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

	EAP-MSCHAPv2 Local認証 設定例	補足
1	access-list 100 permit udp any host 10.0.0.1 eq 500	
2	access-list 100 permit udp any host 10.0.0.1 eq 4500	
3	access-list 100 permit icmp any host 10.0.0.1	
4	access-list 100 permit 50 any host 10.0.0.1	
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	!	
31	ip route 0.0.0.0 0.0.0.0 192.168.0.254	
32	ip route 192.168.1.0 255.255.255.0 null 0	払い出しアドレスを包含するnull経路（ /24 ） ※払い出しアドレスを包含するStatic経路（ /24 ）をデフォルトゲートウェイに設定する前提（ ループ防止 ） ※SA確立時に払い出されるアドレス宛て以外のパケットを廃棄します。
33	ip local pool POOL1 192.168.1.1 192.168.1.254	アドレスプール設定 ※Configuration Payloadによる払い出しアドレスのレンジを指定
34	!	
35	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。
36	!	
37	aaa authentication login default local	本装置にログインする口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）
38	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）
39	!	
40	username guest password guest-secret	ログインユーザ口名（guest）とパスワード口口(guest-secret）の登録
41	!	
42	aaa authentication ike-client AUTH1 local-group LOCAL1	拡張認証方法を指定（ Local認証 ）
43	aaa authorization network CP1 local-group CONFIG1	アドレス払い出し方法を指定
44	!	
45	aaa local group LOCAL1	拡張認証用ローカルデータベース設定
46	username user1 password pass1	EAPのID/Passwordを指定
47	username user2 password pass2	
48	exit	
49	!	
50	ntp server A.B.C.D	NTPサーバと時刻同期する設定 ★お客様の環境に合わせて設定お願いします。
51	!	
52	hostname IPsecGW	hostname指定
53	!	
54	crypto ipsec udp-encapsulation nat-t keepalive interval 60	NAT-T有効化
55	!	
56	crypto ipsec policy IPsec_POLICY	IPsecポリシー設定（ Phase2 SAのパラメータを指定 ）
57	set security-association lifetime seconds 3600	Lifetime(秒)を指定
58	set security-association transform-keysize aes 128 256 256	暗号化アルゴリズム（ AES ）の鍵サイズを指定 ※受け入れ可能な鍵サイズの最小値、最大値、Initiator提案時の最優先値
59	set security-association transform esp-aes esp-sha-hmac	暗号化アルゴリズム（ AES ）とハッシュアルゴリズム（ SHA1 ）を指定
60	set mtu 1500	暗号化後のMTU値を指定（ default: 1500 Bytes ） ★お客様の環境に合わせて設定お願いします。
61	set mss 1360	MSS値を指定　★お客様の環境に合わせて設定お願いします。
62	set ip df-bit 0	ESPパケットのDFビットを"0"に設定
63	set ip fragment post	ポストフラグメント指定
64	sa-up route	SA-UP経路設定 ※Configuration Payloadによる払い出しアドレス宛ての経路を登録します。
65	exit	
66	!	
67	crypto ipsec selector SELECTOR	セレクタ設定
68	src 1 ipv4 any	送信元セレクタ(v4)を指定
69	src 2 ipv6 any	送信元セレクタ(v6)を指定
70	dst 1 ipv4 any	宛先セレクタ(v4)を指定
71	dst 2 ipv6 any	宛先セレクタ(v6)を指定
72	exit	
73	!	
74	crypto isakmp keepalive interval 30	通信が無い場合に、DPDメッセージを30秒間隔で送信
75	crypto isakmp log sa detail	SYSLOGにSA確立・切断のログを出力
76	crypto isakmp log session detail	SYSLOGにSession確立・切断のログを出力 ※IKE SA, CHILD SA両方確立時にSession確立、どちらも削除された際にSession切断となります。
77	crypto isakmp log negotiation-fail detail	SYSLOGにIKEネゴシエーション失敗のログを出力
78	crypto isakmp tunnel-route ip address 10.0.0.2	SA確立時にリモート側IPsec終端アドレス宛ての経路を指定したnexthopで登録

	EAP-MSCHAPv2 Local認証 設定例	補足
79	!	
