FutureNet VPN Client/NET-G

接続設定ガイド SEIL 編

Ver1.0.0



目次

1.	はじめに	. 3
2	. 接続設定例 ~基本的な設定~	. 4
	2-1. ネットワーク構成	. 4
	2-2. 接続条件	. 4
	2-3.SEILの設定	. 5
	2-4.VPN Clientの設定	. 6
	2-4-1. 仮共有鍵の設定	. 6
	2-4-2.IDの設定	. 8
	2-4-3. セキュリティポリシーの設定	. 9
3	. 接続設定例 ~仮想 IP アドレスを使わない設定~	13
	3-1.VPN Clientの設定	13
	3-2.SEILの設定	13
4	. 接続設定例 ~ I P s e c とインターネットの同時接続設定~	14
	4-1.VPN Clientの設定 1	14
5	. 接続設定例 ~センター経由で I P sec 接続を行う設定~	15
	5-1. ネットワーク構成	15
	5-2.VPN Clientの設定	15
	5-3.SEILの設定	16
	5-3-1.SEIL #1(センター側)の設定	16
	5-3-2.SEIL #2(拠点側)の設定	17
6	 接続設定例 ~ NAT 環境下での接続 1 ~ 	18
	6-1. ネットワーク構成	18
	6-2. 接続条件	18
	6-3.SEILの設定	18
	6-4.VPN Clientの設定	19
_	6-5. 複数の VPN Client を接続する場合	21
7.	. 接続設定例 ~ NAT 環境トでの接続 2 ~	22
	7-1. ネットワーク構成	22
	(-2. 連用条件	22
	(-3.SEILの設定	22
	/-4.VPN Clientの設定	23

1. はじめに

FutureNet はセンチュリー・システムズ株式会社の登録商標です。

FutureNet VPN Client/NET-Gはセンチュリー・システムズ株式会社の商標です。

このソフトウェアは、国際著作権法によって保護されています。All rights reserved.

sshはSSH Communications Security Corpの米国および一部の地域での登録商標です。

SSHのロゴ、SSH Certifier、NETG Secure VPN Clientは、SSH Communications Security Corpの商標であり、一部の地域では登録されている場合もあります。その他の名前およびマークは各社の所有物です。

本書の内容の正確性または有用性については、準拠法に従って要求された場合または書面で明示的に合意された場合を除き、一切の保証を致しません。

FutureNet VPN Client/NET-Gのインストール方法および詳細な操作方法につきましては、製品CD-ROM に収録されております「ユーザーマニュアル」をご覧ください。

本ガイドは、以下のFutureNet SEIL製品に対応しております。

- ·CS-SEIL-510/C
- CS-SEIL/Turbo

本ガイドはFutureNet VPN Client/NET-G Ver2.2.2.01, CS-SEIL-510/C Ver1.83, CS-SEIL/Turbo Ver1.83 をベースに作成しております。

<u>2-1. ネットワーク構成</u>

SEILをセンター、VPN Clientを拠点とし、この間 で IPsec トンネルを生成して 192.168.0.0/24 と拠 点側ホストをセキュアに通信可能とします。



<u>2-2. 接続条件</u>

- ・PSK(共通鍵)方式で認証します。
- ・agressive モードで接続します。
- ・仮共通鍵は「ipseckey」とします。
- ・SEIL 側は固定 IP、NET-G 側は動的 IP とします。
- ・IPアドレス等は図中の表記を使うものとします。
- ・IPsec 設定で使用するパラメータ値は以下の通り とします。
 - 暗号方式 : 3DES 整合性 : SHA-1 IKEで使用するグループ : group2 拠点のID : netg.centurysys.co.jp

本ガイドではプライベート IP アドレスを用いた設 定例としておりますが、実環境ではグローバルア ドレスに置き換えて設定してください。

<u>2-3.SEILの設定</u>

以下のように、IPsecの設定を行います。

[IKEの自動接続設定]

ike auto-initiation disable

常に responder となるため、自動接続を無効にします。

[事前共有鍵と識別子の設定]

ike preshared-key add netg.centurysys.co.jp "ipseckey" VPN Clientの識別子(netg.centurysys.co.jp)、および事前共有鍵(ipseckey)を設定します。

[IKE プロポーザルの設定]

ike proposal add PHASE1 encryption 3des hash sha1 authentication preshared-key dh-group modp1024 lifetime-of-time 08h

