# FutureNet VPN Client/NET-G

接続設定ガイド v1.1.1



1		2
1.		. 3
Ζ.		. 4
	2-1. ネットリーク構成	. 4
	2-2. 接続条件	. 4
	2–3. XR の設定	. 5
	パケットフィルタ設定	. 6
	2-4. VPN Clientの設定	. 7
	2−4−1. 仮共有鍵の設定	. 7
	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~	12
	3-1.VPN Clinetの設定	12
	3–2. XR の設定	12
4.	接続設定例 ~ IPsec とインターネットの同時接続設定~	13
	4-1.VPN Client の設定 1	13
	4-2.VPN Clientの設定 2	13
5.	接続設定例 ~センター経由で IPsec 接続をおこなう設定~	14
	5-1. ネットワーク構成	14
	5-2.VPN Clientの設定	14
	5–3. XR の設定	14
	5-3-1.XR #1(センター側)の設定	14
	5-3-2.XR #2(拠点側)の設定	15
	5-3-3. パケットフィルタ設定	15
6.	接続設定例 ~ NAT トラバーサルを用いた接続 1 ~	16
	6-1. ネットワーク構成	16
	6-2. 接続条件	16
	6–3. XR の設定	17
	[パケットフィルタ設定]	18
	6-4. VPN Clinent の設定	19
	6-6. 複数の VPN Clinent を接続する場合	21
	7-7. 異なる複数の LAN から接続する場合	21
	7-7-1. バックアップテキストでの設定	21
7.	接続設定例 ~ NAT トラバーサルを用いた接続 2 ~	22
	7-1. ネットワーク構成	22
	7-2. 運用条件	22
	7–3. XR の設定	23
	7–3–1.#1 の設定	23
	7-3-2. #2 の設定	24
	7-4.VPN Clinent の設定	25
8.	VPN Client のログについて	27

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(R)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、製品に添付の 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 XR 製品に対応しております。

- XR-380、 XR-380/DES
- ・XR-410 シリーズ
- XR-410/CD-L2
- XR-440/C
- XR-640/CD
- XR-640/CD-L2
- XR-510/C
- XR-540/C
- •XR-1000 Ver2.0 以降
- XR-1000/TX4
- ・XR-1100 シリーズ

2-1. ネットワーク構成

XR をセンター、VPN Client を拠点とし、この間で lpsec 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。

・XR 側は固定 IP、SSH 側は動的 IP とします。

・XR 側は PPPoE 接続するものとします。

・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 : ssh

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。

FutureNet VPN Client/NET-G (site host)

# <u>2-3.XRの設定</u>

IPsec 設定画面において以下のように設定します。

### [本装置の設定]

MTUの設定	
主回線使用時のipsecインターフェイスのMTU値	1500
マルチ#2回線使用時のipsecインターフェイスのMTU値	1500
マルチ#3回線使用時のipsecインターフェイスのMTU値	1500
マルチ#4回線使用時のipsecインターフェイスのMTU値	1500
バックアップ回線使用時のipseoインターフェイスのMTU値	1500
Ether Oポート使用時のipsecインターフェイスのMTU値	1500
Ether 1 ポート使用時のipsecインターフェイスのMTU値	1500
NAT Traversalの設定	
NAT Traversal	○ 使用する ⊙ 使用しない
Virtual Private設定	
纏の表示	
本装置のRSA課 (PSKを使用する場合は 必要ありません)	×

[本装置の設定1]

インターフェー スのID	[	 (例:®xr.centurysys)
上位ルータのIPアドレス	%ррр0	
インターフェー スのIPアドレス	192.168.120.1	

[IKE/ISAKMP ポリシーの設定]