80	crypto isakmp client configuration group CONFIG1	Configuration Payloadによる払い出し設定
81	pool POOL1	アドレスプール指定
82	exit	
83	!	
84	crypto isakmp policy ISAKMP_POLICY	ISAKMPポリシー設定(Phase1 SAのパラメータを指定)
85	authentication rsa-sig	RSA認証を指定
86	encryption aes	暗号化アルゴリズムを指定(AES)
87	encryption-keysize aes 128 256 256	暗号化アルゴリズム(AES)の鍵サイズを指定 ※受け入れ可能な鍵サイズの最小値、最大値、Initiator提案時の最優先値
88	group 2 5 14 15	DHグループを指定(2, 5, 14, 15)
89	lifetime 86400	Lifetime(秒)を指定
90	hash sha sha-256 sha-384 sha-512	ハッシュアルゴリズムを指定(SHA1, SHA2-256, 384, 512)
91	exit	
92	!	
93	crypto isakmp profile PROF1	ISAKMPプロファイル設定
94	local-address 10.0.0.1	ローカル側のIPsec終端アドレスを指定
95	self-identity fqdn IPsecGW.example.com	ローカル側のIKE IDを指定(FQDN) 自装置の証明書に含まれる"Subject Alternative Name"と一致している必要があります。 ※Windows端末と接続する場合は"Common Name"とも一致させて下さい。
96	set isakmp-policy ISAKMP_POLICY	ISAKMPポリシーを指定
97	set ipsec-policy IPsec_POLICY	IPsecポリシーを指定
98	ca trustpoint CA1	CA証明書名を指定
99	client authentication list AUTH1	拡張認証方法を指定
100	client authentication type eap-mschapv2	認証方式にEAP MS-CHAPv2を指定
101	client authentication eap-identity request	認証時にEAP IDを要求
102	client configuration address respond	Configuration Payloadによるアドレス払い出し方法を指定(Request/Reply方式)
103	isakmp authorization list CP1	Configuration Payloadによる払い出し情報を指定
104	pki revocation-check none	証明書失効リストチェックの無効化 ※CRLを取得する場合は"crl"、または"crl none"を指定して下さい。
105	exit	
106	!	
107	crypto session identification address	リモート側のIPアドレスでセッションを識別します。
108	!	
109	crypto map MAP1 ipsec-isakmp dynamic	CRYPTOマップ設定
110	match address SELECTOR	セレクタを指定
111	set isakmp-profile PROF1	ISAKMPプロファイルと紐付け
112	exit	
113	!	
114	interface GigaEthernet 1/1	
115	vlan-id 2	
116	bridge-group 2	
117	channel-group 2	
118	exit	
119	!	
120	interface GigaEthernet 2/1	
121	vlan-id 1	
122	bridge-group 1	
123	channel-group 1	
124	ip access-group 100 in	
125	ip access-group 111 out	
126	ip access-group 112 in	
127	ip access-group 113 out	
128	ip access-group 114 out	
129	ip access-group 115 in	
130	ip access-group spi ftp-data enable	
131	exit	
132	!	
133	interface Port-channel 1	
134	ip address 10.0.0.1 255.255.255.252	
135	mtu 1500	MTU値を指定★お客様の環境に合わせて設定お願いします。
136	mss 1360	MSS値を指定★お客様の環境に合わせて設定お願いします。
137	exit	
138	!	
139	interface Port-channel 2	
140	ip address 192.168.0.1 255.255.255.0	
141	mtu 1500	MTU値を指定★お客様の環境に合わせて設定お願いします。
142	mss 1360	MSS値を指定★お客様の環境に合わせて設定お願いします。
143	exit	