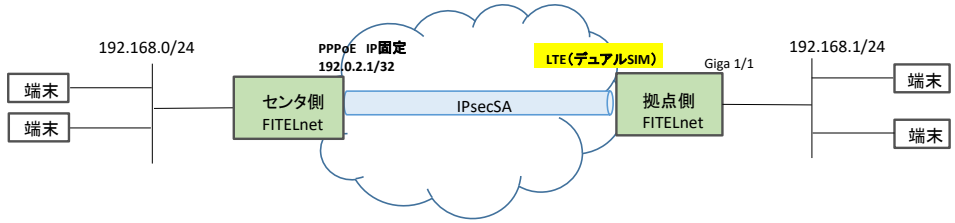
設定例

IPsec/LTEデュアルSIM～イベントアクションでSIM切り替え

概要

LTEを利用したVPN接続を行い、デュアルSIMを利用して、VPNメイン回線が接続断(SIM1断)した場合に、VPNサブ回線に切替接続(SIM2接続) を行うためのサンプルコンフィグです。



・SIM1のLTE回線断(VPN断)した後、まずSIMを切り替えずにLTEの再接続を試行します。LTEの再接続試行回数がmax-call(5回)に到達した状態で接続できない場合に、イベントアクションによりSIMプロファイルをSIM2に切り替えて、接続を試行します。
SIM2でLTE接続した後、LTE断するまでSIM2を使い続けます。

・SIM2でLTE接続断(VPN断)した場合も、上記と同様にSIM1への切り替えを行います。

※SIM切替は各通信網側に不具合があった場合を想定しています。SIM装着の不具合やSIM設定要因などで正常に接続できない場合は切り替えることができませんのでご注意ください。

・本設定例はLTEの接続失敗の一定回数繰り返しを、SIM切り替えの条件としているため、通信断してからもう片方のSIMに切り替え完了するまでに、多少時間がかかります。弊社環境では1分程度となることを確認しておりますが、お使いの環境次第では、更に長くなる可能性もございます。
Survey機能によるICMP接続監視を行って、ICMP echoの到達性がなくなった時点でSIMを切り替えることで、通信断してから切り替え完了までの時間を短縮する方法もございます。

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	3600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	1800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 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 udp any 192.0.2.1 0.0.0.0 eq 4500	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 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
4	access-list 111 deny ip any any	学習フィルタリングの設定
5	access-list 121 spi ip any any	学習フィルタリングの設定
6	ip route 0.0.0.0 0.0.0.0 tunnel 2	Default経路(PPPoE経由)
7	ip route 192.168.1.0 255.255.255.0 tunnel 1	拠点LAN宛て経路(IPsec Tunnel経由) ※"crypto ipsec policy"に"sa-up route"を設定する事により、SA確立時に対向拠点から通知されたセレクタのsrcをTunnel向けの経路として登録する事も出来ます。
8	ip route 192.168.1.0 255.255.255.0 null 0 150	IPsec Tunnelダウン時に拠点LAN宛てパケットを破棄する設定
9	ip nat list 1 192.168.0.0 0.0.0.255	NAT変換対象を定義
10	!	
11	hardware-fault-detection action reboot	ハードウェア故障を検出した際の動作を指定(装置再起動)
12	!	
13	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
14	!	
15	hostname CENTER	hostname指定
16	!	
17	crypto ipsec udp-encapsulation nat-t	NAT-T有効化
18	!	
19	crypto ipsec policy IPsec_POLICY	IPsecポリシー設定(Phase2 SAのパラメータを指定)
20	set pfs group14	PFSのDHグループを指定
21	set security-association lifetime seconds 1800	Phase2 SAのLifetime(秒)を指定 ※defaultのRekeyの開始タイミングはResponder動作時はLifetime満了の30秒前、Initiator動作時は90秒前に開始 set security-association softlimit initiate seconds 90 set security-association softlimit respond seconds 30
22	set security-association transform-keysize aes 256 256 256	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
23	set security-association transform esp-aes 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)を指定
24	set mtu 1454	暗号化後のESPパケット長におけるMTUを指定
25	set ip df-bit 0	ポストフラグメント指定 ※プリフラグメント指定の場合は削除 ※暗号化後のESPパケットのDFビットを"0"に設定します。 (defaultでは暗号化対象パケットのDFビットをコピーします)
26	set ip fragment post	ポストフラグメント指定 ※プリフラグメント指定の場合は削除