暗号アルゴリズムとして 3des を設定します。: encryption 3des hash sha1 認証アルゴリズムとして sha1を設定します。: hash sha1 Diffie-Hellman グループとして group2を選択します。: dh-group modp1024

[IKE Peerの設定]

ike peer add NET-G address dynamic exchange-mode aggressive proposals PHASE1 peers-identifier fqdn netg.centurysys.co.jp

フェーズ1で使用するモードとして、aggressiveモードを設定します。: exchange-mode aggressive 相手識別子としてFQDNを使用します。: peers-identifier fqdn netg.centurysys.co.jp

[セキュリティアソシエーションプロポーザルの設定]

ipsec security-association proposal add PHASE2 pfs-group modp1024 authentication-algorithm hmac-sha1 encryption-algorithm 3des lifetime-of-time 01h

Diffie-Hellman グループを設定します。: pfs-group modp1024 AHで使用する認証アルゴリズムを設定します。: authentication-algorithm hmac-sha1 ESPで使用する暗号アルゴリズムを設定します。: encryption-algorithm 3des

[IKEを使ったセキュリティアソシエーションの設定]

ipsec security-association add DynamicSA tunnel dynamic ike PHASE2 esp enable トンネルモードで IPsec を使用します。: tunnel IPsec トンネルの始点 / 終点 IP アドレスに動的アドレスを使用します。: dynamic

[セキュリティポリシーの設定]

ipsec security-policy add SP01 security-association DynamicSA src 192.168.0.0/24 dst 192.168.50.1/32

送信元 IP アドレスとネットマスク長を指定します。: src 192.168.0.0/24 送信先 IP アドレスとネットマスク長を指定します。: dst 192.168.50.1/32

(VPN Clientのネットマスク長は、/32を指定してください)

<u>2-4.VPN Clientの設定</u>

Windowsのタスクトレイから、VPN Clientの"ポリシーエディタ"を開いて設定します。

<u>2-4-1. 仮共有鍵の設定</u>

📲 NET-G Secure VPN Client ポリシー エディタ 🛛 ? 🗙
セキュリティポリシャ 鍵管理
 信頼されたポリシー サーバ 信頼された証明書 回記証局 回 1700 # ディレクトリ サービス 回 1700 # ご ホストキー 「回 1700 # 「回 100 # 「回 100 # 「回 100 # 「回 100 # 「回 100 # 「回 100 # 「回 100 # 「回 100 # 「回 100 # 「回 100 # 「回 100 # 「回 100 # 「回 100 # 「回 100 # 」 100 # 」 100 # 」 100 # 」 100 # 」 100 # 」 100 # 」 100 # 」 100 #
<u>追加(2)</u> 削除(<u>R</u>) プロパティ(P) 表示(<u>V</u>)
説明 ローカル ホストの認証に使用される鍵です。
OK キャンセル 適用

「鍵管理」タブをクリックします。 「自分の鍵」を選択し、「追加」ボタンをクリック します。



「新しい認証鍵」ウィンドウが開きます。 「既知共有鍵を作成する」を選択して「次へ」ボタ ンをクリックしてください。



- 「事前共有鍵情報」画面が開きます。ここで事前共 有鍵を設定します。
- 「名前」項目には任意の設定名を入力します。 「共有シークレット」「共有シークレットの確認」 項目には、事前共有鍵(PSK)を入力して「完了」を クリックします。このとき、入力した鍵は"*" や""等で表示されます。

📱 NET-G Secure VPN Client ポリシー エディタ 🛛 💽 🗙
セキュリティ ポリシー 鍵管理
 信頼されたポリシーサーバ 信頼された証明書 別正局 リート ホスト ディレクトリ サービス 自分の鍵 ディレクトリ サービス 自分の鍵 ディレクトリ キー 新スト キー manual-pc 証明書 「netg to seil] 通 通加
<u>追加(D)</u> 削除(B) プロパティ(D) 表示(V) 説明 既知共有鍵
OK キャンセル 適用