IKE/ISAKMPポリシー名	
接続する本装置側の設定	本装置側の設定1 👤
インターフェー スのIPアドレス	0.0.0.0
上位ルータのIPアドレス	
インターフェー スのID	@ssh (例:@xr.centurysys)
モードの設定	aggressive モード 💌
transformの設定	1番目 group2-3des-sha1 × 2番目 使用しない × 3番目 使用しない × 4番目 使用しない ×
IKEのライフタイム	3600 秒 (1081~28800秒まで)
鍵の設定	
<ul> <li>PSKを使用する</li> <li>RSAを使用する</li> <li>(X509を使用する場合は RSAに設定してくだれい)</li> </ul>	ipseckey
X509の設定	
接統先の証明書の設定 (X509を使用しない場合は 必要ありません)	

- ・MTUの設定 必要に応じて設定します。
- ・NAT Traversal の設定 「使用しない」
- ・VirtualPrivate設定 「空欄」
- ・鍵の表示 「空欄」

- ・インタフェースの IP アドレス「192.168.120.1」
- ・上位ルータの IP アドレス 「%ppp0」
- ・インタフェースの ID 「空欄」
- ・IKE/ISAKMP ポリシー名 「任意で入力」
- ・接続する本装置側の設定

「本装置側の設定」で設定した番号と同じもの

を選択してください。

- ・インタフェースの IP アドレス 「0.0.0.0」
- ・上位ルーターの IP アドレス 「空欄」
- ・インタフェースの ID 「@ssh」 ・・・( <u>※</u> 1)
- ・モードの設定 「agressive モード」
- ・Transformの設定 1番目 「group2-3des-sha1」 2~3番目は「使用しない」
- ・IKE のライフタイム 「任意で設定」
- ・鍵の表示 「PSK を使用する」を選択し、「ipseckey」
   を入力します。

(※1)XRにおける ID の設定では"@"を付けますが、Sentinel 側では、"@"を付けない形式で設定してください。VPN Clientでも" @"を付けて設定すると接続できません。

・「Responder として使用する」

#### [IPsec ポリシーの設定]

○ 使用する ○ 使用しない ⊙ Resp	onderとして使用する   On-Demandで使用する
使用するIKEポリシー名の選択	(IK E1) 💌
本装置側のLAN側のネットワークアドレス	192.168.0.0/24 (編:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.100.1/32 (陳]:192.168.0.0/24)
PH2のTransFormの選択	3des-sha1 💌
PFS	◉ 使用する ○ 使用しない
DH Groupの選択(PFS使用時に有効)	eroup2
SAのライフタイム	28800 秒 (1081~86400秒まで)

 ・使用する IKE ポリシー名の選択 「IKE1」
 ・本装置側の LAN 側のネットワークアドレス 「192. 168. 0. 0/24」
 ・相手側の LAN 側のネットワークアドレス 「192. 168. 100. 1/32」 ・・・(※2)
 ・PH2 の Transform の設定 「3des-sha1」
 O PFS 「使用する」(推奨)
 O DH Group の選択 「group2」
 O SA のライフタイム 「任意で設定」

(※2) ここで設定したアドレスと同じ値を、VPN Clientの「仮 想 IP アドレスを取得する」項目で設定します。ただし XR の設 定では必ず" <IP address>/32"の形式で設定します。" <IP address>/24"の設定では接続できませんのでご注意ください。

パケットフィルタ設定

入力フィルタで以下の2つの設定を追加してください。

#### (1)

「インタフェース」外部接続しているポートを選択 「gre No.」 空欄 「方向」 パケット受信時 「動作」 許可 「プロトコル」 udp 「送信元アドレス」 空欄 「送信元ポート」 空欄 「あて先アドレス」 空欄

#### (2)

「インタフェース」外部接続しているポートを選択 「gre No.」 空欄 「方向」 パケット受信時 「動作」 許可 「プロトコル」 esp 「送信元アドレス」 空欄 「送信元ポート」 空欄 「あて先アドレス」 空欄

