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

	EAP-MSCHAPv2 Local認証 設定例	補足
1	access-list 111 permit udp any host 10.0.0.1 eq 500	
2	access-list 111 permit udp any host 10.0.0.1 eq 4500	
3	access-list 111 permit icmp any host 10.0.0.1	
4	access-list 111 permit 50 any host 10.0.0.1	
5	access-list 121 spi ip any any	
6	!	
7	ip route 0.0.0.0 0.0.0.0 192.168.0.254	
8	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。
9	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
10	!	
11	logging buffer level informational	装置内部バッファへ出力するログレベルを指定 ※"show logging buffer"で確認可能 ※IPsecのログを出力する場合は"informational"を指定
12	!	
13	aaa authentication ike-client AUTH1 local-group LOCAL1	拡張認証方法を指定(Local認証)
14	aaa authorization network CP1 local-group CONFIG1	アドレス払い出し方法を指定
15	!	
16	aaa local group LOCAL1	拡張認証用ローカルデータベース設定
17	username user1 password pass1	EAPのID/Passwordを指定
18	username user2 password pass2	
19	exit	
20	!	
21	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。
22	!	
23	hostname IPsecGW	hostname指定
24	!	
25	crypto ipsec udp-encapsulation nat-t keepalive interval 60	NAT-T有効化
26	!	
27	crypto ipsec policy IPsec_POLICY	IPsecポリシー設定(Phase2 SAのパラメータを指定)
28	set security-association lifetime seconds 3600	Lifetime(秒)を指定
29	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
30	set security-association transform esp-aes esp-sha-hmac esp-sha256-hmac	暗号化アルゴリズム(AES)とハッシュアルゴリズム(SHA1,SHA256)を指定
31	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。
32	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。
33	set ip df-bit 0	ESPパケットのDFビットを"0"に設定
34	set ip fragment post	ポストフラグメント指定
35	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。
36	exit	
37	!	
38	crypto ipsec selector SELECTOR	セレクタ設定
39	src 1 ipv4 any	送信元セレクタ(v4)を指定
40	src 2 ipv6 any	送信元セレクタ(v6)を指定
41	dst 1 ipv4 any	宛先セレクタ(v4)を指定
42	dst 2 ipv6 any	宛先セレクタ(v6)を指定
43	exit	
44	!	
45	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
46	crypto isakmp log sa detail	SYSLOGにSA確立・切断のログを出力
47	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。
48	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
49	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
50	!	
51	crypto isakmp client configuration group CONFIG1	Configuration Payloadによる払い出し設定
52	pool POOL1	アドレスプール指定
53	exit	
54	!	
55	crypto isakmp policy ISAKMP_POLICY	ISAKMPポリシー設定(Phase1 SAのパラメータを指定)
56	authentication rsa-sig	RSA認証を指定
57	encryption aes	暗号化アルゴリズムを指定(AES)
58	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
59	group 2 5 14 15	DHグループを指定(2, 5, 14, 15)
60	lifetime 86400	Lifetime(秒)を指定
61	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)
62	exit	
63	!	
64	crypto isakmp profile PROF1	ISAKMPプロファイル設定
65	local-address 10.0.0.1	ローカル側のIPsec終端アドレスを指定
66	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。
67	set isakmp-policy ISAKMP_POLICY	ISAKMPポリシーを指定
68	set ipsec-policy IPsec_POLICY	IPsecポリシーを指定
69	ca trustpoint CA1	CA証明書名を指定
70	client authentication list AUTH1	拡張認証方法を指定
71	client authentication type eap-mschapv2	認証方式にEAP MS-CHAPv2を指定
72	client authentication eap-identity request	認証時にEAP IDを要求
73	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)
74	isakmp authorization list CP1	Configuration Payloadによる払い出し情報を指定
75	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。
76	exit	

	EAP-MSCHAPv2 Local認証 設定例	補足
77	!	
78	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。
79	!	
80	crypto map MAP1 ipsec-isakmp dynamic	CRYPTOマップ設定
81	match address SELECTOR	セレクタを指定
82	set isakmp-profile PROF1	ISAKMPプロファイルと紐付け
83	exit	
84	!	
85	interface GigaEthernet 1/1	
86	vlan-id 2	
87	bridge-group 2	
88	channel-group 2	
89	exit	
90	!	
91	interface GigaEthernet 2/1	
92	vlan-id 1	
93	bridge-group 1	
94	channel-group 1	
95	ip access-group 111 in	
96	ip access-group 121 out	
97	exit	
98	!	
99	interface Port-channel 1	
100	ip address 10.0.0.1 255.255.255.252	
101	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。
102	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。
103	exit	
104	!	
105	interface Port-channel 2	
106	ip address 192.168.0.1 255.255.255.0	
107	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。
108	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。
109	exit	