「鍵管理」画面に戻ります。事前共有鍵情報が登録 されていることを確認したら、「適用」ボタンをク リックしてください。

「適用」ボタンをクリックしないと適切に設定され ない場合があります。

<u>2.IDの設定</u>	
	? ▲ 引き続き「鍵管理」画面で、登録した事前共有鍵 情報を選択して「プロパティ」ボタンをクリック
のない六月残認証は、当争者のあが大いの六月ソークレットに参加 て行われます。 知共有鍵情報	します。
名前: netg to seil 鍵D: 古いりには	「事前共有鍵」画面が開きますので、「ID」タブを クリックします。
有シークレット 共有シークレット: ********* 2. http://www.setational.com/setational	(この画面では仮共有鍵を変更できます。)
シークレットの確認。 ンガーブリント	
警告 一般的な語句は辞書攻撃に対する脆弱性があるため、共有シ ークレットとしては使用しないでください。	
OK	2)
清鍵	? 🗙 " ローカル " 側項目について、 プライマリ ID は
通常は、ID を指定する必要はありません。ただし、IKE アグレッシ モードでは、両方の ID を指定する必要があります。	「ホスト ドメイン名」を選択し、ホストドメイン
ーカル	るに しを パリ しよ す。 ここには、 <u>2-3.SEILの 設定</u> の [事前共有鍵と 識別子
たストドメイン名: netg.centurysys.co.jp	の設定]で指定した識別子を入力します。
モート プライマリ ID: 🕵 ID なし 💌	[事前共有鍵と識別子の設定] ike preshared-key add netg.centurysys.co.jp "ip
	」↓ 「OK」ボタンをクリックすると「鍵管理」画面に戻
浩 選択した ID は、IKE メイン モードでは使用できません。	ります。
OK ++>>セ	
T-G Secure VPN Client ポリシー エディタ	ここまでの設定が終わったら 必ず「適田・ボタ
- ○ 信頼されたポリシーサーバ - ○ 信頼されたポリシーサーバ - ○ 信頼された証明書	ンをクリックしてください。
 ■ 2011 読むしの ■ 2011 ビート ホスト ■ ディレクトリ サービス (※) 自分の鍵 	「適用」ボタンをクリックしないと適切に設定されない場合があります
□ 🐨 ホストキー 🚰 manual-pc 証明書 133 追加	
🌮 netg to seil 检 追加	続いて SEIL への IPsec 接続設定を行ないます。
追加(2)	
20月	

8

適用

OK

٢

- ++>UU

2-4-3. セキュリティポリシーの設定



ポリシーエディタの「セキュリティーポリシー」 タブをクリックします。

「VPN 接続」を選択し「追加」ボタンをクリックします。

「VPN接続を追加」画面が開きます。

VPN 接続を追加 ? 🔀				
	ゲートウェイ IP アドレス:	192.168.100.1	P	
••• <u>I</u>	リモート ネットワーク:	any 🗸		
	認証鍵	🕬 netg to seil	~	
		▶ レガシ候補を使用する(U)		
診断(D) フロパティ(P) OK キャンセル				

「ゲートウェイ名」は、右端の"IP"をクリックし て「ゲートウェイ IP アドレス」とし、SEILのWAN 側 IP アドレスを入力します。

「認証鍵」は<u>2-4-1. 仮共有鍵の設定</u>で登録した仮 共有鍵の設定名を選択します。

「レガシ候補を使用する」にはチェックを入れま す。

さらに、「リモートネットワーク」については、右 端にある"..."をクリックしてください。

ネットワーク エディタ			? 🗙		
ネットワークおよびサブネットワークに独自の名前を付けます。この 名前を後で使用して規則を作成できます。 定義されたネットワーク					
名前	IP アドレス	サブネット マスク			
any anyfi	0.0.0.0 0::0	0.0.0.0 0::0			
seil-lan	192.168.0.0	255.255.255.0			
	(新	規(<u>N)</u> 削除(E	v)		
ネットワーク名:	seil-lan				
IP アドレス:	192.168.0.0		N		
サブネット マスク:	255.255.255.0				
		ОК * +>)	セル		

"...."をクリックすると、「ネットワークエディ タ」画面が開きます。

「ネットワークエディタ」画面では、「ネットワー ク名」は任意の設定名を付けます。 「IPアドレス」「サブネットマスク」は、SEILに接 続しているLANについて入力します。

