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/F225/F310/F220 EX/F221 EX（F70/F71/F310は拠点のみ）

概要

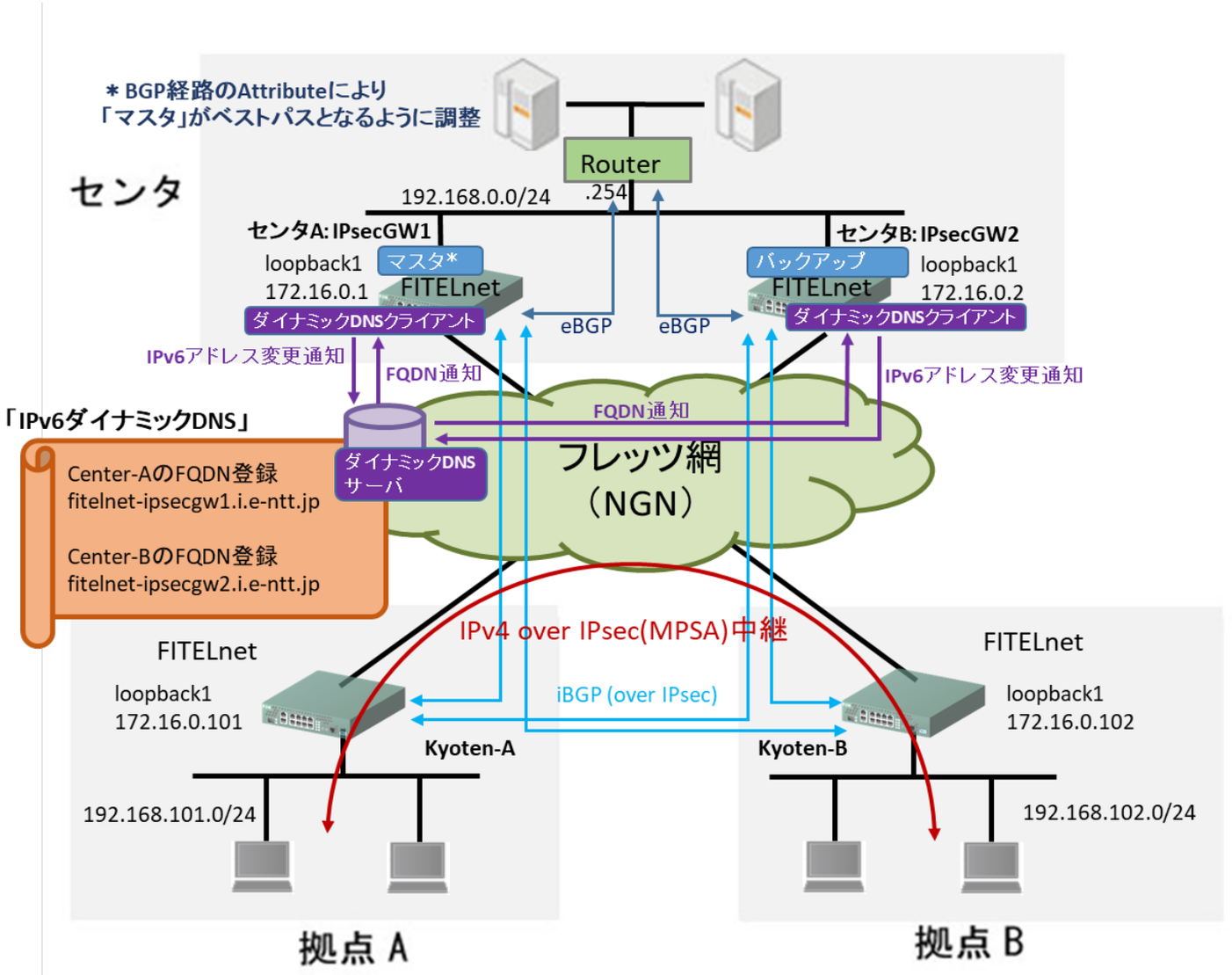
NGN（IPv6）網内で、マルチポイントSAを利用した拠点間通信を行う設定例です。
マルチポイントSAの詳細につきましては、下記リンクをご確認ください。
　マルチポイント SAについての機能概要

