設定例

マルチポイントSAによる拠点間通信を利用する設定例（センタ2台構成、「IPv6ダイナミックDNS」サービスを利用）
対象装置：F70/F71/F220/F221/F220 EX/F221 EX

概要

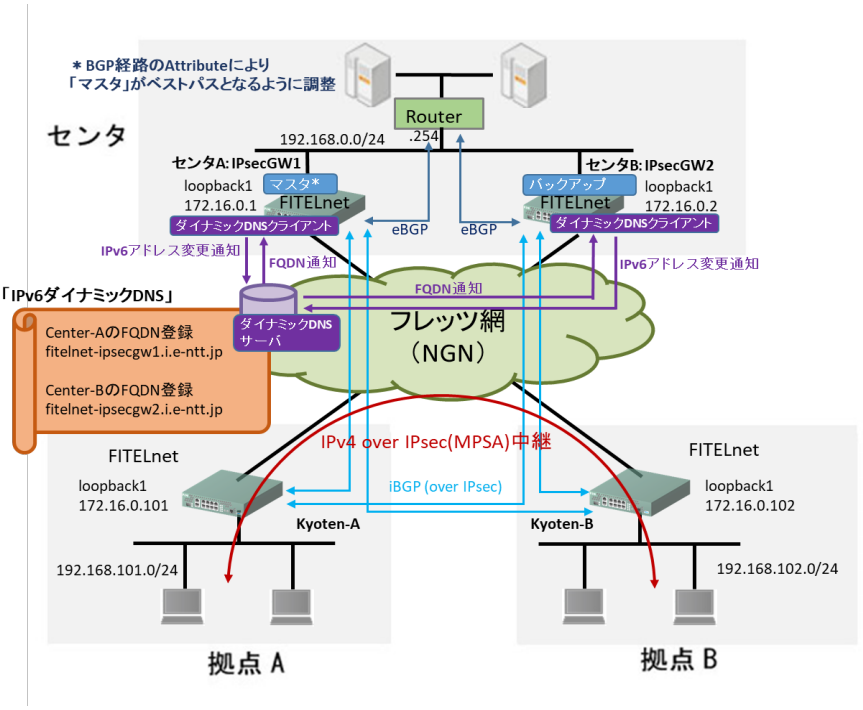
NGN（IPv6）網内で、マルチポイントSAを利用した拠点間通信を行う設定例です。
マルチポイントSAの詳細につきましては、下記リンクをご確認ください。
　マルチポイント SAについての機能概要

本設定例のセンタ側設定は、F220/F221/F220 EX/F221 EXで利用可能です。F220/F221の場合、V01.05以降のバージョンをお使いください。
F220/F221 V01.04以前のバージョンは、ダイナミックDNSクライアント機能のHTTPS通信に対応しておりません（HTTP通信であれば利用可能です）。
本設定例の拠点側設定は、F70/F71（V01.01以降）、F220/F221（V01.03以降）で利用可能です。

F220 EX/F221 EXをお使いの場合、対応ファームウェアバージョン情報はセンタ／拠点とも弊社にお問い合わせください。

本設定例を利用するには、NTT東日本「IPv6ダイナミックDNS」サービスをご利用いただくことが必要です。下記のURLをご参照ください。
https://ddns.e-ntt.jp/
2022年10月時点では、NTT西日本では「IPv6ダイナミックDNS」に類するサービスは行っておらず、NTT東日本サービス地域でのみご利用頂けます。
VPNプライオ等、VPNサービスのご契約は不要です。

本設定例は、マルチポイントSAサーバ2台冗長構成としております。
マルチポイントSAサーバ1台で運用する場合は、センタLAN側のRouter(eBGPピア)は不要です。コマンド設定例の右端に「不要」と記載のあるコマンドは不要となります。



パラメータ設定例

ISAKMPポリシー

IKEバージョン	2
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

※上記以外のパラメータは下記に合わせております。
https://www.furukawa.co.jp/fitelnet/product/f200/setting/detail/groupsa_1.html

コマンド設定例

「IPv6ダイナミックDNS」サービス利用のための設定を、黄色セルで示します。

センタA側FITELnetの設定

※：センタ1台構成で不要な行に「不要」と記載しています。

	設定例（センタ）	補足	※
1	access-list 4000 permit icmp6 any any neighbor-advertisement	IPv6アクセスリスト（NA許可）	
2	access-list 4000 permit icmp6 any any neighbor-solicitation	IPv6アクセスリスト（NS許可）	
3	access-list 4000 permit icmp6 any any router-advertisement	IPv6アクセスリスト（RA許可）	
4	access-list 4000 permit udp any any eq 546	IPv6アクセスリスト（DHCPv6許可）	
5	access-list 4000 permit udp any eq 500 any eq 500	IPv6アクセスリスト（IKE許可）	
6	access-list 4000 permit 50 any any	IPv6アクセスリスト（ESP許可）	