設定後に「OK」をクリックすると「セキュリ ティーポリシー」画面に戻ります。

NET-G Secure VPN Clie	nt ポリシー エディタ 🛛 💽 🔀				
セキュリティ ポリシー 鍵管理					
ポリシー: 📾 デフォルト 🔽 🛅 🕎					
 PSec 前フィルタ YPN 接続 ジロ VPN 接続 ジロ 1921681001 (self ジロ 100 ジロ 100	「 」 見 り の 評 価 順 序 ・ プロパティ(P) 診断(D)				
	K たいわれ 通田				
規則のプロパティ	? 🗙				
全般 詳細					
リモート エンドポイント ー					
「「「「「」 「」 ゲートウェイ IP アドレス:	192.168.100.1				
リモート ネットワーク:	seil-lan 🗸 🛄				
IPSec / IKE 候補					
- 😵 認証鍵:	🐖 netg toseil 🛛 👻				
● 候補テンプレート:	legacy 💙				
仮想 IP アドレスを取得する 仮想 IP アドレスは、内部ネットワークのアドレス です。 びす。 VPN ゲートウェイでは、IKE XAuth、RADIUS、 Income					
変更②					
 OK 年ャンセル					
パラメータ候補 ? 🔀					
IKE 候補と IPSec 候補	的各パラメータ値を設定します。				
IKE 候補					
暗ち化アルゴリズム:	3DES 💌				
整合性関数:	SHA-1				
整合性関数: IKE モード:	SHA-1				

IPSec 候補

暗号化アルゴリズム:

整合性関数

IPSec モード:

PFS グループ:

□ 選択した値のみを候補に加える

3DES

tunnel

HMAC-SHA-1

MODP 1024 (group 2)

OK

「セキュリティーポリシー」画面で、これまでのセ キュリティーポリシー設定が登録されていること を確認したら、「適用」ボタンをクリックしてくだ さい。

「適用」 ボタンをクリックしないと適切に設定され ない場合があります。

引き続いて、登録した設定を選択し、「プロパティ」 ボタンをクリックしてください。

「規則のプロパティ」画面が開きます。

3つある「設定」ボタンのうち、一番上の 「IPsec / IKE 候補」の「設定」ボタンをクリック します。

「パラメータ候補」画面が開きます。ここで暗号化 方式などについて設定します。

「IKE モード」は"agressive mode"に設定してく ださい。

設定後に「OK」ボタンをクリックしてください。 「規則のプロパティ」画面に戻ります。

×

~

~

キャンセル

規則のプロ	パティ		? 🗙
全般	羊糸田		
ሀቺ-ኑ:	エンドポイント ――		
	ゲートウェイ IP アドレス:	192.168.100.1	IP
-T	リモート ネットワーク:	seil-lan	✓
IPSec /	IKE 候補		
*	認証鍵	🐖 netg to seil	~
4	候補テンプレート	legacy	~
			設定
☑仮想	IP アドレスを取得する		
- • 3	仮想 IP アドレスは、内部ネ です。	ットワークのアドレス	設定
□拡張	認証 - VPN ゲートウーイでは TVE		
	ern が Fingla Califie または CHAP 認証が必要と す。	へAddin、CADIDS、 となる場合がありま	
-=±uH-			変更(<u>C</u>)
		ОК	キャンセル

仮想 IP アドレス	? 🛛
使想 IP アドレス 行います。 プロトコル O IPSec 経由の DHCP O L2TP (Layer Two Tu O IKE 設定モード	いに割り当てるプロトコルを選択するか、手動で設定を
 ● 手動で指定: IP アドレス: 	192.168.50.1
サブネット マスク:	255.255.255.0
DNS サーバと WINS DNS サーバ WINS サーバ	サーバを指定する:

「規則のプロパティ」画面に戻りましたら、続いて 「仮想 IP アドレスを取得する」にチェックを入れ、 2つ目の「設定」ボタンをクリックしてください。

「仮想 IP アドレス」 画面が開きます。

「仮想 IP アドレス」画面では、ホストが SEIL に IPsec 接続する際に使用する仮想的な IP アドレス を設定します。

SEIL から見たときには、仮想 IP アドレスが IPsec 対向のホストということになります。

「プロトコル」は"手動で指定"を選択し、任意の プライベート IP アドレスとサブネットマスクを入 力します。

ここで入力する IP アドレスは、<u>2-3.SEIL の設定</u>の [セキュリティポリシーの設定]で指定した送信先 IP アドレスと一致させます。 ただしサブネットマスクは24 ビットマスクとして