本設定例のセンタ側設定は、F220/F221/F225/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	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。	
20	!		
21	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)	
22	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)	
23	!		
24	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	
25	!		
26	hostname IPsecGW1	hostname設定	
27	!		
28	crypto ipsec replay-check disable		
29	crypto ipsec sequence-overflow disable		
30	!		
31	crypto ipsec policy IPsec_POLICY		
32	set pfs group14		
33	set security-association rekey always		
34	set security-association lifetime seconds 28800		
35	set security-association transform-keysize aes 256 256 256		
36	set security-association transform esp-aes esp-sha256-hmac		
37	set ip df-bit 0		
38	set ip fragment post		
39	sa-up route		
40	exit		
41	!		
42	crypto ipsec selector SELECTOR1		
43	src 1 ipv4 any		
44	dst 1 ipv4 any		
45	exit		
46	!		
47	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)	
48	set security-association transform esp-aes esp-sha256-hmac		
49	set security-association transform-keysize aes 256		
50	set security-association lifetime seconds 600		
51	set security-association softlimit seconds 60		
52	rollover 30 30	マルチポイントSAの更新遅延時間の設定	
53	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)。 ・センター拠点間で接続する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	
54	exit		
55	!		
56	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
57	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
58	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
59	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
60	crypto isakmp keepalive interval 60 always-send		
61	crypto isakmp log session detail		
62	crypto isakmp log negotiation-fail		
63	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	
64	!		
65	crypto isakmp policy ISAKMP_POLICY		
66	authentication pre-share		
67	encryption aes		
68	encryption-keysize aes 256 256 256		
69	group 14		
70	lifetime 86400		
71	hash sha-256		
72	exit		
73	!		
74	crypto isakmp profile ISAPROF_1		
75	self-identity fqdn IPsecGW1.example.jp	本装置の識別方法を設定(ホスト名(ID-TYPE=FQDN))	
76	set isakmp-policy ISAKMP_POLICY		
77	set ipsec-policy IPsec_POLICY		
78	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	
79	ike-version 2	IKEv2を有効にする設定	
80	local-key SecretKey		
81	exit		
82	!		
83	crypto session release ipsec-lost-time 1		
84	crypto session release reset delete-send		
85	!		
86	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	
87	match address SELECTOR1		
88	set isakmp-profile ISAPROF_1		
89	exit		
90	!		

MPSA設定例 「IPv6ダイナミックDNS」サービスを利用

	設定例(センタ)	補足	※
91	interface GigaEthernet 1/1	物理インターフェース(LAN側)	
92	vlan-id 1		
93	bridge-group 1		
94	channel-group 1	LAN側論理インタフェース(Port-channel)と紐付け	
95	exit		
96	!		
97	interface GigaEthernet 2/1	物理インターフェース(WAN側)	
98	vlan-id 2		
99	bridge-group 2		
100	channel-group 2	WAN側論理インタフェース(Port-channel)と紐付け	
101	ipv6 access-group 4000 in	IPv6アクセスリスト紐付け(permit)	
102	ipv6 access-group 4009 in	IPv6アクセスリスト紐付け(deny)	
103	ipv6 access-group 4010 out	IPv6アクセスリスト紐付け(SPI)	
104	exit		
105	!		
106	interface Loopback 1	Loopback1インタフェースの設定	
107	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)	
108	exit		
109	!		
110	interface Port-channel 2	論理インターフェース(WAN側)	
111	ipv6 enable	IPv6リンクローカルアドレス設定	
112	ipv6 address autoconfig	IPv6アドレス設定(RAからアドレス生成)	
113	ipv6 nd receive-ra	RA受信設定	
114	ipv6 dhcp service client	DHCPv6クライアント設定	
115	ipv6 dhcp client-profile ipv6dns_client	DHCPv6クライアントプロファイル紐付け	
116	mtu 1500	MTU設定	
117	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	
118	exit		
119	!		
120	interface Port-channel 1	論理インターフェース(LAN側)	
121	ip address 192.168.0.1 255.255.255.0		
122	exit		
123	!		
124	router bgp 65000		
125	bgp router-id 172.16.0.1	BGPルータID設定	
126	bgp log-neighbor-changes	BGP関連ログ情報の出力	
127	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)	
128	neighbor 192.168.0.254 remote-as 65001	BGPピアのAS番号の設定(eBGP)	不要
129	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	
130	neighbor PEER_GROUP_1 remote-as 65000	BGPピアのAS番号の設定(iBGP)	
131	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	
132	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	
133	!		
134	address-family ipv4 unicast		
135	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
136	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
137	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	
138	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	
139	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 ＊
140	exit		
141	!		
142	exit		
143	!		
144	route-map RMAP_LAN_LOCPRF_SET permit 1	route-map設定モードへの移行	不要
145	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
146	exit		不要
147	!		
148	route-map RMAP_PE_MED_SET permit 1	route-map設定モードへの移行	不要
149	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
150	exit		不要
151	!		
152	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	
153	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	
154	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	
155	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	
156	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	
157	logging on	HTTPクライアントのログ出力を行う設定	
158	exit		
159	!		
160	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

