設定例

ローカルブレイクアウト（LBO）：Windows Update / Microsoft Update
対象装置：FITELnet F70/F71/F220/F221/F225/F310/F220 EX/F221 EX

パラメータ設定例

ISAKMPポリシー

IKEバージョン	1
モード	Aggressiveモード
認証方式	事前共有鍵方式
暗号化方式	AES 256ビット
ハッシュ方式	SHA-256
Diffie-Hellman	Group 14
ライフタイム	86400秒

IPSECポリシー

PFS	Group 14
暗号化方式	AES 256ビット
ハッシュ方式	SHA-256
ライフタイム	28800秒
フラグメント	ポストフラグメント

コマンド設定例

センタ側FITELnetの設定

	設定例	補足
1	access-list 100 permit udp any eq 500 192.0.2.1 0.0.0.0 eq 500	VPNで使用するパケットを受信許可するフィルタリングの設定
2	access-list 100 permit 50 any 192.0.2.1 0.0.0.0	VPNで使用するパケットを受信許可するフィルタリングの設定
3	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。
4	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。
5	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。
6	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。
7	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。
8	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。
9	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。
10	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。
11	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。
12	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。
13	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。
14	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。
15	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。
16	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。
17	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。
18	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。
19	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。
20	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。
21	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。
22	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。
23	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。
24	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。
25	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。
26	access-list 114 permit ip any any	全てのIPトラフィックを許可します。
27	access-list 115 deny ip any any	全てのIPトラフィックを拒否します。
28	!	
29	ip route 0.0.0.0 0.0.0.0 192.168.0.1	Default経路(FW経由)
30	ip route 192.168.1.0 255.255.255.0 tunnel 2	拠点LAN宛てStatic経路(IPsec Tunnel経由)
31	ip route 192.168.1.0 255.255.255.0 null 0 250	IPsec Tunnelダウン時に拠点LAN宛てパケットを破棄する設定
32	!	
33	hostname CENTER	
34	!	
35	crypto ipsec policy P2-POLICY	IPSECポリシーの設定
36	set pfs group14	
37	set security-association lifetime seconds 28800	
38	set security-association transform-keysize aes 256 256 256	
39	set security-association transform esp-aes esp-sha256-hmac	
40	set mtu 1454	
41	set ip df-bit 0	
42	set ip fragment post	
43	exit	
44	!	
45	crypto ipsec selector SELECTOR	VPNセレクタの設定
46	src 1 ipv4 any	
47	dst 1 ipv4 any	
48	exit	
49	!	

	設定例	補足
50	crypto isakmp keepalive	KeepAlive機能として使用するDPDの設定
51	logging level informational	VPN通信動作中の詳細なログを残す設定
52	crypto isakmp log sa	
53	crypto isakmp log session	
54	crypto isakmp log negotiation-fail	
55	crypto isakmp tunnel-route ip interface tunnel 1	VPNピアへの経路情報をTunnel 1向けに登録する設定(トンネルルート機能)
56	!	
57	crypto isakmp policy P1-POLICY	ISAKMP ポリシーの設定
58	authentication pre-share	
59	encryption aes	
60	encryption-keysize aes 256 256 256	
61	group 14	
62	lifetime 86400	
63	hash sha-256	
64	initiate-mode aggressive	
65	exit	
66	!	
67	crypto isakmp profile PROF0001	ISAKMPプロファイルの設定
68	match identity user id-kyoten	
69	local-address 192.0.2.1	
70	set isakmp-policy P1-POLICY	
71	set ipsec-policy P2-POLICY	
72	ike-version 1	
73	local-key SECRET-VPN	
74	exit	
75	!	
76	crypto map KYOTEN ipsec-isakmp	拠点のVPNピアとのセレクタ情報のエントリー
77	match address SELECTOR	
78	set isakmp-profile PROF0001	
79	exit	
80	!	
81	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。
82	!	
83	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）
84	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）
85	!	
86	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
87	!	
88	hostname FITELnet	hostname設定
89	!	
90	!	
91	interface GigaEthernet 1/1	GigaEthernet インタフェースに、port-channel をリンク付け
92	vlan-id 1	
93	bridge-group 1	
94	channel-group 1	
95	exit	
96	!	
97	interface GigaEthernet 2/1	PPPoE 通信で使用する物理インタフェースの設定
98	vlan-id 2	
99	bridge-group 2	
100	pppoe enable	
101	exit	
102	!	
103	interface Port-channel 1	Port-channel にLAN側IPアドレスを設定
104	ip address 192.168.0.254 255.255.255.0	
105	mss 1300	
106	exit	
107	!	
108	interface Tunnel 1	Tunnel インタフェース（PPPoE）の設定
109	description FLETS	
110	ip address 192.0.2.1　255.255.255.255	
111	ip access-group 100 in	
112	ip access-group 111 out	IPv4アクセスリスト紐づけ
113	ip access-group 112 in	IPv4アクセスリスト紐づけ
114	ip access-group 113 out	IPv4アクセスリスト紐づけ
115	ip access-group 114 out	IPv4アクセスリスト紐づけ
116	ip access-group 115 in	IPv4アクセスリスト紐づけ
117	ip access-group spi ftp-data enable	学習フィルタ追加
118	tunnel mode pppoe profile PPPOE_PROF	
119	pppoe interface gigaethernet 2/1	
120	exit	
121	!	Tunnel インタフェース（IPsec）の設定
122	interface Tunnel 2	
123	tunnel mode ipsec map KYOTEN	
124	link-state sync-sa	
125	exit	
126	!	
127	pppoe profile PPPOE_PROF	PPPoEの設定
128	account abc012@***.***.ne.jp xxxyyyzzz	
129	exit	
130	!	
131	end	