All Rights Reserved, Copyright(C) FURUKAWA ELECTRIC CO., LTD. 2020

	設定例	補足
27	exit	
28	!	
29	crypto ipsec selector SELECTOR1	セレクタ設定
30	src 1 ipv4 any	送信元セレクタを指定
31	dst 1 ipv4 any	宛先セレクタを指定
32	exit	
33	!	
34	crypto isakmp keepalive interval 35	DPD設定 ※always-sendを指定しない場合はinterval内にESP、又はDPD-R-U-THEREパケットを受信していない場合にRequestを送信します。
35	crypto isakmp log sa	SYSLOGにSA確立・切断のログを出力
36	crypto isakmp log session	SYSLOGにSession確立・切断のログを出力 ※Phase1, 2 SA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
37	crypto isakmp log negotiation-fail	SYSLOGにIKEネゴシエーション失敗のログを出力
38	!	
39	crypto isakmp policy ISAKMP_POLICY	ISAKMPポリシー設定(Phase1 SAのパラメータを指定)
40	authentication pre-share	Pre-shared Key認証を指定
41	encryption aes	暗号化アルゴリズムを指定
42	encryption-keysize aes 256 256 256	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
43	group 14	DHグループを指定
44	lifetime 3600	Phase1 SAのLifetime(秒)を指定 ※Lifetime満了時にISAKMP SAを削除し、Rekey、及びDPD契機で再接続します
45	hash sha-256	ハッシュアルゴリズムを指定
46	initiate-mode aggressive	IKE接続方式としてAggressiveモードを指定
47	exit	
48	!	
49	crypto isakmp profile PROF1	ISAKMPプロファイル設定
50	match identity host id-kyoten	リモート側のIKE IDを指定(FQDN)
51	local-address 192.0.2.1	ローカル側のIPsec終端アドレスを指定
52	self-identity address 192.0.2.1	ローカル側のIKE IDを指定(アドレス)
53	set isakmp-policy ISAKMP_POLICY	ISAKMPポリシーを指定
54	set ipsec-policy IPsec_POLICY	IPsecポリシーを指定
55	ike-version 1	IKEバージョンを指定
56	local-key SECRET-VPN	Pre-shared Keyを指定
57	exit	
58	!	
59	crypto map MAP1 ipsec-isakmp	CRYPTO MAP設定
60	match address SELECTOR1	セレクタを指定
61	set isakmp-profile PROF1	ISAKMPプロファイルと紐付け
62	exit	
63	!	
64	interface GigaEthernet 1/1	物理インタフェース(LAN側)
65	vlan-id 1	VLAN指定(ポートVLAN) ※必須 ※サブインタフェース"interface GigaEthernet 1/x.y"に設定した場合にタグVLANとして動作します。
66	bridge-group 1	bridge-group指定 ※必須 ※同一bridge-groupのポートを複数設定する場合、vlan-id, channel-groupも同じものを設定して下さい。
67	channel-group 1	論理インタフェース(Port-channel)と紐付け ※アドレス等は論理インタフェースで設定
68	exit	
69	!	
70	interface GigaEthernet 2/1	物理インタフェース(WAN側 ※PPPoE)
71	vlan-id 2	VLAN指定(ポートVLAN) ※必須
72	bridge-group 2	bridge-group指定 ※必須
73	pppoe enable	PPPoEインタフェースに指定
74	exit	
75	!	
76	interface Port-channel 1	論理インタフェース設定(LAN側 Giga 1/1と紐付け)
77	ip address 192.168.0.1 255.255.255.0	アドレス設定
78	exit	
79	!	
80	interface Tunnel 1	Tunnelインタフェース設定(IPsec Tunnel)
81	tunnel mode ipsec map MAP1	CRYPTO MAPと紐付け
82	link-state sync-sa	SA確立・切断と連動してTunnelインタフェースをアップ・ダウン
83	exit	
84	!	
85	interface Tunnel 2	Tunnelインタフェース設定(PPPoE)
86	ip address 192.0.2.1 255.255.255.255	アドレス設定
87	ip nat inside source list 1 interface	NAT+設定
88	tunnel mode pppoe profile PPPOE_PROF	PPPoEプロファイルと紐付け
89	pppoe interface gigaethernet 2/1	物理インタフェースGiga 2/1と紐付け
90	ip access-group 100 in	
91	ip access-group 111 in	
92	ip access-group 121 out	
93	exit	
94	!	
95	pppoe profile PPPOE_PROF	PPPoEプロファイル設定
96	account user@xxxx.ne.jp secret	アカウント設定
97	exit	
98	!	
99	!	
100	end	

拠点側FITELnetの設定

	設定例	補足
1	access-list 100 permit udp any eq 67 any eq 68	LTE内蔵モジュールよりアドレスを取得するための、DHCP 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 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
3	access-list 100 permit udp 192.0.2.1 0.0.0.0 eq 4500 any eq 4500	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
4	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
5	access-list 111 deny ip any any	学習フィルタリングの設定
6	access-list 121 spi ip any any	学習フィルタリングの設定
7		
8	ip route 0.0.0.0 0.0.0.0 dhcp port-channel 1	Default経路(LTE経由)