	設定例(センタ)	補足	※
19	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。	不要
20	!		不要
21	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)	不要
22	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)	不要
23	!		不要
24	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	不要
25	!		不要
26	hostname IPsecGW2	hostname設定	不要
27	!		不要
28	crypto ipsec replay-check disable		不要
29	crypto ipsec sequence-overflow disable		不要
30	!		不要
31	crypto ipsec policy IPsec_POLICY		不要
32	set pfs group14		不要
33	set security-association rekey always		不要
34	set security-association lifetime seconds 28800		不要
35	set security-association transform-keysize aes 256 256 256		不要
36	set security-association transform esp-aes esp-sha256-hmac		不要
37	set ip df-bit 0		不要
38	set ip fragment post		不要
39	sa-up route		不要
40	exit		不要
41	!		不要
42	crypto ipsec selector SELECTOR1		不要
43	src 1 ipv4 any		不要
44	dst 1 ipv4 any		不要
45	exit		不要
46	!		不要
47	crypto ipsec group-security policy GSA_POLICY		不要
48	set security-association transform esp-aes esp-sha256-hmac		不要
49	set security-association transform-keysize aes 256		不要
50	set security-association lifetime seconds 600		不要
51	set security-association softlimit seconds 60		不要
52	rollover 30 30		不要
53	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	不要
54	exit		不要
55	!		不要
56	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
57	crypto group-security server ha keepalive-interval 10		不要
58	crypto group-security server ha keepalive-timeout 20		不要
59	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
60	crypto isakmp keepalive interval 60 always-send		不要
61	crypto isakmp log session detail		不要
62	crypto isakmp log negotiation-fail		不要
63	crypto isakmp log gsa		不要
64	!		不要
65	crypto isakmp policy ISAKMP_POLICY		不要
66	authentication pre-share		不要
67	encryption aes		不要
68	encryption-keysize aes 256 256 256		不要
69	group 14		不要
70	lifetime 86400		不要
71	hash sha-256		不要
72	exit		不要
73	!		不要
74	crypto isakmp profile ISAPROF_1		不要
75	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
76	set isakmp-policy ISAKMP_POLICY		不要
77	set ipsec-policy IPsec_POLICY		不要
78	set group-security-policy GSA_POLICY		不要
79	ike-version 2		不要
80	local-key SecretKey		不要
81	exit		不要
82	!		不要
83	crypto session release ipsec-lost-time 1		不要
84	crypto session release reset delete-send		不要
85	!		不要
86	crypto map MAP_1 ipsec-isakmp dynamic		不要
87	match address SELECTOR1		不要
88	set isakmp-profile ISAPROF_1		不要
89	exit		不要
90	!		不要
91	interface GigaEthernet 1/1	物理インターフェース(LAN側)	不要
92	vlan-id 1		不要
93	bridge-group 1		不要
94	channel-group 1	LAN側論理インタフェース(Port-channel)と紐付け	不要
95	exit		不要
96	!		不要
97	interface GigaEthernet 2/1	物理インターフェース(WAN側)	不要
98	vlan-id 2		不要
99	bridge-group 2		不要
100	channel-group 2	WAN側論理インタフェース(Port-channel)と紐付け	不要
101	ipv6 access-group 4000 in		不要
102	ipv6 access-group 4009 in		不要
103	ipv6 access-group 4010 out		不要
104	exit		不要
105	!		不要