	設定例(センタ)	補足	※
7	access-list 4009 deny ipv6 any any	IPv6アクセスリスト(全拒否)	
8	access-list 4010 spi ipv6 any any	IPv6アクセスリスト(SPI)	
9	!		
10	ip route 172.16.0.2 255.255.255.255 192.168.0.2	バックアップ(センタB)側Loopbackインタフェースアドレス宛の経路を設定	不要
11	!		
12	ipv6 route ::/0 dhcp port-channel 2	IPv6デフォルトルート設定(デフォルトルートをDHCP port-channelに設定)	
13	!		
14	ipv6 dhcp client-profile ipv6dns client	DHCPv6クライアントプロファイル	
15	option-request dns-server	DNSサーバー要求設定	
16	retries infinity	DHCPv6メッセージの返信があるまで再送する設定	
17	exit		
18	!		
19	logging buffer level informational		
20	!		
21	hostname IPsecGW1		
22	!		
23	crypto ipsec replay-check disable		
24	crypto ipsec sequence-overflow disable		
25	!		
26	crypto ipsec policy IPsec_POLICY		
27	set pfs group14		
28	set security-association rekey always		
29	set security-association lifetime seconds 28800		
30	set security-association transform-keysize aes 256 256 256		
31	set security-association transform esp-aes esp-sha256-hmac		
32	set ip df-bit 0		
33	set ip fragment post		
34	sa-up route		
35	exit		
36	!		
37	crypto ipsec selector SELECTOR1		
38	src 1 ipv4 any		
39	dst 1 ipv4 any		
40	exit		
41	!		
42	crypto ipsec group-security policy GSA_POLICY	グループ鍵 IPsec設定モードへの移行(マルチポイントSAサーバ機能に関する設定)	
43	set security-association transform esp-aes esp-sha256-hmac		
44	set security-association transform-keysize aes 256		
45	set security-association lifetime seconds 600		
46	set security-association softlimit seconds 60		
47	rollover 30 30	マルチポイントSAの更新遅延時間の設定	
48	spi mask hex ffcfffff 00200000	マルチポイントSAのSPIの範囲を指定 ・マルチポイントSAサーバ毎に異なるように設定を行ってください(本設定例では、センタAの下位21bit目を0、センタBの下位21bit目を1、となるようにそれぞれ設定しています)。 ・センタ-拠点間で接続するSAと重複しないように、下位22bit目が1(0x00200000)となるように設定を行ってください	
49	exit		
50	!		
51	crypto group-security server ha local-address 172.16.0.1 remote-address 172.16.0.2	マルチポイントSAサーバの冗長機能を有効にする設定	不要
52	crypto group-security server ha keepalive-interval 10	マルチポイントSAサーバ冗長のKeepaliveメッセージの送信間隔の設定	不要
53	crypto group-security server ha keepalive-timeout 20	マルチポイントSAサーバ冗長のKeepaliveメッセージのタイムアウト時間の設定	不要
54	crypto group-security server priority 254	マルチポイントSAサーバの冗長機能で使用するサーバ優先度の設定	不要
55	crypto isakmp keepalive interval 60 always-send		
56	crypto isakmp log session detail		
57	crypto isakmp log negotiation-fail		
58	crypto isakmp log gsa	マルチポイントSA生成・削除・配布完了のログ出力設定	
59	!		
60	crypto isakmp policy ISAKMP_POLICY		
61	authentication pre-share		
62	encryption aes		
63	encryption-keysize aes 256 256 256		
64	group 14		
65	lifetime 86400		
66	hash sha-256		
67	exit		
68	!		
69	crypto isakmp profile ISAPROF_1		
70	self-identity fqdn IPsecGW1.example.jp	本装置の識別方法を設定(ホスト名(ID-TYPE=FQDN))	
71	set isakmp-policy ISAKMP_POLICY		
72	set ipsec-policy IPsec_POLICY		
73	set group-security-policy GSA_POLICY	マルチポイントSAクライアントに配布するマルチポイントSAポリシー名の設定	
74	ike-version 2	IKEv2を有効にする設定	
75	local-key SecretKey		
76	exit		
77	!		
78	crypto session release ipsec-lost-time 1		
79	crypto session release reset delete-send		
80	!		
81	crypto map MAP_1 ipsec-isakmp dynamic	ダイナミックセレクタとして動作させる設定	
82	match address SELECTOR1		
83	set isakmp-profile ISAPROF_1		
84	exit		
85	!		
86	interface GigaEthernet 1/1	物理インターフェース(LAN側)	
87	vlan-id 1		
88	bridge-group 1		
89	channel-group 1	LAN側論理インタフェース(Port-channel)と紐付け	
90	exit		
91	!		