設定後に「OK」ボタンをクリックしてください。

[セキュリティポリシーの設定]

ipsec security-policy add SP01 security-association DynamicSA src 192.168.0.0/24 dst 192.168.50.1/32

ください。



「規則のプロパティ」の「詳細」画面で、[設定]を クリックします。

セキュリティの関連付けの有効期間	? 🗙			
ここでの設定は、この接続規則のみに影響があります。				
IKE セキュリティの関連付け 有効期間(分):				
480分				
有効期間 (MB): 				
IPSec セキュリティの関連付け				
▲ 有効期間 (分): 				
有効期間 (MB): 400 MB				
デフォルト OK キャンセノ	<i>L</i>			

有効期間を設定します。2-3.SEILの設定の[IKEプロポーザルの設定]、および[セキュリティアソシ エーションプロポーザルの設定]で指定した lifetime-of-timeの値に合わせます。

設定後に「OK」ボタンをクリックしてください。

以上で VPN Client の設定は完了です。

IPsec接続を開始してください。 (操作方法につきましては、製品マニュアルをご参照ください。)

[IKE プロポーザルの設定]

ike proposal add PHASE1 encryption 3des hash sha1 authentication preshared-key dh-group modp1024 **lifetime-of-time 08h**

[セキュリティアソシエーションプロポーザルの設定]

ipsec security-association proposal add PHASE2 pfs-group modp1024 authentication-algorithm hmac-sha1 encryption-algorithm 3des **lifetime-of-time 01h**

3. 接続設定例 ~ 仮想 IP アドレスを使わない設定~

前セクションの基本設定例では、VPN Clinet 側で IPsec 接続時に使われる「仮想 IP アドレス」を設 定しました。このとき SEIL 側の LAN からは、VPN Client に設定した「仮想 IP アドレス」に対して IPsec 経由での通信を行います。

この設定以外に、「仮想 IP アドレス」を使わずに、 VPN Client と SEIL シリーズを IPsec 接続すること もできます。

「仮想 IP アドレス」を使わないときは、SEIL 側の LAN からは、VPN Clinet が動作しているホスト自 身が持つ IP アドレスに対して IPsec 通信を行いま す。 <u>3-1.VPN Clinet の設定</u>

「規則のプロパティ」画面の「仮想 IP アドレスを 取得する」にチェックを入れずに設定します。

規則のプロパティ ? 🔀						
全般 詳細						
リモートエン	ドポイント					
三 ゲ	'ートウェイ IP アドレス:	192.168.100.1	IP			
J	モート ネットワーク:	seil-lan	✓			
IPSec / IKE	:候補					
🍄 IZ	温正鍵:	🕬 netg to seil	~			
(例	ミオテンプレート:	legacy	~			
			設定			
□仮想 P ● 個 の の の の の の の の の の の の の の の の の の	アドレスを取得する 想 IP アドレスは、内部ネ す。	ットワークのアドレス	設定			
	証 PN ゲートウェイでは、IKE たは CHAP 認証が必要と 。	XAuth、RADIUS、 なる場合がありま	設定			
			<u>変更(<u>C</u>)</u>			
		ОК	キャンセル			

設定後に「OK」ボタンをクリックしてください。

以上でVPN Clientの設定は完了です。

<u>3-2.SEILの設定</u>

<u>2-3.SEILの設定</u>からの変更点を記します。

[変更前]

ipsec security-association add DynamicSA tunnel dynamic ike PHASE2 esp enable ipsec security-policy add SPO1 security-association DynamicSA src 192.168.0.0/24 dst 192.168.50.1/32

[変更後] IPsecトンネルに動的アドレスを使用し、対応するセキュリティポリシを自動生成します。 ipsec security-association add AUTO tunnel auto ike PHASE2 esp enable

<この設定での注意点>

VPN Client 側が動的 IP 側の場合、IPsec 接続中に VPN Client 側の IP アドレスが何らかの理由で変わってしまうと、一時的に通信できない状態となります。 もしこのような状況になったときは、VPN Client を操作して IPsec 接続を再確立してください。 基本設定例にしたがって設定したときは、IPsec通信とインターネットの同時アクセスができません。 IPsecとインターネットを同時に利用するときは、 次の設定を行ってください。

