# Amazon Virtual Private Cloud (Amazon VPC) とVPN接続する：FITELnet設定例

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

※ログインID/パスワードは test/test です。

| | 設定例 | 補足 |
|---|---|---|
| 1 | access-list 100 permit udp host ##Tunnel#1_Outside_IP(Virtual_Private_Gateway)## 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<br><br>##Tunnel#1_Outside_IP(Virtual_Private_Gateway)## :<br>##Tunnel#2_Outside_IP(Virtual_Private_Gateway)## :<br>VPCの設定（aws_console_vpc.pdf）の手順10でダウンロードした<br>ファイルにてご確認ください |
| 2 | access-list 100 permit udp host ##Tunnel#2_Outside_IP(Virtual_Private_Gateway)## eq 500 any eq 500 | |
| 3 | access-list 100 permit 50 host ##Tunnel#1_Outside_IP(Virtual_Private_Gateway)## any | |
| 4 | access-list 100 permit 50 host ##Tunnel#2_Outside_IP(Virtual_Private_Gateway)## any | |
| 5 | access-list 111 deny ip any any | Internet向け学習フィルタリングの設定 |
| 6 | access-list 121 spi ip any any | |
| 7 | ! | |
| 8 | ip route 0.0.0.0 0.0.0.0 tunnel 3 | デフォルト経路（PPPoE経由） |
| 9 | ip nat list 1 192.168.100.0 0.0.0.255 | Internet向けNAT設定 |
| 10 | ! | |
| 11 | crypto ipsec policy IPSECPOL_001 | IPsecポリシー設定（Tunnel#1） |
| 12 | set pfs group14 | |
| 13 | set security-association always-up | |
| 14 | set security-association rekey always | |
| 15 | set security-association lifetime seconds 3600 | |
| 16 | set security-association transform-keysize aes 256 256 256 | |
| 17 | set security-association transform esp-aes esp-sha256-hmac | |
| 18 | set mtu 1454 | OuterのMTU長：PPPoEのMTUに合わせて1454を設定 |
| 19 | exit | |
| 20 | ! | |
| 21 | crypto ipsec policy IPSECPOL_002 | IPsecポリシー設定（Tunnel#2） |
| 22 | set pfs group14 | |
| 23 | set security-association always-up | |
| 24 | set security-association rekey always | |
| 25 | set security-association lifetime seconds 3600 | |
| 26 | set security-association transform-keysize aes 256 256 256 | |
| 27 | set security-association transform esp-aes esp-sha256-hmac | |
| 28 | set mtu 1454 | OuterのMTU長：PPPoEのMTUに合わせて1454を設定 |
| 29 | exit | |
| 30 | ! | |
| 31 | crypto ipsec selector SELECTOR_1 | VPNセレクタ設定（Tunnel#1,#2） |
| 32 | src 1 ipv4 any | |
| 33 | dst 1 ipv4 any | |
| 34 | exit | |
| 35 | ! | |
| 36 | crypto isakmp log sa | crypto isakmp log コマンドで、VPNの詳細なログ情報を残すようにしてください。 |
| 37 | crypto isakmp log session | |
| 38 | crypto isakmp log negotiation-fail | |
| 39 | crypto isakmp negotiation retry timer 10 limit 3 timer-max 30 guard-time 0 | |
| 40 | crypto isakmp negotiation always-up-params interval 1000 max-initiate 10 max-pending 10 delay 1 | |
| 41 | ! | |
| 42 | crypto isakmp policy ISAPOL_001 | ISAKMPポリシー設定（Tunnel#1） |
| 43 | authentication pre-share | |
| 44 | encryption aes | |
| 45 | encryption-keysize aes 256 256 256 | |
| 46 | group 14 | |
| 47 | lifetime 28800 | |
| 48 | hash sha-256 | |
| 49 | initiate-mode main | |
| 50 | exit | |
| 51 | ! | |
| 52 | crypto isakmp policy ISAPOL_002 | ISAKMPポリシー設定（Tunnel#2） |
| 53 | authentication pre-share | |
| 54 | encryption aes | |
| 55 | encryption-keysize aes 256 256 256 | |
| 56 | group 14 | |
| 57 | lifetime 28800 | |
| 58 | hash sha-256 | |
| 59 | initiate-mode main | |
| 60 | exit | |
| 61 | ! | |
| 62 | crypto isakmp profile ISAPROF_001 | ISAKMPプロファイル設定（Tunnel#1）<br>##Tunnel#1_Outside_IP(Virtual_Private_Gateway)## :<br>##Tunnel#1_Pre-Shared_Key##:<br>VPCの設定（aws_console_vpc.pdf）の手順10でダウンロードした<br>ファイルにてご確認ください |
| 63 | match identity address ##Tunnel#1_Outside_IP(Virtual_Private_Gateway)## | |
| 64 | keepalive interval 10 | |
| 65 | set isakmp-policy ISAPOL_001 | |
| 66 | set ipsec-policy IPSECPOL_001 | |
| 67 | set peer ##Tunnel#1_Outside_IP(Virtual_Private_Gateway)## | |
| 68 | ike-version 1 | |
| 69 | local-key ascii ##Tunnel#1_Pre-Shared_Key## | |
| 70 | exit | |
| 71 | ! | |
| 72 | crypto isakmp profile ISAPROF_002 | ISAKMPプロファイル設定（Tunnel#2）<br>##Tunnel#2_Outside_IP(Virtual_Private_Gateway)## :<br>##Tunnel#2_Pre-Shared_Key##:<br>VPCの設定（aws_console_vpc.pdf）の手順10でダウンロードした<br>ファイルにてご確認ください |
| 73 | match identity address ##Tunnel#2_Outside_IP(Virtual_Private_Gateway)## | |
| 74 | keepalive interval 10 | |
| 75 | set isakmp-policy ISAPOL_002 | |
| 76 | set ipsec-policy IPSECPOL_002 | |
| 77 | set peer ##Tunnel#2_Outside_IP(Virtual_Private_Gateway)## | |
| 78 | ike-version 1 | |
| 79 | local-key ascii ##Tunnel#2_Pre-Shared_Key## | |
| 80 | exit | |
| 81 | ! | |