	設定例(センタ)	補足	※
92	interface GigaEthernet 2/1	物理インターフェース(WAN側)	
93	vlan-id 2		
94	bridge-group 2		
95	channel-group 2	WAN側論理インタフェース(Port-channel)と紐付け	
96	ipv6 access-group 4000 in	IPv6アクセスリスト紐付け(permit)	
97	ipv6 access-group 4009 in	IPv6アクセスリスト紐付け(deny)	
98	ipv6 access-group 4010 out	IPv6アクセスリスト紐付け(SPI)	
99	exit		
100	!		
101	interface Loopback 1	Loopback1インタフェースの設定	
102	ip address 172.16.0.1	(センタと各拠点装置は、このアドレスでBGPセッションを確立します)	
103	exit		
104	!		
105	interface Port-channel 2	論理インターフェース(WAN側)	
106	ipv6 enable	IPv6リンクローカルアドレス設定	
107	ipv6 address autoconfig	IPv6アドレス設定(RAからアドレス生成)	
108	ipv6 nd receive-ra	RA受信設定	
109	ipv6 dhcp service client	DHCPv6クライアント設定	
110	ipv6 dhcp client-profile ipv6dns_client	DHCPv6クライアントプロファイル紐付け	
111	mtu 1500	MTU設定	
112	ddns-client address ipv6 action http-client 1 delay 10 interval 60	ダイナミックDNSクライアント設定	
113	exit		
114	!		
115	interface Port-channel 1	論理インターフェース(LAN側)	
116	ip address 192.168.0.1 255.255.255.0		
117	exit		
118	!		
119	router bgp 65000		
120	bgp router-id 172.16.0.1	BGPルータID設定	
121	bgp log-neighbor-changes	BGP関連ログ情報の出力	
122	bgp listen range 0.0.0.0/0 peer-group PEER_GROUP_1	動的にBGP接続を許可するネットワークアドレスの設定(ピアグループのポリシーを適用)	
123	neighbor 192.168.0.254 remote-as 65001	BGPピアのAS番号の設定(eBGP)	不要
124	neighbor PEER_GROUP_1 passive	本装置からBGPセッション接続要求を送信しないように設定	
125	neighbor PEER_GROUP_1 remote-as 65000	BGPピアのAS番号の設定(iBGP)	
126	neighbor PEER_GROUP_1 update-source loopback 1	BGPセッション確立の際の送信元アドレスの設定	
127	neighbor PEER_GROUP_1 peer-group	同じBGPポリシーを持つ複数のBGPピアをピアグループとして設定	
128	!		
129	address-family ipv4 unicast		
130	neighbor 192.168.0.254 route-map RMAP_LAN_LOCPRF_SET in	BGPピアにroute-mapを適用する設定(受信時に適用)	不要
131	neighbor 192.168.0.254 route-map RMAP_PE_MED_SET out	BGPピアにroute-mapを適用する設定(送信時に適用)	不要
132	neighbor PEER_GROUP_1 route-reflector-client	BGPピアをルートリフレクタクライアントとする設定	
133	neighbor PEER_GROUP_1 disable-nexthop-validation	BGPピアから学習した経路のNexthop到達性チェックを行わず、経路を有効と判定する設定	
134	redistribute connected route-map RMAP_LAN_LOCPRF_SET	経路情報を再広告する設定(connected経路にroute-mapを適用) ＊センタ1台構成ではroute-map指定は不要	左記＊
135	exit		
136	!		
137	exit		
138	!		
139	route-map RMAP_LAN_LOCPRF_SET permit 1	route-map設定モードへの移行	不要
140	set local-preference 200	route-mapに該当する経路情報のLOCAL-PREF値の設定(値が大きい方が優先)	不要
141	exit		不要
142	!		
143	route-map RMAP_PE_MED_SET permit 1	route-map設定モードへの移行	不要
144	set metric 100	route-mapに該当する経路情報のメトリック値の設定(値が小さい方が優先)	不要
145	exit		不要
146	!		
147	http-client 1	IPv6ダイナミックDNSサービスに接続するためのHTTPクライアントの設定	
148	request-timeout 10 retry 5	登録要求メッセージの応答受信待ち許容時間とリトライ回数を設定	
149	method 1 get url https://ddnsapi-v6.e-ntt.jp/api/renew/ <ホストキー> $i6	HTTPのRequest-Lineの設定 ＊「ホストキー」は、IPv6ダイナミックDNS管理画面の「ホストキー情報」をご確認くだ	
150	reference-interface port-channel 2	methodコマンドで参照するインタフェースを指定	
151	source-interface port-channel 2	登録要求メッセージの送信元アドレスを指定	
152	logging on	HTTPクライアントのログ出力を行う設定	
153	exit		
154	!		
155	end		

センタB側FITELnetの設定

※:センタ1台構成で不要な行に「不要」と記載しています。

	設定例(センタ)	補足	※
1	access-list 4000 permit icmp6 any any neighbor-advertisement		不要
2	access-list 4000 permit icmp6 any any neighbor-solicitation		不要
3	access-list 4000 permit icmp6 any any router-advertisement		不要
4	access-list 4000 permit udp any any eq 546		不要
5	access-list 4000 permit udp any eq 500 any eq 500		不要
6	access-list 4000 permit 50 any any		不要
7	access-list 4009 deny ipv6 any any		不要
8	access-list 4010 spi ipv6 any any		不要
9	!		不要
10	ip route 172.16.0.1 255.255.255.255 192.168.0.1	メイン(センタA)側Loopbackインタフェースアドレス宛の経路を設定	不要
11	!		不要
12	ipv6 route ::/0 dhcp port-channel 2		不要
13	!		不要
14	ipv6 dhcp client-profile ipv6dns_client		不要
15	option-request dns-server		不要
16	retries infinity		不要
17	exit		不要
18	!		不要
19	logging buffer level informational		不要
20	!		不要
21	hostname IPsecGW2		不要
22	!		不要
23	crypto ipsec replay-check disable		不要
24	crypto ipsec sequence-overflow disable		不要