拠点側FITELnetの設定

黄色セル:LBO機能、もしくは上記構成にてLBO機能を利用するために必要な設定です。
赤色セル:Windows Update / Microsoft Update をLBOするために必要な設定です。

	設定例	補足
1	access-list 100 permit udp 192.0.2.1 0.0.0.0 eq 500 any eq 500	VPNで使用するパケットを受信許可するフィルタリングの設定
2	access-list 100 permit 50 192.0.2.1 0.0.0.0 any	VPNで使用するパケットを受信許可するフィルタリングの設定
3	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。
4	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。
5	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。
6	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。
7	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。
8	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。
9	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。
10	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。
11	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。
12	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。
13	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。
14	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。
15	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。
16	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。
17	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。
18	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。
19	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。
20	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。
21	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。
22	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。
23	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。
24	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。
25	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。
26	access-list 114 permit ip any any	全てのIPトラフィックを許可します。
27	access-list 115 deny ip any any	全てのIPトラフィックを拒否します。
28	!	
29	ip route 192.0.2.1 255.255.255.255 tunnel 1	センタPPPoEIFへの経路(PPPoE経由)
30	ip route 0.0.0.0 0.0.0.0 tunnel 2	Default経路(IPsec Tunnel経由)
31	ip nat list 1 192.168.1.0 0.0.0.255	NATの設定
32	!	
33	ip dhcp server-profile lan1	DHCP サーバ機能を利用する設定
34	address 192.168.1.1 192.168.1.200	配布IPアドレスの範囲
35	lease-time 28800	DHCPリース期間(秒)
36	dns 192.168.0.100	プライマリDNSサーバIPアドレス
37	gateway 192.168.1.254	デフォルトルータのIPアドレス
38	exit	
39	!	
40	crypto ipsec policy P2-POLICY	IPSECポリシーの設定
41	set pfs group14	
42	set security-association always-up	
43	set security-association lifetime seconds 28800	
44	set security-association transform-keysize aes 256 256 256	
45	set security-association transform esp-aes esp-sha256-hmac	
46	set mtu 1454	
47	set ip df-bit 0	
48	set ip fragment post	
49	exit	
50	!	
51	crypto ipsec selector SELECTOR	VPNセレクタの設定
52	src 1 ipv4 any	
53	dst 1 ipv4 any	
54	exit	
55	!	
56	crypto isakmp keepalive	KeepAlive機能として使用するDPDの設定
57	logging level informational	VPN通信動作中の詳細なログを残す設定
58	crypto isakmp log sa	
59	crypto isakmp log session	
60	crypto isakmp log negotiation-fail	
61	!	
62	hostname KYOTEN	
63	!	
64	crypto isakmp policy P1-POLICY	ISAKMP ポリシーの設定
65	authentication pre-share	
66	encryption aes	
67	encryption-keysize aes 256 256 256	
68	group 14	
69	lifetime 86400	
70	hash sha-256	
71	initiate-mode aggressive	
72	exit	
73	!	