# 2-4. VPN Client の設定

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。

#### 2-4-1. 仮共有鍵の設定

# ? × セキュリティ ポリシー 鍵管理 □ · 回 信頼されたポリシー サーバ □ · ☑ 信頼された証明書 🖻 🗻 認証局 🙆 追加... (追加(D)...) 削除(R) ブロパティ(P)... 表示(V)... 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。



Ŗ	現知共有鍵に自分だけが参照	留するための名前を付けます。入力ミスを防ぐために共有シークレットを 2
H	コスノーしょう。フィンカーフリン 確認します。	トゼロを用して、美国にシークレットを設示せ タビル単合相子とシークレットを
F	既知共有鍵	
	名前:	test key
	共有シークレット	****
	共有シークレットの確認	****
	フィンガープリント (SHA-1)	: 01bc 4b2f

「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。



「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>2-4-2.IDの設定</u>

既知共有鍵	?×
プロパティ(ID	
(1) (1)	、当事者のみが知る共有シークレットに基づい
既知共有鏈情報 -	o
名前:	test key
鍵 ID:	
共有シークレット	
共有シークレット:	*****
シークレットの確認	*****
フィンガープリント	
01bc 4b2f	
警告 - 一般的な語句は辞 - クレットとしては使用	書攻撃に対する脆弱性があるため、共有シ 目しないでください。
	OK キャンセル

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」ボタンをクリックします。

「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(この画面では仮共有鍵を変更できます)。



"ローカル"側項目について、プライマリ ID は「ホスト ドメイン名」を選択し、ホストドメイン名に ID を入力し ます。

ここには XR シリーズの IPsec 設定「IKE/ISAKMP ポリシー 設定」における"インタフェース ID"と同じ ID を入力し ます。

ただしこのとき、ホストドメイン名には"@"を付けない で入力してください。

「OK」ボタンをクリックすると「鍵管理」画面に戻ります。

□ □ 信頼されたポ	リシー サーバ 油中		
	:en音 +7 b		
□ □ ブイレクトリ サ	ービス		
日 <b>四</b> 日 700歳 日 <b>空</b> ホスト キ の <b>空</b> orde			
ende 通 追加	avor alfoha		
Ssh to x 逸追加			
		CENTURY	SYSTEMS
追加(0)	削除( <u>R</u> )	プロパティ( <u>P</u> )	表示())
説明 酒日も溜切 ア/#さ	7.5		
項目を選択してたさ	:670		

ここまでの設定が終わったら、必ず「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。

続いて XR への IPsec 接続設定を行ないます。

2-4-3.	セキュ	リテ	ィポリ	シーの設定

SSH Sentinel 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	- E 🔄 😟
・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	8 月 の 評 価 順 序
	CENTURY SYSTEMS
道加(A)	プロパティ化)
説明 ローカル ホストがセキュリティ ゲートウ ークへの IPSec 接続を確立するとき( されます。	ェイ経由でリモート ブライベート ネットワ こ、仮想ブライベート ネットワークが作成
OK	キャンセル 適用

VPN 接続	を追加					? ×
	ゲートウェイ IP アドレス:	192	168	120	1	IP
- <b>P</b>	リモート ネットワーク:	any				
	認証鍵	쿋 ssh t	to xr			•
		▶ レガシ	候補を使	用する(U)	)	
診断	f( <u>D</u> ) プロパティ(P).		OK		キャンセ	211

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。

「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、XR の WAN 側 IP アドレスを入力します。

「認証鍵」は<u>1.事前共有鍵の設定</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。続いて「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



■SSH Sentinel 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	• • • •
	規 則 の 評 価 順 序 Y SYSTEMS
<u>、追加(A) 肖明余(R) プロパラ</u> 「説明	イ(P)」 … … … … … … … … … … … … …
OK *	ヤンセル 適用

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、XR 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。