	設定例(センタ)	補足	※
25	!		不要
26	crypto ipsec policy IPsec_POLICY		不要
27	set pfs group14		不要
28	set security-association rekey always		不要
29	set security-association lifetime seconds 28800		不要
30	set security-association transform-keysize aes 256 256 256		不要
31	set security-association transform esp-aes esp-sha256-hmac		不要
32	set ip df-bit 0		不要
33	set ip fragment post		不要
34	sa-up route		不要
35	exit		不要
36	!		不要
37	crypto ipsec selector SELECTOR1		不要
38	src 1 ipv4 any		不要
39	dst 1 ipv4 any		不要
40	exit		不要
41	!		不要
42	crypto ipsec group-security policy GSA_POLICY		不要
43	set security-association transform esp-aes esp-sha256-hmac		不要
44	set security-association transform-keysize aes 256		不要
45	set security-association lifetime seconds 600		不要
46	set security-association softlimit seconds 60		不要
47	rollover 30 30		不要
48	spi mask hex ffcfffff 00300000	マルチポイントSAのSPIの範囲を指定 ・マルチポイントSAサーバ毎に異なるように設定を行ってください(本設定例では、センタAの下位21bit目を0、センタBの下位21bit目を1、となるようにそれぞれ設定しています)。 ・センタ-拠点間で接続するSAと重複しないように、下位22bit目が1(0x00200000)となるように設定を行ってください	不要
49	exit		不要
50	!		不要
51	crypto group-security server ha local-address 172.16.0.2 remote-address 172.16.0.1	マルチポイントSAサーバの冗長機能を有効にする設定	不要
52	crypto group-security server ha keepalive-interval 10		不要
53	crypto group-security server ha keepalive-timeout 20		不要
54	crypto group-security server priority 253	マルチポイントSAサーバの冗長機能で使用するサーバ優先度の設定	不要
55	crypto isakmp keepalive interval 60 always-send		不要
56	crypto isakmp log session detail		不要
57	crypto isakmp log negotiation-fail		不要
58	crypto isakmp log gsa		不要
59	!		不要
60	crypto isakmp policy ISAKMP_POLICY		不要
61	authentication pre-share		不要
62	encryption aes		不要
63	encryption-keysize aes 256 256 256		不要
64	group 14		不要
65	lifetime 86400		不要
66	hash sha-256		不要
67	exit		不要
68	!		不要
69	crypto isakmp profile ISAPROF_1		不要
70	self-identity fqdn IPsecGW2.example.jp	本装置の識別方法を設定(ホスト名(ID-TYPE=FQDN))	不要
71	set isakmp-policy ISAKMP_POLICY		不要
72	set ipsec-policy IPsec_POLICY		不要
73	set group-security-policy GSA_POLICY		不要
74	ike-version 2		不要
75	local-key SecretKey		不要
76	exit		不要
77	!		不要
78	crypto session release ipsec-lost-time 1		不要
79	crypto session release reset delete-send		不要
80	!		不要
81	crypto map MAP 1 ipsec-isakmp dynamic		不要
82	match address SELECTOR1		不要
83	set isakmp-profile ISAPROF_1		不要
84	exit		不要
85	!		不要
86	interface GigaEthernet 1/1	物理インターフェース(LAN側)	不要
87	vlan-id 1		不要
88	bridge-group 1		不要
89	channel-group 1	LAN側論理インタフェース(Port-channel)と紐付け	不要
90	exit		不要
91	!		不要
92	interface GigaEthernet 2/1	物理インターフェース(WAN側)	不要
93	vlan-id 2		不要
94	bridge-group 2		不要
95	channel-group 2	WAN側論理インタフェース(Port-channel)と紐付け	不要
96	ipv6 access-group 4000 in		不要
97	ipv6 access-group 4009 in		不要
98	ipv6 access-group 4010 out		不要
99	exit		不要
100	!		不要
101	interface Loopback 1	Loopback1インタフェースの設定	不要
102	ip address 172.16.0.2	(センタと各拠点装置は、このアドレスでBGPセッションを確立します)	不要
103	exit		不要
104	!		不要
105	interface Port-channel 2	論理インターフェース(WAN側)	不要
106	ipv6 enable		不要
107	ipv6 address autoconfig		不要
108	ipv6 nd receive-ra		不要
109	ipv6 dhcp service client		不要
110	ipv6 dhcp client-profile ipv6dns_client		不要
111	mtu 1500		不要
112	ddns-client address ipv6 action http-client 1 delay 10 interval 60	ダイナミックDNSクライアント設定	不要
113	exit		不要
114	!		不要