	設定例(センタ)	補足	※
106	interface Loopback 1	Loopback1インタフェースの設定	不要
107	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
108	exit		不要
109	!		不要
110	interface Port-channel 2	論理インターフェース(WAN側)	不要
111	ipv6 enable		不要
112	ipv6 address autoconfig		不要
113	ipv6 nd receive-ra		不要
114	ipv6 dhcp service client		不要
115	ipv6 dhcp client-profile ipv6dns_client		不要
116	mtu 1500		不要
117	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
118	exit		不要
119	!		不要
120	interface Port-channel 1	論理インターフェース(LAN側)	不要
121	ip address 192.168.0.2 255.255.255.0		不要
122	exit		不要
123	!		不要
124	router bgp 65000		不要
125	bgp router-id 172.16.0.2	BGPルータID設定	不要
126	bgp log-neighbor-changes		不要
127	bgp listen range 0.0.0.0/0 peer-group PEER_GROUP_1		不要
128	neighbor 192.168.0.254 remote-as 65001		不要
129	neighbor PEER_GROUP_1 passive		不要
130	neighbor PEER_GROUP_1 remote-as 65000		不要
131	neighbor PEER_GROUP_1 update-source loopback 1		不要
132	neighbor PEER_GROUP_1 peer-group		不要
133	!		不要
134	address-family ipv4 unicast		不要
135	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
136	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
137	neighbor PEER_GROUP_1 route-reflector-client		不要
138	neighbor PEER_GROUP_1 disable-nexthop-validation		不要
139	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
140	exit		不要
141	!		不要
142	exit		不要
143	!		不要
144	route-map RMAP_LAN_LOCPRF_SET permit 1	route-map設定モードへの移行	不要
145	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
146	exit		不要
147	!		不要
148	route-map RMAP_PE_MED_SET permit 1	route-map設定モードへの移行	不要
149	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
150	exit		不要
151	!		不要
152	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
153	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
154	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
155	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
156	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
157	logging on	HTTPクライアントのログ出力を行う設定	不要
158	exit		不要
159	!		不要
160	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	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。	
21	!		
22	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）	
23	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）	
24	!		
25	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	
26	!		
27	hostname kyoten-a	hostname設定	
28	!		
29	crypto ipsec security-association softlimit initiate seconds 90		
30	crypto ipsec security-association softlimit respond seconds 90		
31	crypto ipsec replay-check disable		
32	crypto ipsec sequence-overflow disable		
33	!		
34	crypto ipsec policy IPsec_POLICY		
35	set pfs group14		
36	set security-association always-up		
37	set security-association rekey always		
38	set security-association lifetime seconds 28800		
39	set security-association transform-keysize aes 256 256 256		
40	set security-association transform esp-aes esp-sha256-hmac		
41	set ip df-bit 0		
42	set ip fragment post		
43	exit		
44	!		
45	crypto ipsec selector SELECTOR1		
46	src 1 ipv4 172.16.0.101 255.255.255.255		
47	dst 1 ipv4 any		
48	exit		
49	!		
50	crypto isakmp keepalive interval 60 always-send		
51	crypto isakmp log session detail		
52	crypto isakmp log negotiation-fail		
53	crypto isakmp log gsa		
54	crypto isakmp negotiation retry timer 10 limit 3 timer-max 30 guard-time		
55	crypto isakmp negotiation expire-time 90		
56	crypto isakmp negotiation always-up-params interval 100 max-initiate 10 max-pending 1 delay 1		
57	!		
58	crypto isakmp policy ISAKMP_POLICY		
59	authentication pre-share		
60	encryption aes		
61	encryption-keysize aes 256 256 256		
62	group 14		
63	lifetime 86000		
64	hash sha-256		
65	exit		
66	!		
67	crypto isakmp profile ISAPROF_1	センタA向けのISAKMPプロファイルを設定	
68	match identity host IPsecGW1.example.jp	VPNピアの識別方法を設定（ホスト名(ID-TYPE=FQDN)）	不要
69	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)）	不要
70	set isakmp-policy ISAKMP_POLICY		不要
71	set ipsec-policy IPsec_POLICY		不要
72	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）	不要
73	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	不要
74	ike-version 2	IKEv2を有効にする設定	不要
75	local-key SecretKey		不要
76	exit		不要