<u>4-1.VPN Clientの設定 1</u>

「規則のプロパティ」画面の「詳細」タブをクリッ クし、「分割トンネリングを拒否する」のチェック を外します。



設定後に「OK」ボタンをクリックしてください。

以上で VPN Client の設定は完了です。

<u>5-1. ネットワーク構成</u>

VPN Clientは、センター側LAN (LAN A(center)) と拠点側LAN (LAN B)にIPsecで接続します。 拠点側にはセンター経由 (SEIL #1)でIPsec 接続 します。

IPsec トンネルは、VPN Client とSEIL #1 間、 SEIL #2とSEIL #1 間で生成します。



<u>5-2.VPN Clientの設定</u>

基本設定については<u>2-4. VPN Clientの設定</u>を参照してください。 ただし「規則のプロパティ」画面では、次のよう に設定してください。

・「リモートネットワーク」を指定する項目では、 「any」を選択します。

規則のプロパティ 🔹 🔀				
全般 🚦	羊糸田			
リモート:	エンドポイント ――			
	ゲートウェイ IP アドレス:	192.168.100.1	P	
- T	リモート ネットワーク:	any	✓ …	
IPSec /	IKE 候補			
P	認証鍵:	🕬 netg to seil	~	
v	候補テンプレート:	legacy	~	
			設定	
☑ 仮想	IP アドレスを取得する			
-	仮想 IP アドレスは、内部ネ です。	ットワークのアドレス	設定	
□拡張				
	VPN ケートウェイ Cla、IKE または CHAP 認証が必要と す。	XAuth、RADIUS、 なる場合がありま	設定	
一説明-				
		OK	キャンセル	

設定後に「OK」ボタンをクリックしてください。

以上でVPN Clientの設定は完了です。

5-3.SEILの設定

5-3-1.SEIL #1(センター側)の設定 IPsec ポリシーについては、以下のような設定をしてください。

a. (VPN Client とセンター側 LAN を結ぶ設定) 本装置側のLAN側のネットワークアドレス any 相手側のLAN側のネットワークアドレス

VPN Client の仮想 IP アドレス 192.168.50.1/32

- b. (センター側LAN と拠点側LAN を結ぶ設定) 本装置側のLAN側のネットワークアドレス any
 - 相手側のLAN側のネットワークアドレス 192.168.10.0/24

ike auto-initiation disable

ike preshared-key add netg.centurysys.co.jp "ipseckey"

ike preshared-key add 510c.centurysys.co.jp "ipseckey"

ike proposal add PHASE1 encryption 3des hash sha1 authentication preshared-key dh-group modp1024 lifetime-of-time 08h

ike peer add 510C address dynamic exchange-mode aggressive proposals PHASE1 peers-identifier fqdn 510c.centurysys.co.jp

ike peer add NET-G address dynamic exchange-mode aggressive proposals PHASE1 peers-identifier fqdn netg.centurysys.co.jp

ipsec security-association proposal add PHASE2 pfs-group modp1024 authentication-algorithm hmac-md5,hmac-sha1 encryption-algorithm 3des,des,aes128 lifetime-of-time 01h ipsec security-association add NET-G tunnel dynamic ike PHASE2 esp enable ipsec security-association add 510C tunnel dynamic ike PHASE2 esp enable

[特殊なセキュリティアソシエーションの追加]

ipsec security-association add sapass pass ipsec security-policy add sppass security-association sapass src 192.168.0.1/32 dst 192.168.0.0/24

配下の端末から SEIL #1への Telnet 通信を許可するための設定です。

ipsec security-policy add SP01 security-association NET-G src any dst 192.168.50.1/32 ipsec security-policy add SP02 security-association 510C src any dst 192.168.10.0/24

<u>5-3-2.SEIL #2(拠点側)の設定</u>

IPsec ポリシーについては、以下のような設定をしてください。

a. (センター側LAN と拠点側LAN を結ぶ設定)

本装置側のLAN側のネットワークアドレス 192.168.10.0/24 相手側のLAN側のネットワークアドレス any

ike preshared-key add 510c.centurysys.co.jp "ipseckey" ike proposal add PHASE1 encryption 3des hash sha1 authentication preshared-key dh-group modp1024 ike peer add Turbo address 192.168.100.1 exchange-mode aggressive proposals PHASE1 my-identifier fqdn 510c.centurysys.co.jp ipsec security-association proposal add PHASE2 pfs-group modp1024 authentication-algorithm hmac-sha1 encryption-algorithm 3des ipsec security-association add SA01 tunnel Ian1 192.168.100.1 ike PHASE2 esp enable