	設定例(センタ)	補足	※
115	interface Port-channel 1	論理インターフェース(LAN側)	不要
116	ip address 192.168.0.2 255.255.255.0		不要
117	exit		不要
118	!		不要
119	router bgp 65000		不要
120	bgp router-id 172.16.0.2	BGPルータID設定	不要
121	bgp log-neighbor-changes		不要
122	bgp listen range 0.0.0.0/0 peer-group PEER_GROUP_1		不要
123	neighbor 192.168.0.254 remote-as 65001		不要
124	neighbor PEER_GROUP_1 passive		不要
125	neighbor PEER_GROUP_1 remote-as 65000		不要
126	neighbor PEER_GROUP_1 update-source loopback 1		不要
127	neighbor PEER_GROUP_1 peer-group		不要
128	!		不要
129	address-family ipv4 unicast		不要
130	neighbor 192.168.0.254 route-map RMAP_LAN_LOCPRF_SET in	BGPピアにroute-mapを適用する設定(受信時に適用)	不要
131	neighbor 192.168.0.254 route-map RMAP_PE_MED_SET out	BGPピアにroute-mapを適用する設定(送信時に適用)	不要
132	neighbor PEER_GROUP_1 route-reflector-client		不要
133	neighbor PEER_GROUP_1 disable-nexthop-validation		不要
134	redistribute connected route-map RMAP_LAN_LOCPRF_SET	経路情報を再広告する設定(connected経路にroute-mapを適用)	不要
135	exit		不要
136	!		不要
137	exit		不要
138	!		不要
139	route-map RMAP_LAN_LOCPRF_SET permit 1	route-map設定モードへの移行	不要
140	set local-preference 100	route-mapに該当する経路情報のLOCAL-PREF値の設定(値が大きい方が優先)	不要
141	exit		不要
142	!		不要
143	route-map RMAP_PE_MED_SET permit 1	route-map設定モードへの移行	不要
144	set metric 200	route-mapに該当する経路情報のメトリック値の設定(値が小さい方が優先)	不要
145	exit		不要
146	!		不要
147	http-client 1	IPv6ダイナミックDNSサービスに接続するためのHTTPクライアントの設定	不要
148	request-timeout 10 retry 5	登録要求メッセージの応答受信待ち許容時間とリトライ回数を設定	不要
149	method 1 get url https://ddnsapi-v6.e-ntt.jp/api/renew/ <ホストキー> $i6	HTTPのRequest-Lineの設定 ＊「ホストキー」は、IPv6ダイナミックDNS管理画面の「ホストキー情報」をご確認くだ	不要
150	reference-interface port-channel 2	methodコマンドで参照するインタフェースを指定	不要
151	source-interface port-channel 2	登録要求メッセージの送信元アドレスを指定	不要
152	logging on	HTTPクライアントのログ出力を行う設定	不要
153	exit		不要
154	!		不要
155	end		不要