	設定例(拠点)	補足	※
77	!		不要
78	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	
79	match identity host IPsecGW2.example.jp		
80	self-identity user-fqdn kyoten-a@example.jp		
81	set isakmp-policy ISAKMP_POLICY		
82	set ipsec-policy IPsec_POLICY		
83	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)	
84	group-security client spi mask hex ffdfffff 00200000		
85	ike-version 2		
86	local-key SecretKey		
87	exit		不要
88	!		不要
89	crypto session release ipsec-lost-time 1		不要
90	crypto session release reset delete-send		不要
91	!		
92	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	
93	match address SELECTOR1		
94	set isakmp-profile ISAPROF_1		
95	exit		
96	!		
97	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	
98	match address SELECTOR1		
99	set isakmp-profile ISAPROF_2		
100	exit		
101	!		
102	interface GigaEthernet 1/1	物理インターフェース(LAN側)	
103	vlan-id 1		
104	bridge-group 1		
105	channel-group 1	LAN側論理インタフェース(Port-channel)と紐付け	
106	exit		
107	!		
108	interface GigaEthernet 2/1	物理インターフェース(WAN側)	
109	vlan-id 2		
110	bridge-group 2		
111	channel-group 2	WAN側論理インタフェース(Port-channel)と紐付け	
112	ipv6 access-group 4000 in		
113	ipv6 access-group 4009 in		
114	ipv6 access-group 4010 out		
115	exit		
116	!		
117	interface Loopback 1	Loopback1インタフェースの設定	
118	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)	
119	exit		
120	!		
121	interface Port-channel 2	論理インターフェース(WAN側)	
122	ipv6 enable		
123	ipv6 address autoconfig		
124	ipv6 nd receive-ra		
125	ipv6 dhcp service client		
126	ipv6 dhcp client-profile ipv6dns_client		
127	mtu 1500		
128	exit		不要
129	!		不要
130	interface Port-channel 1	論理インターフェース(LAN側)	不要
131	ip address 192.168.101.1 255.255.255.0		
132	exit		
133	!		
134	interface Tunnel 1		
135	tunnel mode ipsec map MAP_1		不要
136	exit		
137	!		
138	interface Tunnel 2		
139	tunnel mode ipsec map MAP_2		
140	exit		
141	!		
142	interface Tunnel 3		
143	tunnel mode ipsec		不要
144	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	不要
145	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)	
146	exit		
147	!		
148	router bgp 65000		
149	bgp router-id 172.16.0.101	BGPルータID設定	
150	bgp log-neighbor-changes		不要
151	neighbor 172.16.0.1 remote-as 65000	BGPピアのAS番号の設定(iBGP)	不要
152	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	不要
153	neighbor 172.16.0.2 remote-as 65000		
154	neighbor 172.16.0.2 update-source loopback 1		
155	!		
156	address-family ipv4 unicast		
157	neighbor 172.16.0.1 disable-nexthop-validation		
158	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	
159	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	
160	neighbor 172.16.0.2 disable-nexthop-validation		
161	neighbor 172.16.0.2 encap endpoint ipv6 interface port-channel 2		
162	neighbor 172.16.0.2 encap type ipsec-tunnel		
163	redistribute connected	経路情報を再広告する設定	
164	exit		
165	!		
166	exit		
167	!		

	設定例(拠点)	補足	※
168	ip name-server ::1	DNSサーバー設定(自装置をサーバーに設定)	
169	!		
170	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)	
171	!		
172	dns-server ipv6 enable	DNSv6サーバー設定(ProxyDNS機能を有効にする)	
173	!		
174	proxydns domain 1 any * any dhcp ipv6 port-channel 2	proxyDNS 順引き設定(IPv6 DNS / any)	
175	proxydns address 1 any dhcp ipv6 port-channel 2	proxyDNS 逆引き設定(IPv6 DNS / any)	
176	!		
177	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		
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	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。	
21	!		
22	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)	
23	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)	
24	!		
25	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	
26	!		
27	hostname kyoten-b	hostname設定	
28	!		
29	crypto ipsec security-association softlimit initiate seconds 90		
30	crypto ipsec security-association softlimit respond seconds 90		
31	crypto ipsec replay-check disable		
32	crypto ipsec sequence-overflow disable		
33	!		
34	crypto ipsec policy IPsec_POLICY		
35	set pfs group14		
36	set security-association always-up		
37	set security-association rekey always		
38	set security-association lifetime seconds 28800		
39	set security-association transform-keysize aes 256 256 256		
40	set security-association transform esp-aes esp-sha256-hmac		
41	set ip df-bit 0		
42	set ip fragment post		
43	exit		
44	!		
45	crypto ipsec selector SELECTOR1		
46	src 1 ipv4 172.16.0.102 255.255.255.255		
47	dst 1 ipv4 any		
48	exit		
49	!		
50	crypto isakmp keepalive interval 60 always-send		
51	crypto isakmp log session detail		
52	crypto isakmp log negotiation-fail		
53	crypto isakmp log gsa		
54	crypto isakmp negotiation retry timer 10 limit 3 timer-max 30 guard-time		
55	crypto isakmp negotiation expire-time 90		
56	crypto isakmp negotiation always-up-params interval 100 max-initiate 10 max-pending 1 delay 1		
57	!		
58	crypto isakmp policy ISAKMP_POLICY		
59	authentication pre-share		
60	encryption aes		
61	encryption-keysize aes 256 256 256		
62	group 14		
63	lifetime 86000		
64	hash sha-256		
65	exit		
66	!		