[特殊なセキュリティアソシエーションの追加]

ipsec security-association add sapass pass

ipsec security-policy add sppass01 security-association sapass src 192.168.10.1/32 dst 192.168.10.0/24

配下の端末から SEIL #2への Telnet 通信を許可するための設定です。

ipsec security-policy add SPO1 security-association SA01 src 192.168.10.0/24 dst any

これらの設定によって、VPN Client は全てのパケットをセンター側に送信し、センター側LAN および拠 点側LAN に IPsec 接続可能となります。

この設定を用いると、動的 IP アドレスを持つ拠点 / クライアント同士を IPsec 接続できるようになります。

またこの運用においては、通常のインターネットアクセスもすべてセンター経由となります。

NAT ルータの配下にあるホストから IPsec 通信を行うための設定例です。

6-1. ネットワーク構成

SEILをセンター側(LAN A)、VPN Clientを拠点側 とします。RouterはNATルータとして機能します。 この環境下で、VPN ClientとLAN A間でのセキュ アな通信を確立させます。



<u>6-2. 接続条件</u>

- ・PSK(共通鍵)方式で認証します。
- ・agressive モードで接続します。
- ・SEIL 側は固定 IP とします。
- ・NET-Gの上位ルータは、IPマスカレード処理だけ をしているものとします。
- ・それぞれの LAN は以下の設定とします。 LAN A : 192.168.0.0/24 LAN B : 192.168.1.0/24
- ・NET-Gの仮想 IP アドレスは以下のようにします。 192.168.50.1/255.255.255.0
- ・IPアドレス等は図中の表記を使うものとします。
- ・IPsec 設定で使用するパラメータ値は以下の通り とします。

暗号方式 : 3DES 整合性 : SHA-1 IKEで使用するグループ : group2 PSK : ipseckey 拠点のID : netg.centurysys.co.jp

<u>6-3.SEILの設定</u>

SEILの設定は、<u>2-3.SEILの設定</u>と同じにしてください。

SEIL は、NAT トラバーサル未対応のため、この条 件下で IPsec 接続できる VPN Client 数は「1」で す。

<u>6-4.VPN Clientの設定</u>

[規則のプロパティ < 全般 > 設定]

規則のプロパティ ? 🔀	・ゲートウェイ IP アドレス
全般 詳細	「192.168.100.1」
リモート エンドポイント デートウェイ IP アドレス: リモート ネットワーク: リモート ネットワーク: IPSec / IKE 候補 デー 認証理: (候補テンプレート: normal (飯想 IP アドレスを取得する) 仮想 IP アドレスを取得する (仮想 IP アドレスを取得する) (仮想 IP アドレスを取得する) (取得) (内) (内) (取得) (四	 ・リモートネットワーク 作成したリモートネットワーク設定を選択しま す(次項を参照ください)。 ・認証鍵:事前に作成した鍵を選択します。 ・候補テンプレート 「normal」 ・仮想 IP アドレスを使用する 「チェックなし」 ・拡張認証 「チェックなし」

[リモートネットワークの設定]

ネットワーク エディタ スットワークおよびサブネットワークに独自の名前を付けます。この 名前を後で使用して規則を作成できます。	「新規」をクリックしてい さい。	以下のように設定してくだ
定義されにエットリーク 名前 IP アドレス サブネット マスク	・IPアドレス	「192.168.0.0」
any 0.0.0 0.0.0 any6 0:0 0:0 新しいネットワーク 192.168.0.0 255.255.255.0	・サブネットマス	[「] 255.255.255.0」
新規(<u>N</u>) 削除(<u>R</u>)		
ネットワーク名: 新しいネットワーク		
IP アドレス: 192.168.0.0		
サブネットマスク: 255.255.0		
OK キャンセル		

[パラメータの設定]

IKE 1疾補		
暗ち化アルコリスム:	3DES	×
整合性関数	SHA-1	*
IKE モード:	aggressive mode	~
IKE グループ:	MODP 1024 (group 2)	~
IPSec 候補		
暗号化アルゴリズム:	3DES	~
整合性関数:	HMAC-SHA-1	~
IPSec モード:	tunnel	~
PFS グループ:	MODP 1024 (group 2)	~