拠点A側FITELnetの設定

※：センタ1台構成で不要な行に「不要」と記載しています。

	設定例（拠点）	補足	※
1	access-list 4000 permit icmp6 any any neighbor-advertisement		
2	access-list 4000 permit icmp6 any any neighbor-solicitation		
3	access-list 4000 permit icmp6 any any router-advertisement		
4	access-list 4000 permit udp any any eq 546		
5	access-list 4000 permit udp any eq 500 any eq 500		
6	access-list 4000 permit 50 any any		
7	access-list 4009 deny ipv6 any any		
8	access-list 4010 spi ipv6 any any		
9	!		
10	ip route 172.16.0.1 255.255.255.255 tunnel 1	メイン（センタA）側Loopbackインタフェースアドレス宛の経路を設定	
11	ip route 172.16.0.2 255.255.255.255 tunnel 2	メイン（センタB）側Loopbackインタフェースアドレス宛の経路を設定	
12	!		
13	ipv6 route ::/0 dhcp port-channel 2		
14	!		
15	ipv6 dhcp client-profile ipv6dns client		
16	option-request dns-server		
17	retries infinity		
18	exit		
19	!		
20	logging buffer level informational		
21	!		
22	hostname kyoten-a		
23	!		
24	crypto ipsec security-association softlimit initiate seconds 90		
25	crypto ipsec security-association softlimit respond seconds 90		
26	crypto ipsec replay-check disable		
27	crypto ipsec sequence-overflow disable		
28	!		
29	crypto ipsec policy IPsec_POLICY		
30	set pfs group14		
31	set security-association always-up		
32	set security-association rekey always		
33	set security-association lifetime seconds 28800		
34	set security-association transform-keysize aes 256 256 256		
35	set security-association transform esp-aes esp-sha256-hmac		
36	set ip df-bit 0		
37	set ip fragment post		
38	exit		
39	!		
40	crypto ipsec selector SELECTOR1		
41	src 1 ipv4 172.16.0.101 255.255.255.255		
42	dst 1 ipv4 any		
43	exit		
44	!		
45	crypto isakmp keepalive interval 60 always-send		
46	crypto isakmp log session detail		
47	crypto isakmp log negotiation-fail		
48	crypto isakmp log gsa		
49	crypto isakmp negotiation retry timer 10 limit 3 timer-max 30 guard-time 0		
50	crypto isakmp negotiation expire-time 90		
51	crypto isakmp negotiation always-up-params interval 100 max-initiate 10 max-pending 1 delay 1		
52	!		
53	crypto isakmp policy ISAKMP_POLICY		
54	authentication pre-share		
55	encryption aes		
56	encryption-keysize aes 256 256 256		
57	group 14		
58	lifetime 86000		
59	hash sha-256		
60	exit		
61	!		
62	crypto isakmp profile ISAPROF_1	センタA向けのISAKMPプロファイルを設定	
63	match identity host IPsecGW1.example.jp	VPNピアの識別方法を設定（ホスト名(ID-TYPE=FQDN)）	
64	self-identity user-fqdn kyoten-a@example.jp	本装置の識別方法を設定（ユーザ名(ID-TYPE=User-FQDN)）	
65	set isakmp-policy ISAKMP_POLICY		
66	set ipsec-policy IPsec_POLICY		
67	set peer domain fitelnet-ipsecgw1.i.e-ntt.jp v6	VPNピアをドメイン名で指定する（IPv6ダイナミックDNSサービスにて登録したFQDNを指定）	
68	group-security client spi mask hex ffdfffff 00200000	マルチポイントSAクライアントとして、マルチポイントSAサーバからマルチポイントSAを受信可能とする設定 本設定はマルチポイントSAサーバー2台の生成するマルチポイントSAを受信可能なSPIレンジとすることが必要です	
69	ike-version 2	IKEv2を有効にする設定	
70	local-key SecretKey		
71	exit		
72	!		
73	crypto isakmp profile ISAPROF_2	同様に、センタB向けのISAKMPプロファイルを設定	不要
74	match identity host IPsecGW2.example.jp		不要
75	self-identity user-fqdn kyoten-a@example.jp		不要
76	set isakmp-policy ISAKMP_POLICY		不要
77	set ipsec-policy IPsec_POLICY		不要
78	set peer domain fitelnet-ipsecgw2.i.e-ntt.jp v6	VPNピアをドメイン名で指定する（IPv6ダイナミックDNSサービスにて登録したFQDNを指定）	不要
79	group-security client spi mask hex ffdfffff 00200000		不要
80	ike-version 2		不要
81	local-key SecretKey		不要
82	exit		不要
83	!		
84	crypto session release ipsec-lost-time 1		
85	crypto session release reset delete-send		
86	!		

	設定例(拠点)	補足	※
87	crypto map MAP_1 ipsec-isakmp	センタA向けのVPNピアとのセレクタ情報のエントリを設定	
88	match address SELECTOR1		
89	set isakmp-profile ISAPROF_1		
90	exit		
91	!		
92	crypto map MAP_2 ipsec-isakmp	センタB向けのVPNピアとのセレクタ情報のエントリを設定	不要
93	match address SELECTOR1		不要
94	set isakmp-profile ISAPROF_2		不要
95	exit		不要
96	!		
97	interface GigaEthernet 1/1	物理インターフェース(LAN側)	
98	vlan-id 1		
99	bridge-group 1		
100	channel-group 1	LAN側論理インタフェース(Port-channel)と紐付け	
101	exit		
102	!		
103	interface GigaEthernet 2/1	物理インターフェース(WAN側)	
104	vlan-id 2		
105	bridge-group 2		
106	channel-group 2	WAN側論理インタフェース(Port-channel)と紐付け	
107	ipv6 access-group 4000 in		
108	ipv6 access-group 4009 in		
109	ipv6 access-group 4010 out		
110	exit		
111	!		
112	interface Loopback 1	Loopback1インタフェースの設定	
113	ip address 172.16.0.101	(センタと各拠点装置は、このアドレスでBGPセッションを確立します)	
114	exit		
115	!		
116	interface Port-channel 2	論理インターフェース(WAN側)	
117	ipv6 enable		
118	ipv6 address autoconfig		
119	ipv6 nd receive-ra		
120	ipv6 dhcp service client		
121	ipv6 dhcp client-profile ipv6dns_client		
122	mtu 1500		
123	exit		
124	!		
125	interface Port-channel 1	論理インターフェース(LAN側)	
126	ip address 192.168.101.1 255.255.255.0		
127	exit		
128	!		
129	interface Tunnel 1		
130	tunnel mode ipsec map MAP_1		
131	exit		
132	!		
133	interface Tunnel 2		不要
134	tunnel mode ipsec map MAP_2		不要
135	exit		不要
136	!		
137	interface Tunnel 3		
138	tunnel mode ipsec		
139	crypto group-security map MAP_1	マルチポイントSAサーバからマルチポイントSAを受信する設定	
140	crypto group-security map MAP_2	(マルチポイントSAサーバの冗長機能を使用する場合は複数指定)	不要
141	exit		
142	!		
143	router bgp 65000		
144	bgp router-id 172.16.0.101	BGPルータID設定	
145	bgp log-neighbor-changes		
146	neighbor 172.16.0.1 remote-as 65000	BGPピアのAS番号の設定(iBGP)	
147	neighbor 172.16.0.1 update-source loopback 1	BGPセッション確立の際の送信元アドレスの設定	
148	neighbor 172.16.0.2 remote-as 65000		不要
149	neighbor 172.16.0.2 update-source loopback 1		不要
150	!		
151	address-family ipv4 unicast		
152	neighbor 172.16.0.1 disable-nexthop-validation		
153	neighbor 172.16.0.1 encap endpoint ipv6 interface port-channel 2	BGPピアに対するトンネルエンドポイントを設定 本装置をマルチポイントSAクライアントとして動作させる場合に設定	
154	neighbor 172.16.0.1 encap type ipsec-tunnel	BGPピアに対するカプセル化方式を設定 本装置をマルチポイントSAクライアントとして動作させる場合に設定	
155	neighbor 172.16.0.2 disable-nexthop-validation		不要
156	neighbor 172.16.0.2 encap endpoint ipv6 interface port-channel 2		不要
157	neighbor 172.16.0.2 encap type ipsec-tunnel		不要
158	redistribute connected	経路情報を再広告する設定	
159	exit		
160	!		
161	exit		
162	!		
163	ip name-server ::1	DNSサーバー設定(自装置をサーバーに設定)	
164	!		
165	crypto ip name-server ::1	VPNピアのアドレス問い合わせを行うDNSサーバー設定(自装置をサーバーに設定)	
166	!		
167	dns-server ipv6 enable	DNSv6サーバー設定(ProxyDNS機能を有効にする)	
168	!		
169	proxydns domain 1 any * any dhcp ipv6 port-channel 2	proxyDNS 順引き設定(IPv6 DNS / any)	
170	proxydns address 1 any dhcp ipv6 port-channel 2	proxyDNS 逆引き設定(IPv6 DNS / any)	
171	!		
172	end		

