dhcp server-profile DHCPv6_server	DHCPv6サーバプロファイル紐付け
123	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。）
124	link-state always-up	本論理インター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ためMAPルール取得に失敗するため、本設定を推奨します。
125	exit	
126	!	
127	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
128	ip address 192.0.2.6 255.255.255.248	IPv4アドレス設定 ※固定IP8で払い出されたアドレスを、お客様の環境に合わせて設定してください。
129	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。）
130	exit	
131	!	
132	interface Port-channel 20	論理インターフェース（WAN側）
133	ipv6 enable	IPv6リンクローカルアドレス設定
134	ipv6 nd receive-ra prefix-delegation port-channel 11	RA-proxy設定
135	ipv6 router-lifetime-receive-enable	RA default経路登録設定
136	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。
137	ipv6 dhcp service client	DHCPv6クライアント設定
138	ipv6 dhcp client-profile DHCPv6_client	DHCPv6クライアントプロファイル紐付け
139	exit	
140	!	
141	interface Tunnel 1	MAPトンネルインターフェース
142	ip access-group 100 in	IPv4アクセスリスト紐付け（permit）
143	ip access-group 111 out	IPv4アクセスリスト紐づけ
144	ip access-group 112 in	IPv4アクセスリスト紐づけ
145	ip access-group 113 out	IPv4アクセスリスト紐づけ
146	ip access-group 114 out	IPv4アクセスリスト紐づけ
147	ip access-group 115 in	IPv4アクセスリスト紐づけ
148	ip access-group spi ftp-data enable	学習フィルタ追加
149	ip access-group spi ftp-data enable	ダイナミックフィルタリング（FTP）
150	ip nat inside source list 1 map-encap overload	MAP用NAT+設定
151	tunnel mode ipinip tunnel-profile MAPCE	MAP用プロファイルと紐付け
152	exit	
153	!	
154	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。
155	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。
156	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
157	exit	
158	!	
159	line telnet	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。
160	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。
161	exit	
162	!	

	設定例	補足
163	class-map DNS6	ポリシールーティング用class-map
164	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）
165	exit	
166	!	
167	class-map DNS6_LO	ポリシールーティング用class-map
168	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）
169	exit	
170	!	
171	policy-route-map DNS-POLICY	ポリシールーティング用のポリシー設定
172	!	
173	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）
174	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）
175	count	クラスにマッチしたパケット数をカウントする設定
176	action nexthop ##ネクストホップアドレス (IPv6) ##	<p>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含まれるような場合に、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。</p> <p>※IPv6デフォルトルートに含ま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）に含まれないアドレスであれば、問題ありません。</p>
177	exit	
178	!	
179	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）
180	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）
181	count	クラスにマッチしたパケット数をカウントする設定
182	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
183	exit	
184	!	
185	exit	
186	!	
187	local policy-route DNS-POLICY	自発パケットのポリシールーティング設定
188	!	
189	dns-server ip enable	DNSv4サーバ設定
190	dns-server ipv6 enable	DNSv6サーバ設定
191	!	
192	proxydns domain 1 any * any dhcp ipv6 port-channel 20 source-interface port-channel 11	proxyDNS 順引き設定（any）
193	proxydns address 1 any dhcp ipv6 port-channel 20 source-interface port-channel 11	proxyDNS 逆引き設定（any）
194	!	
195	end	