| | 設定例 | 補足 |
|---|---|---|
| 82 | crypto map MAP1 ipsec-isakmp | VPNピアとのセレクタ情報のエントリの設定（Tunnel#1） |
| 83 | match address SELECTOR_1 | |
| 84 | set isakmp-profile ISAPROF_001 | |
| 85 | exit | |
| 86 | ! | |
| 87 | crypto map MAP2 ipsec-isakmp | VPNピアとのセレクタ情報のエントリの設定（Tunnel#2） |
| 88 | match address SELECTOR_1 | |
| 89 | set isakmp-profile ISAPROF_002 | |
| 90 | exit | |
| 91 | ! | |
| 92 | logging buffer level informational | logging level設定：informationalを設定してください |
| 93 | ! | |
| 94 | aaa authentication login default local | |
| 95 | aaa authorization exec default local | |
| 96 | ! | |
| 97 | username test privilege 15 password 2 $1$LAruCQ4A$T3O69MOhXaiNub6xoHNsG1 | |
| 98 | ! | |
| 99 | hostname FITELnet | |
| 100 | ! | |
| 101 | interface GigaEthernet 1/1 | GigaEthernet 1/1 に Port-channel 1 をリンク付け |
| 102 | vlan-id 1 | |
| 103 | bridge-group 1 | |
| 104 | channel-group 1 | |
| 105 | exit | |
| 106 | ! | |
| 107 | interface GigaEthernet 2/1 | GigaEthernet 2/1 にてPPPoEを有効にする |
| 108 | vlan-id 2 | |
| 109 | bridge-group 2 | |
| 110 | pppoe enable | |
| 111 | exit | |
| 112 | ! | |
| 113 | interface Port-channel 1 | Port-channel 1 にLANのアドレスを設定 |
| 114 | ip address 192.168.100.1 255.255.255.0 | |
| 115 | mss 1350 | |
| 116 | exit | |
| 117 | ! | |
| 118 | interface Tunnel 1 | トンネルインタフェース設定（VPN：Tunnel#1） |
| 119 | ip address ##Tunnel#1_Inside IP(Customer_Gateway)## | |
| 120 | tunnel mode ipsec map MAP1 | |
| 121 | link-state sync-sa | |
| 122 | exit | |
| 123 | ! | |
| 124 | interface Tunnel 2 | トンネルインタフェース設定（VPN：Tunnel#2） |
| 125 | ip address ##Tunnel#2_Inside_IP(Customer_Gateway)## | |
| 126 | tunnel mode ipsec map MAP2 | |
| 127 | link-state sync-sa | |
| 128 | exit | |
| 129 | ! | |
| 130 | interface Tunnel 3 | トンネルインタフェース設定（PPPoE） |
| 131 | ip access-group 100 in | |
| 132 | ip access-group 111 in | |
| 133 | ip access-group 121 out | |
| 134 | ip nat inside source list 1 interface | |
| 135 | tunnel mode pppoe profile PPPOE_PROF0001 | |
| 136 | pppoe interface gigaethernet 2/1 | GigaEthernet 2/1にリンク付け |
| 137 | exit | |
| 138 | ! | |
| 139 | router bgp 65000 | |
| 140 | bgp router-id 192.168.100.1 | BGP設定<br>Amazon VPCの経路情報（10.0/16）を受信、かつ拠点LANの経路情報（192.168.100/24）を広告するためにBGPを使用します。<br><br>bgp log-neighbor-changes コマンドを設定してBGPのログ情報を残すようにしてください。<br><br>##Tunnel#1_Inside_IP(Virtual_Private_Gateway)##：<br>##Tunnel#2_Inside_IP(Virtual_Private_Gateway)##：<br>VPCの設定（aws_console_vpc.pdf）の手順10でダウンロードしたファイルにてご確認ください<br><br>network コマンドで拠点LANの経路情報を設定します。 |
| 141 | bgp log-neighbor-changes | |
| 142 | neighbor ##Tunnel#1_Inside_IP(Virtual_Private_Gateway)## remote-as 64512 | |
| 143 | neighbor ##Tunnel#1_Inside_IP(Virtual_Private_Gateway)## timers 10 30 | |
| 144 | neighbor ##Tunnel#2_Inside_IP(Virtual_Private_Gateway)## remote-as 64512 | |
| 145 | neighbor ##Tunnel#2_Inside_IP(Virtual_Private_Gateway)## timers 10 30 | |
| 146 | ! | |
| 147 | address-family ipv4 unicast | |
| 148 | neighbor ##Tunnel#1_Inside_IP(Virtual_Private_Gateway)## activate | |
| 149 | neighbor ##Tunnel#2_Inside_IP(Virtual_Private_Gateway)## activate | |
| 150 | network 192.168.100.0 255.255.255.0 | |
| 151 | exit | |
| 152 | ! | |
| 153 | exit | |
| 154 | ! | |
| 155 | pppoe profile PPPOE_PROF0001 | PPPoEプロファイル設定 |
| 156 | account user@xxxx.ne.jp secret | |
| 157 | exit | |
| 158 | ! | |
| 159 | end | |