「IKE/IPsec 候補」項目の「設定 . . . 」をクリック します。

IKE 候補

- ・暗号化アルゴリズム 「3DES」
- ・整合性関数 「SHA-1」
- ・IKE モード 「aggressive mode」
- ・IKE グループ 「MODP 1024 (group2)」

IPsec 候補

- ・暗号化アルゴリズム 「3DES」
- ・整合性関数 「HMAC SHA-1」
- ・PFS グループ 「MODP 1024 (group2)」

[規則のプロパティ < 詳細 > 設定]



仮想 IP アドレス	? 🛛	
● 仮想 IP アドレス 行います。 プロトコル ● IPSec 経由の DHCP ● L2TP (Layer Two Tu ● IKE 設定モード ● 手動で指示。	A(に書り当てるプロトコルを選択するか、手動で設定を 	
	192.168.50.1	
サブネット マスク:	255 255 255 0	
・ ・ ・ ・ ・ </td		
	OK キャンセル	

[規則のプロパティ < 仮想 IP アドレス > 設定] 「規則のプロパティ」画面の「仮想 IP アドレスを 取得する」にチェックを入れます。

続いて「設定」ボタンをクリックします。

仮想 IP アドレス画面では、次のように設定します。 ・手動で設定にチェック

- ・IPアドレス 「192.168.50.1」
- ・サブネットマスク 「255.255.255.0」

<u>6-5. 複数の VPN Client を接続する場合</u>

SEIL は、NAT トラバーサル未対応のため、複数の VPN Client を接続することはできません。この条 件下で IPsec 接続できる VPN Client 数は「1」で す。 NAT 環境下での IPsec 接続と、通常の IPsec 接続を 同時に行うための設定です。

<u>7-1. ネットワーク構成</u>



<u>7-2. 運用条件</u>

- ・SEIL #1 は固定 IP アドレス、Router と SEIL #2 は動的 IP アドレスとします。
- ・Router は通常のNAT ルータとして動作します。
- ・SEIL #1とPCは、NATトラバーサルによって IPsec接続を行います。
- ・SEIL #1とSEIL #2はaggressiveモードで IPsec 接続を行います。

・それぞれのLANは以下の設定とします。 LAN A : 192.168.0.0/24 LAN B : 192.168.10.0/24 LAN C : 192.168.20.0/24

- その他の IP アドレス等は図中の表記を使うものとします。
- ・IPsec 設定で使用するパラメータ値は以下の通り とします。

暗号方式	:	3DES
整合性	:	SHA-1
IKEで使用するグループ	:	group2

・VPN Client の仮想 IP アドレス設定は以下の通り とします。

192.168.50.1/255.255.255.0

<u>7-3.SEILの設定</u>

<u>7-3-1.SEIL#1の設定</u> <u>5-3-1.SEIL #1(センター側)の設定</u>を参照してくだ さい。

<u>7-3-2.SEIL#2の設定</u>

<u>5-3-2.SEIL #2(拠点側)の設定</u>を参照してください。

SEIL は、NAT トラバーサル未対応のため、この条 件下で IPsec 接続できる VPN Client 数は「1」で す。

<u>7-4.VPN Clientの設定</u>

[規則のプロパティ < 全般 > 設定]

規則のフロ	パティー		? 🛛
全般 🔡	羊糸田		
リモート:	エンドポイント ――		
	ゲートウェイ IP アドレス:	192.168.100.1	IP
.	リモート ネットワーク:	any	✓ …
IPSec /	IKE 候補		
*	認証鍵:	🐖 netg to seil	~
v	候補テンプレート:	normal	~
			設定
 ✓ 仮想 ● 優遇 	IP アドレスを取得する 仮想 IP アドレスは、内部ネ です。	、ットワークのアドレス	
	認証 VPN ゲートウェイでは、IKE または CHAP 認証が必要。 す。	XAuth、RADIUS、 となる場合がありま	設定
			<u>変更(C)</u>
		ОК	**>セル

リモートネットワークとして、anyを選択します。

その他の設定は、<u>6-4.VPN Clientの設定</u>を参照し てください。 FutureNet VPN Client/NET-G 接続設定ガイド SEIL編 v1.0.0 2008年3月版 発行 センチュリー・システムズ株式会社 Copyright (c) 2008 Century Systems Co., Ltd. All rights reserved.