「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。

	セキュリティ ゲートウェイ:	192 168	120	1 [P
(inter	リモート ネットワーク:	xr-lan		<b>•</b>
Sec /	IKE 候補			
<b>&gt;</b>	認証鍵	🐖 ssh to xr		-
	候補テンプレート	legacy		-
	「 「 「 「 「 「 「 「 「 「 」 「 」 「 」 「 」 「 」	ベッドリークのアトレス XAuth、RADIUS、 となる場合がありま		設定 設定
<b>光</b> 明 -	9.		変更	I@

3 つある「設定」ボタンのうち、一番上のボタンをクリッ クします。

E 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 (group 2)	-
Sec 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	7
PFS グループ:	MODP 1024 (group 2)	-

「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。

	セキュリティ ゲートウェイ:	192 168	120 1 <b>I</b> P
	リモート ネットワーク:	xr-lan	<b>.</b>
IPSec /	IKE 候補		
<b>?</b>	認証鍵	🐖 ssh to xr	-
0	候補テンプレート:	legacy	
	仮想 IP アドレスは、内部 です。 WZ部E VPN ゲートウェイでは、IKE または CHAP 認証が必要 す。	ネットワークのアドレス E XAuth、RADIUS、 となる場合がありま	
脱明			変更( <u>C</u> )

「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 行います。	レスに割り当う	てるプロト	コルを選択	マするか、手	■動で設定を
C IPSec 経由の DH	CP (Dynami	c Host (	Configura	tion Proto	col)
C L2TP (Layer Two	Tunneling F	Protocol)			
○ IKE 設定モード					
● 手動で指定:					
IP アドレス:	192	168	100	1	
サブネット マスク:	255	255	255	0	
🗖 DNS サーバと WIN	IS サーバを指	定する			
DNS サーバ					
WINS サーバ					
				-	

「仮想 IP アドレス」画面では、ホストが XR 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。XR からみたときには、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。 ここで設定する IP アドレスは、XR の IPsec 設定における 「IPsec ポリシー」設定の"相手側の LAN 側のネットワーク 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ください。設定後に「OK」ボタンをク リックしてください。

ここまで設定しましたら、すべての画面で「OK」をクリックして設定完了です。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

前セクションの基本設定例では、VPN Clinet 側 では 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 XR 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 経由での通信をおこないます。

この設定以外に、「仮想 IP アドレス」を使わずに、 VPN Clinet と XR 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、XR 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 通信をお こないます。

<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。



<u>3-2.XRの設定</u>

IPsec 設定の「IPsec ポリシー」にある「相手側のLAN 側のネットワークアドレス」について、 この項目を ″空欄 ″に設定します。

○ 使用する ○ 使用しない ● Resp	onderとして使用する 🕓 On-Demandで使用する
使用するIKEポリシー名の選択	(IKE1)
本装置側のLAN側のネットワークアドレス	192.168.0.0/24 (編:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	(調:192.168.0.0/24)
PH2のTransFormの選択	3des-sha1 ▼
PFS	◉ 使用する ◎ 使用しない
DH Groupの選択(PFS使用時に有効)	group2
SAのライフタイム	28800 秒 (1081~86400秒まで)

(画面は設定例です)

この2点以外については、基本設定と同様に設 定してください。

く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、XR 側が保 持している IPsec SA が無効となるまで再接続で きません。

※ XR が保持する IPsec SA が無効になるのは以下の場合です。

- XRの IPsecKeep-Alive 機能により、IPsecSA を削除したとき
- ・IPsec SA のライフタイムが経過したとき
- ・削除ペイロードを受信したとき
- ・XR 側を再起動したとき

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、つぎのいずれかの設定をおこなってくださ 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。



<u>4-2.VPN Clientの設定 2</u>

「3. 接続設定例 ~仮想 IP アドレスを使わない設定」にしたがって設定します。

5-1. ネットワーク構成

VPN Client は、センター側 LAN と拠点側 LAN に IPsec で接続します。

拠点側にはセンター側 LAN を経由して IPsec 接続します。 IPsec トンネルは、VPN Client と XR #1 間、XR #2 と XR #1 間で生成します。