拠点B側FITELnetの設定

※:センタ1台構成で不要な行に「不要」と記載しています。

	設定例(拠点)	補足	※
1	access-list 4000 permit icmp6 any any neighbor-advertisement		
2	access-list 4000 permit icmp6 any any neighbor-solicitation		
3	access-list 4000 permit icmp6 any any router-advertisement		

	設定例(拠点)	補足	※
4	access-list 4000 permit udp any any eq 546		
5	access-list 4000 permit udp any eq 500 any eq 500		
6	access-list 4000 permit 50 any any		
7	access-list 4009 deny ipv6 any any		
8	access-list 4010 spi ipv6 any any		
9	!		
10	ip route 172.16.0.1 255.255.255.255 tunnel 1		
11	ip route 172.16.0.2 255.255.255.255 tunnel 2		
12	!		
13	ipv6 route ::/0 dhcp port-channel 2		
14	!		
15	ipv6 dhcp client-profile ipv6dns_client		
16	option-request dns-server		
17	retries infinity		
18	exit		
19	!		
20	logging buffer level informational		
21	!		
22	hostname kyoten-b		
23	!		
24	crypto ipsec security-association softlimit initiate seconds 90		
25	crypto ipsec security-association softlimit respond seconds 90		
26	crypto ipsec replay-check disable		
27	crypto ipsec sequence-overflow disable		
28	!		
29	crypto ipsec policy IPsec_POLICY		
30	set pfs group14		
31	set security-association always-up		
32	set security-association rekey always		
33	set security-association lifetime seconds 28800		
34	set security-association transform-keysize aes 256 256 256		
35	set security-association transform esp-aes esp-sha256-hmac		
36	set ip df-bit 0		
37	set ip fragment post		
38	exit		
39	!		
40	crypto ipsec selector SELECTOR1		
41	src 1 ipv4 172.16.0.102 255.255.255.255		
42	dst 1 ipv4 any		
43	exit		
44	!		
45	crypto isakmp keepalive interval 60 always-send		
46	crypto isakmp log session detail		
47	crypto isakmp log negotiation-fail		
48	crypto isakmp log gsa		
49	crypto isakmp negotiation retry timer 10 limit 3 timer-max 30 guard-time 0		
50	crypto isakmp negotiation expire-time 90		
51	crypto isakmp negotiation always-up-params interval 100 max-initiate 10 max-pending 1 delay 1		
52	!		
53	crypto isakmp policy ISAKMP_POLICY		
54	authentication pre-share		
55	encryption aes		
56	encryption-keysize aes 256 256 256		
57	group 14		
58	lifetime 86000		
59	hash sha-256		
60	exit		
61	!		
62	crypto isakmp profile ISAPROF_1	センタA向けのISAKMPプロファイルを設定	
63	match identity host IPsecGW1.example.jp		
64	self-identity user-fqdn kyoten-b@example.jp		
65	set isakmp-policy ISAKMP_POLICY		
66	set ipsec-policy IPsec_POLICY		
67	set peer domain fitelnet-ipsecgw1.i.e-ntt.jp v6	VPNピアをドメイン名で指定する(IPv6ダイナミックDNSサービスにて登録したFQDNを指定)	
68	group-security client spi mask hex ffdfffff 00200000	マルチポイントSAクライアントとして、マルチポイントSAサーバからマルチポイントSAを受信可能とする設定 本設定はマルチポイントSAサーバー2台の生成するマルチポイントSAを受信可能なSPIレンジとすることが必要です	
69	ike-version 2		
70	local-key SecretKey		
71	exit		
72	!		
73	crypto isakmp profile ISAPROF_2	同様に、センタB向けのISAKMPプロファイルを設定	不要
74	match identity host IPsecGW2.example.jp		不要
75	self-identity user-fqdn kyoten-b@example.jp		不要
76	set isakmp-policy ISAKMP_POLICY		不要
77	set ipsec-policy IPsec_POLICY		不要
78	set peer domain fitelnet-ipsecgw2.i.e-ntt.jp v6	VPNピアをドメイン名で指定する(IPv6ダイナミックDNSサービスにて登録したFQDNを指定)	不要
79	group-security client spi mask hex ffdfffff 00200000		不要
80	ike-version 2		不要
81	local-key SecretKey		不要
82	exit		不要
83	!		
84	crypto session release ipsec-lost-time 1		
85	crypto session release reset delete-send		
86	!		
87	crypto map MAP_1 ipsec-isakmp		
88	match address SELECTOR1		
89	set isakmp-profile ISAPROF_1		
90	exit		
91	!		