	設定例(拠点)	補足	※
67	crypto isakmp profile ISAPROF_1	センタA向けのISAKMPプロファイルを設定	
68	match identity host IPsecGW1.example.jp		不要
69	self-identity user-fqdn kyoten-b@example.jp		不要
70	set isakmp-policy ISAKMP_POLICY		不要
71	set ipsec-policy IPsec_POLICY		不要
72	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)	不要
73	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	不要
74	ike-version 2		不要
75	local-key SecretKey		不要
76	exit		不要
77	!		不要
78	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	
79	match identity host IPsecGW2.example.jp		
80	self-identity user-fqdn kyoten-b@example.jp		
81	set isakmp-policy ISAKMP_POLICY		
82	set ipsec-policy IPsec_POLICY		
83	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)	
84	group-security client spi mask hex ffdfffff 00200000		
85	ike-version 2		
86	local-key SecretKey		
87	exit		不要
88	!		不要
89	crypto session release ipsec-lost-time 1		不要
90	crypto session release reset delete-send		不要
91	!		
92	crypto map MAP_1 ipsec-isakmp		
93	match address SELECTOR1		
94	set isakmp-profile ISAPROF_1		
95	exit		
96	!		
97	crypto map MAP_2 ipsec-isakmp		
98	match address SELECTOR1		
99	set isakmp-profile ISAPROF_2		
100	exit		
101	!		
102	interface GigaEthernet 1/1	物理インターフェース(LAN側)	
103	vlan-id 1		
104	bridge-group 1		
105	channel-group 1	LAN側論理インタフェース(Port-channel)と紐付け	
106	exit		
107	!		
108	interface GigaEthernet 2/1	物理インターフェース(WAN側)	
109	vlan-id 2		
110	bridge-group 2		
111	channel-group 2	WAN側論理インタフェース(Port-channel)と紐付け	
112	ipv6 access-group 4000 in		
113	ipv6 access-group 4009 in		
114	ipv6 access-group 4010 out		
115	exit		
116	!		
117	interface Loopback 1	Loopback1インタフェースの設定	
118	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)	
119	exit		
120	!		
121	interface Port-channel 2	論理インターフェース(WAN側)	
122	ipv6 enable		
123	ipv6 address autoconfig		
124	ipv6 nd receive-ra		
125	ipv6 dhcp service client		
126	ipv6 dhcp client-profile ipv6dns_client		
127	mtu 1500		
128	exit		不要
129	!		不要
130	interface Port-channel 1	論理インターフェース(LAN側)	不要
131	ip address 192.168.102.1 255.255.255.0		
132	exit		
133	!		
134	interface Tunnel 1		
135	tunnel mode ipsec map MAP_1		不要
136	exit		
137	!		
138	interface Tunnel 2		
139	tunnel mode ipsec map MAP_2		
140	exit		
141	!		
142	interface Tunnel 3		
143	tunnel mode ipsec		不要
144	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	不要
145	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)	
146	exit		
147	!		

	設定例(拠点)	補足	※
148	router bgp 65000		
149	bgp router-id 172.16.0.102	BGPルータID設定	
150	bgp log-neighbor-changes		不要
151	neighbor 172.16.0.1 remote-as 65000	BGPピアのAS番号の設定(iBGP)	不要
152	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	不要
153	neighbor 172.16.0.2 remote-as 65000		
154	neighbor 172.16.0.2 update-source loopback 1		
155	!		
156	address-family ipv4 unicast		
157	neighbor 172.16.0.1 disable-nexthop-validation		
158	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	
159	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	
160	neighbor 172.16.0.2 disable-nexthop-validation		
161	neighbor 172.16.0.2 encap endpoint ipv6 interface port-channel 2		
162	neighbor 172.16.0.2 encap type ipsec-tunnel		
163	redistribute connected		
164	exit		
165	!		
166	exit		
167	!		
168	ip name-server ::1		
169	!		
170	crypto ip name-server ::1		
171	!		
172	dns-server ipv6 enable		
173	!		
174	proxydns domain 1 any * any dhcp ipv6 port-channel 2		
175	proxydns address 1 any dhcp ipv6 port-channel 2		
176	!		
177	end		