5-2. VPN Clientの設定

P.3からの設定通りに設定します。 ただし「規則のプロパティ」画面では、つぎのように設定 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。(P.7を参照)

# <u>5-3.XRの設定</u>

<u>5-3-1.XR #1(センター側)の設定</u> 本装置の設定、および IKE/ISAKMP ポリシー設定について は、固定 IP - 動的 IP(aggressive モード)での接続設定 をおこないます。

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。

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 「0. 0. 0. 0/0」 相手側の LAN 側のネットワークアドレス

「192. 168. 0. 0/24」

<u>5-3-2.XR #2(拠点側)の設定</u>

本装置の設定、および IKE/ISAKMP ポリシー設定について は、固定 IP - 動的 IP(aggressive モード) での接続設定 をおこないます (P.4、もしくは IPsec 設定ガイドをご参照 下さい)。

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. 0. 0/24」 相手側の LAN 側のネットワークアドレス 「0. 0. 0. 0/0」

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。 <u>5-3-3. パケットフィルタ設定</u> 各 XR の入力フィルタで以下の 2 つの設定を加えます。

а.

「インタフェース」外部接続しているポートを選択 「gre No.」 空欄 「方向」 パケット受信時 「動作」 許可 「プロトコル」 udp 「送信元アドレス」 空欄 「送信元ポート」 空欄 「あて先アドレス」 空欄 「あて先ポート」 500

b.

「インタフェース」外部接続しているポートを選択 「gre No.」 空欄 「方向」 パケット受信時 「動作」 許可 「プロトコル」 esp 「送信元アドレス」 空欄 「送信元ポート」 空欄 「あて先アドレス」 空欄 6. 接続設定例 ~ NAT トラバーサルを用いた接続 1~

NAT トラバーサル機能を使って、NAT ルータの下にあるホ ストから IPsec 通信をおこなうための設定例です。

6-1. ネットワーク構成

XR #2 をセンター、VPN Client を拠点とします。VPN ClientとLAN Aをセキュアに通信可能とします。ただし、「ルー タ」はNAT ルータとして機能するものとします。



# 6-2. 接続条件

PSK(共通鍵)方式で認証します。

agressive モードで接続します。

・XR 側は PPPoE 接続 / 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。
 LANA: 192.168.10.0/24
 LANB: 192.168.1.0/24

・NET-Gの仮想 IP アドレスは「192.168.20.1/24」とします。

・XR 側は PPPoE 接続するものとします。

・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 PSK:「ipseckey」 拠点の ID : ssh

6. 接続設定例 ~ NAT トラバーサルを用いた接続1~

# <u>6-3.XRの設定</u>

### [本装置側の設定]

インターフェー スのIPアドレス	100.100.100.1	
上位ルータのIPアドレス	%рррО	
インターフェー スのID		(例:@×r.centurysys

### [本装置の設定]

主回線使用時のipseoインターフェイスのMTU値	1500
マルチ#2回線使用時のipsecインターフェイスのMTU値	1500
マルチ#3回線使用時のipsecインターフェイスのMTU値	1500
マルチ#4回線使用時のipsecインターフェイスのMTU値	1500
バックアップ回線使用時のipseoインターフェイスのMTU値	1500
Ether 0ポート使用時のipsecインターフェイスのMTU値	1500
Ether 1 ポート使用時のipsecインターフェイスのMTU値	1500
NAT Traversalの設定	
NAT Traversal	💿 使用する 🔘 使用しない
Virtual Private設定	%v4:192.168.20.0/2
纏の表示	
本装置のRSA類 (PSKを使用する場合は 必要ありません)	×