	設定例(拠点)	補足	※
92	crypto map MAP_2 ipsec-isakmp		不要
93	match address SELECTOR1		不要
94	set isakmp-profile ISAPROF_2		不要
95	exit		不要
96	!		
97	interface GigaEthernet 1/1	物理インターフェース(LAN側)	
98	vlan-id 1		
99	bridge-group 1		
100	channel-group 1	LAN側論理インタフェース(Port-channel)と紐付け	
101	exit		
102	!		
103	interface GigaEthernet 2/1	物理インターフェース(WAN側)	
104	vlan-id 2		
105	bridge-group 2		
106	channel-group 2	WAN側論理インタフェース(Port-channel)と紐付け	
107	ipv6 access-group 4000 in		
108	ipv6 access-group 4009 in		
109	ipv6 access-group 4010 out		
110	exit		
111	!		
112	interface Loopback 1	Loopback1インタフェースの設定	
113	ip address 172.16.0.102	(センタと各拠点装置は、このアドレスでBGPセッションを確立します)	
114	exit		
115	!		
116	interface Port-channel 2	論理インターフェース(WAN側)	
117	ipv6 enable		
118	ipv6 address autoconfig		
119	ipv6 nd receive-ra		
120	ipv6 dhcp service client		
121	ipv6 dhcp client-profile ipv6dns_client		
122	mtu 1500		
123	exit		
124	!		
125	interface Port-channel 1	論理インターフェース(LAN側)	
126	ip address 192.168.102.1 255.255.255.0		
127	exit		
128	!		
129	interface Tunnel 1		
130	tunnel mode ipsec map MAP_1		
131	exit		
132	!		
133	interface Tunnel 2		不要
134	tunnel mode ipsec map MAP_2		不要
135	exit		不要
136	!		
137	interface Tunnel 3		
138	tunnel mode ipsec		
139	crypto group-security map MAP_1	マルチポイントSAサーバからマルチポイントSAを受信する設定	
140	crypto group-security map MAP_2	(マルチポイントSAサーバの冗長機能を使用する場合は複数指定)	不要
141	exit		
142	!		
143	router bgp 65000		
144	bgp router-id 172.16.0.102	BGPルータID設定	
145	bgp log-neighbor-changes		
146	neighbor 172.16.0.1 remote-as 65000	BGPピアのAS番号の設定(iBGP)	
147	neighbor 172.16.0.1 update-source loopback 1	BGPセッション確立の際の送信元アドレスの設定	
148	neighbor 172.16.0.2 remote-as 65000		不要
149	neighbor 172.16.0.2 update-source loopback 1		不要
150	!		
151	address-family ipv4 unicast		
152	neighbor 172.16.0.1 disable-nexthop-validation		
153	neighbor 172.16.0.1 encap endpoint ipv6 interface port-channel 2	BGPピアに対するトンネルエンドポイントを設定 本装置をマルチポイントSAクライアントとして動作させる場合に設定	
154	neighbor 172.16.0.1 encap type ipsec-tunnel	BGPピアに対するカプセル化方式を設定 本装置をマルチポイントSAクライアントとして動作させる場合に設定	
155	neighbor 172.16.0.2 disable-nexthop-validation		不要
156	neighbor 172.16.0.2 encap endpoint ipv6 interface port-channel 2		不要
157	neighbor 172.16.0.2 encap type ipsec-tunnel		不要
158	redistribute connected		
159	exit		
160	!		
161	exit		
162	!		
163	ip name-server ::1		
164	!		
165	crypto ip name-server ::1		
166	!		
167	dns-server ipv6 enable		
168	!		
169	proxydns domain 1 any * any dhcp ipv6 port-channel 2		
170	proxydns address 1 any dhcp ipv6 port-channel 2		
171	!		
172	end		