All Rights Reserved, Copyright(C) FURUKAWA ELECTRIC CO., LTD. 2020

	設定例	補足
9	ip route 192.168.0.0 255.255.255.0 tunnel 1	センターLAN宛てStatic経路(IPsec Tunnel経由)
10	ip route 192.168.0.0 255.255.255.0 null 0 150	IPsec Tunnelダウン時にセンターLAN宛てパケットを破棄する設定
11	ip nat list 1 192.168.1.0 0.0.0.255	NAT変換対象を定義：LTEモジュールでNAT変換する場合は不要 ※使用環境に合わせて設定お願いします
12	!	
13	monitor signal-quality logging lte-module interval 600	電波状態のログ出力間隔を600秒に設定
14	!	
15	syslog filter LTE_LIMIT	syslogフィルタ
16	message Call count reached limit	LTEの接続回数がmax-callに達した際に出力されるログ"Call count reached limit"を監視
17	exit	
18	!	
19	event-action 1	イベントアクション設定 ※LTEの接続回数がmax-callに達した際にSIMを切り替え
20	event syslog filter LTE_LIMIT	SYSLOGフィルタで指定したログが出力された際にイベント発生
21	action 1.1 cli exec command crypto isakmp discard	IKEネゴシエーション停止
22	action 2.1 cli exec command clear crypto sa	SA削除
23	action 3.1 cli exec command lte-module disconnect moff	LTE切断
24	action 4.1 cli exec command lte-module connect reverse moff	SIMを切り替えてLTE再接続
25	action 5.1 cli exec command no crypto isakmp discard	IKEネゴシエーション再開
26	exit	
27	!	
28	hardware-fault-detection action reboot	ハードウェア故障を検出した際の動作を指定(装置再起動)
29	!	
30	logging filter 1 LTE_LIMIT event-action	SYSLOGフィルタにマッチしたログをイベントアクションで使用します。
31	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
32	!	
33	!	
34	hostname KYOTEN	hostname指定
35	!	
36	crypto ipsec udp-encapsulation nat-t	NAT-T有効化
37	!	
38	crypto ipsec policy IPsec_POLICY	IPsecポリシー設定(Phase2 SAのパラメータを指定)
39	set pfs group14	PFSのDHグループを指定
40	set security-association always-up	常時接続設定(Trafficの有無に関わらず常にInitiatorとして接続を試みます)
41	set security-association rekey always	Trafficの有無に関わらず常にRekeyします
42	set security-association lifetime seconds 1800	Phase2 SAのLifetime(秒)を指定 ※defaultのRekeyの開始タイミングはResponder動作時はLifetime満了の30秒前、Initiator動作時は90秒前に開始 set security-association softlimit initiate seconds 90 set security-association softlimit respond seconds 30
43	set security-association transform-keysize aes 256 256 256	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
44	set security-association transform esp-aes esp-sha256-hmac	暗号化アルゴリズム(AES)とハッシュアルゴリズム(SHA-256)を指定
45	set mtu 1454	暗号化後のESPパケット長におけるMTUを指定
46	set ip df-bit 0	ポストフラグメント指定 ※プリフラグメント指定の場合は削除 ※暗号化後のESPパケットのDFビットを"0"に設定します。 (defaultでは暗号化対象パケットのDFビットをコピーします)
47	set ip fragment post	ポストフラグメント指定 ※プリフラグメント指定の場合は削除
48	exit	
49	!	
50	crypto ipsec selector SELECTOR1	セレクタ設定
51	src 1 ipv4 any	送信元セレクタを指定
52	dst 1 ipv4 any	宛先セレクタを指定
53	exit	
54	!	
55	crypto isakmp keepalive always-send interval 30	DPD設定 ※always-sendを指定しない場合はinterval内にESP、又はDPD-R-U-THEREパケットを受信していない場合にRequestを送信します。
56	crypto isakmp log sa	SYSLOGにSA確立・切断のログを出力
57	crypto isakmp log session	SYSLOGにSession確立・切断のログを出力 ※Phase1, 2 SA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
58	crypto isakmp log negotiation-fail	SYSLOGにIKEネゴシエーション失敗のログを出力
59	!	
60	crypto isakmp policy ISAKMP_POLICY	ISAKMPポリシー設定(Phase1 SAのパラメータを指定)
61	authentication pre-share	Pre-shared Key認証を指定
62	encryption aes	暗号化アルゴリズムを指定
63	encryption-keysize aes 256 256 256	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
64	group 14	DHグループを指定
65	lifetime 3600	Phase1 SAのLifetime(秒)を指定 ※Lifetime満了時にISAKMP SAを削除し、Rekey、及びDPD契機で再接続します
66	hash sha-256	ハッシュアルゴリズムを指定
67	initiate-mode aggressive	IKE接続方式としてAggressiveモードを指定
68	exit	
69	!	
70	crypto isakmp profile PROF1	ISAKMPプロファイル設定
71	match identity address 192.0.2.1	リモート側のIKE IDを指定(アドレス)
72	local-address source-interface port-channel 1	ローカル側のIPsec終端アドレスを指定
73	self-identity fqdn id-kyoten	ローカル側のIKE IDを指定(FQDN)
74	set isakmp-policy ISAKMP_POLICY	ISAKMPポリシーを指定
75	set ipsec-policy IPsec_POLICY	IPsecポリシーを指定
76	set peer 192.0.2.1	リモート側のIPsec終端アドレスを指定 ※Initiator動作させる場合に設定
77	ike-version 1	IKEバージョンを指定
78	local-key SECRET-VPN	Pre-shared Keyを指定
79	exit	
80	!	
81	crypto map MAP1 ipsec-isakmp	CRYPTO MAP設定
82	match address SELECTOR1	セレクタを指定
83	set isakmp-profile PROF1	ISAKMPプロファイルと紐付け
84	exit	
85	!	
86	interface GigaEthernet 1/1	物理インタフェース(LAN側)
87	vlan-id 2	VLAN指定(ポートVLAN) ※必須 ※サブインタフェース"interface GigaEthernet 1/x.y"に設定した場合にタグVLANとして動作します。