74	crypto isakmp profile PROF0001	ISAKMPプロファイルの設定
75	self-identity user-fqdn id-kyoten	
76	set isakmp-policy P1-POLICY	
77	set ipsec-policy P2-POLICY	
78	set peer 192.0.2.1	
79	ike-version 1	
80	local-key SECRET-VPN	
81	exit	
82	!	
83	crypto map CENTER ipsec-isakmp	センタのVPNピアとのセレクタ情報のエントリー
84	match address SELECTOR	
85	set isakmp-profile PROF0001	
86	exit	
87	!	
88	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。
89	!	
90	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）
91	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）
92	!	
93	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
94	!	
95	hostname FITELnet	hostname設定
96	!	
97	interface GigaEthernet 1/1	GigaEthernet インタフェースに、port-channel をリンク付け
98	vlan-id 1	
99	bridge-group 1	
100	channel-group 1	
101	exit	
102	!	
103	interface GigaEthernet 2/1	PPPoE 通信で使用する物理インタフェースの設定
104	vlan-id 2	
105	bridge-group 2	
106	pppoe enable	
107	exit	
108	!	
109	interface Port-channel 1	Port-channel にLAN側IPアドレスを設定
110	ip address 192.168.1.254 255.255.255.0	
111	ip dhcp service server	DHCPサーバ機能を有効化
112	ip dhcp server-profile lan1	DHCPサーバ機能で使用するプロファイルの指定
113	mss 1300	
114	exit	
115	!	
116	interface Tunnel 1	Tunnel インタフェース（PPPoE）の設定
117	description FLETS	
118	ip access-group 100 in	
119	ip access-group 111 out	IPv4アクセスリスト紐づけ
120	ip access-group 112 in	IPv4アクセスリスト紐づけ
121	ip access-group 113 out	IPv4アクセスリスト紐づけ
122	ip access-group 114 out	IPv4アクセスリスト紐づけ
123	ip access-group 115 in	IPv4アクセスリスト紐づけ
124	ip access-group spi ftp-data enable	学習フィルタ追加
125	ip nat inside source list 1 interface	
126	tunnel mode pppoe profile PPPOE_PROF	
127	pppoe interface gigaethernet 2/1	
128	exit	
129	!	
130	interface Tunnel 2	Tunnel インタフェース（IPsec）の設定
131	tunnel mode ipsec map CENTER	
132	dns-snooping enable	dns-snooping機能を有効とする設定
133	exit	
134	!	
135	pppoe profile PPPOE_PROF	PPPoEの設定
136	account abc345@***.***.ne.jp zzzyyyxxx	
137	exit	
138	!	
139	local-breakout enable	ローカルブレイクアウトを行う設定
140	local-breakout LBO1 tunnel 1	ローカルブレイクアウト対象パケットの中継先を設定

141	!	
142	lbo-profile LB01	LBOプロファイル設定
143	dns-snooping enable	dns-snooping機能を有効とする設定
144	dns-snooping expire 86400	dns-snooping により登録した経路の有効期限を設定
145	domain update.microsoft.com	ローカルブレイクアウト対象ドメインを設定
146	domain *.update.microsoft.com	
147	domain download.windowsupdate.com	
148	domain *.download.windowsupdate.com	
149	domain download.microsoft.com	
150	domain *.download.microsoft.com	
151	domain windowsupdate.com	
152	domain *.windowsupdate.com	
153	domain ntservicepack.microsoft.com	
154	domain login.live.com	
155	domain mp.microsoft.com	
156	domain *.mp.microsoft.com	
157	domain *.do.dsp.mp.microsoft.com	
158	domain *.dl.delivery.mp.microsoft.com	
159	domain *.emdl.ws.microsoft.com	
160	domain *.prod.do.dsp.mp.microsoft.com	
161	domain emdl.ws.microsoft.com	
162	domain *.delivery.mp.microsoft.com	
163	domain adl.windows.com	
164	domain tsfe.trafficshaping.dsp.mp.microsoft.com	
165	exit	
166	!	
167	end	