#### [IKE/ISAKMP ポリシーの設定]

IKE/ISAKMPポリシー名	
接続する本装置側の設定	本装置側の設定1 ▼
インターフェー スのIPアドレス	0.0.0.0
上位ルータのIPアドレス	
インターフェー スのID	@ssh (例:@xr.centurysys)
モードの設定	aggressive モード ▼
transformの設定	1番目 group2-3des-sha1 マ 2番目 使用しない マ 3番目 使用しない マ 4番目 使用しない マ
IKEのライフタイム	3600 秒 (1081~28800秒まで)
鍵の設定	
<ul> <li>PSKを使用する</li> <li>RSAを使用する</li> <li>(X509を使用する場合は RSAに設定してくだれい)</li> </ul>	ipseckey
X509の設定	
接統先の証明書の設定 (X509を使用しない場合は 必要ありません)	A

#### [IPsec ポリシーの設定]

○ 使用する ○ 使用しない ⊙ Respo	onderとして使用する 🕓 On-Demandで使用する
使用するIKEポリシー名の選択	(IKE1) 💌
本装置側のLAN側のネットワークアドレス	192.168.10.0/24 (Mg:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	vhost:\$priv (例:192.168.0.0/24)
PH2のTransFormの選択	3des-sha1 ▼
PFS	● 使用する ● 使用しない
DH Groupの選択(PFS使用時に有効)	group2
SAのライフタイム	28800 秒 (1081~86400秒まで)

- 「本装置側の設定1」を選択します。
- ・インタフェースの IP アドレス「100.100.100.1」
- ・上位ルータの IP アドレス 「%ppp0」
- ・インタフェースの ID 「空欄」
- ・NAT Traversal 「使用する」にチェック
- ・Virtual Private 設定 「%v4:192.168.20.0/24」(※3)
- ・本装置の RSA 鍵 「空欄」

(※3) VPN Client の仮想 IP アドレス設定と同じネットワークア ドレスを指定します。

- ・IKE/ISAKMP ポリシー名 「任意設定」
- ・接続する本装置側の設定 「本装置側の設定」で設定した番号と同じもの を選択してください。
- ・インタフェースの IP アドレス 「0.0.0.0」
- ・上位ルータの IP アドレス 「空欄」
- ・インタフェースの ID 「@ssh」
- ・モードの設定 「aggressive モード」
- ・transformの設定1番目「group2-3des-sha1」 2~3番目は「使用しない」
- ・IKE のライフタイム 「任意で設定」
- ・鍵の表示 「PSK を使用する」を選択し、 「ipseckey」を入力します。
- ・X.509の設定 「空欄」
- ・「Responder として使用する」にチェック。
- ・使用する IKE ポリシー名の選択 「IKE/ISAKMP ポリシー」で設定したものを選択
   ・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

「vhost:%priv」

- ・PH2のTransformの設定 「3des-sha1」
- PFS 「使用する」(推奨)
- ・DH Groupの選択 「group2」
- ・SAのライフタイム 「任意で設定」

6. 接続設定例 ~ NAT トラバーサルを用いた接続1~

[パケットフィルタ設定] 入力フィルタで以下の設定を加えます。

a.

「インタフェース」外部接続しているポートを選択 「gre No.」 空欄 「方向」 パケット受信時 「動作」 許可 「プロトコル」 udp 「送信元アドレス」 空欄 「送信元ポート」 空欄 「あて先アドレス」 500 「あて先ポート」 空欄

b.

「インタフェース」外部接続しているポートを選択 「gre No.」 空欄 「方向」 パケット受信時 「動作」 許可 「プロトコル」 udp 「送信元アドレス」 空欄 「送信元ポート」 空欄 「あて先アドレス」 4500 「あて先ポート」 空欄 [パケットフィルタ設定時の注意点] NAT ルータ配下の複数の VPN Client から同時に IPsec 接続 する場合は、XR の入力フィルタ設定を以下のようにしてく ださい。

a. 「インタフェース」外部接続しているポートを選択 「gre No.」 空欄 「方向」 パケット受信時 「動作」 許可 「プロトコル」 udp 「送信元アドレス」 空欄 「送信元ポート」 空欄 「あて先アドレス」 空欄 「あて先ポート」 空欄