All Rights Reserved, Copyright(C) FURUKAWA ELECTRIC CO., LTD. 2020

	設定例	補足
88	bridge-group 2	bridge-group指定 ※必須 ※同一bridge-groupのポートを複数設定する場合、vlan-id, channel-groupも同じものを設定して下さい。
89	channel-group 2	論理インタフェース(Port-channel)と紐付け ※アドレス等は論理インタフェースで設定
90	exit	
91	!	
92	interface Port-channel 1	論理インタフェース設定(LTEと紐付け)
93	ip dhcp service client	DHCPクライアント指定
94	ip nat inside source list 1 interface	NAT+設定 :LTEモジュールでNAT変換する場合は不要 ※使用環境に合わせて設定お願いします
95	exit	
96	!	
97	interface Port-channel 2	論理インタフェース設定(LAN側 Giga 1/1と紐付け)
98	ip address 192.168.1.1 255.255.255.0	アドレス設定
99	exit	
100	!	
101	!	
102	interface Tunnel 1	Tunnelインタフェース設定(IPsec Tunnel)
103	tunnel mode ipsec map MAP1	CRYPTO MAPと紐付け
104	link-state sync-sa	SA確立・切断と連動してTunnelインタフェースをアップ・ダウン
105	exit	
106	!	
107	interface LTE-Module 1	LTEインタフェース
108	channel-group 1	論理インタフェース(Port-channel)と紐付け ※アドレス等は論理インタフェースで設定
109	sim-profile 1 SIM1 default	SIMスロットとプロファイルを紐付(default: 最初に使用)
110	sim-profile 2 SIM2	SIMスロットとプロファイルを紐付
111	ip access-group 100 in	フィルタリングの設定
112	ip access-group 111 in	フィルタリングの設定
113	ip access-group 121 out	フィルタリングの設定
114	exit	
115	!	
116	sim-profile SIM1	SIMプロファイル設定
117	account xxx123yyy@xxxxx.xx.jp XXX123	LTEの認証に使用するユーザIDとパスワードを設定
118	pdp ipv4	LTEで通信するためのPDP typeをIPv4に指定
119	apn-name lte-ocn.ntt.com	LTEで通信するためのAPNを設定
120	max-call 5	1時間当たりの接続回数のリミッタ設定を5回に設定
121	exit	
122	!	
123	sim-profile SIM2	SIMプロファイル設定
124	account xxx456yyy@xxxxx.xx.jp XXX456	LTEの認証に使用するユーザIDとパスワードを設定
125	pdp ipv4	LTEで通信するためのPDP typeをIPv4に指定
126	apn-name lte-ocn.ntt.com	LTEで通信するためのAPNを設定
127	max-call 5	1時間当たりの接続回数のリミッタ設定を5回に設定
128	exit	
129	!	
130	!	
131	end	

All Rights Reserved, Copyright(C) FURUKAWA ELECTRIC CO., LTD. 2020