# <u>6-4.VPN Clinentの設定</u>

[規則のプロパティく全般>設定]

■   ノドポイント セキュリティ ゲートウェイ:	100 100 100 1	
ッドポイント セキュリティ ゲートウェイ:	1001001001	
セキュリティ ゲートウェイ:	1001001001	
	1100.100.100.1	IP
リモート ネットワーク:	新しいネットワーク	
E 候補		
忍証鍵	🚧 test key	-
候補テンプレート:	legacy	-
		設定
P アドレスを取得する		
反想 IP アドレスは、内部ネ です。	ミットワークのアドレス	設定
VFN リードリコイ Cla、IKE または CHAP 認証が必要。 す。	スAuth、RADIUS、 となる場合がありま	
	_	変更( <u>C</u> )
	OK.	キャンセル
	ビキュリティ ケードリェイ: リモート ネットワーク: E 候補 認証鍵: 愛補テンプレート: P アドレスを取得する 反想 IP アドレスは、内部パ です。 PT PT たい、IXE または CHAP 認証が必要 す。	Uモートネットワーク: 新しいネットワーク E 候補  認証録:  Generation P アドレスを取得する 反想 IP アドレスは、内部ネットワークのアドレス です。  Appl ゲートウェイでは、IKE XAuth、RADIUS、 Static CHAP 認証が必要となる場合がありま す。  Contemporation Co

[リモートネットワークの設定]

24		14	1
<u>名則</u> 2014	0000	<u> </u>	
any6	0:0	0:0.0.0	
新しいネットワーク	192.168.10.0	255.255.255.0	
		新規( <u>N</u> )	削除( <u>R</u> )
、ットワーク名:	新しいネットワー	新規(N)	削除( <u>R</u> )
ットワーク名: ? アドレス:	新しいネットワー 192.168.10.0	新規( <u>N</u> ) ク	削除( <u>R</u> )

- ・セキュリティゲートウェイ 「100.100.100.1」
- ・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」

- ・「新規」をクリックして以下のように設定してください。
- ・IPアドレス 「192.168.10.0」
- ・サブネットマスク 「255.255.255.0」

6. 接続設定例 ~ NAT トラバーサルを用いた接続1~

IKE 1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 (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 「SHA-1」

詳細オプション項目にある

NAT 装置を経由する

の2カ所にチェックをしてください。

以上で VPN Client の設定は完了です。

• NAT-T

・PFS グループ 「MODP 1024 (group2)」

[規則のプロパティ〈詳細〉設定]



[規則のプロパティ < 仮想 IP アドレス > 設定]

C IPSec 経由の DI	HCP (Dynamic Host Configuration Protocol)
C L2TP (Layer Tw	o Tunneling Protocol)
○ IKE 設定モード	
- ● 手動C指定: IP アドレス:	192.168.20.1
サブネット マスク:	255.255.255.0
	INS サーバを指定する:
DNS サー/%	
WINS サーバ	

「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 「192.168.20.1」
- ・サブネットマスク 「255. 255. 255. 0」

#### <u>6-6. 複数の VPN Clinent を接続する場合</u>

NAT ルータ配下の複数の VPN Client から同時に IPsec 接続 する場合は、それぞれの VPN Client に重複しないインタ フェース ID、仮想 IP アドレスを設定してください。

XR 側では、インタフェース ID ごとに IKE/ISAKMP ポリシー 設定・IPsec ポリシー設定を追加してください。

また XR のフィルタ設定も異なります。 フィルタ設定については P18[パケットフィルタ設定時の 注意点]を参照してください。

<u>7-7. 異なる複数の LAN から接続する場合</u> 複数の異なる LAN 内にある VPN Client から IPsec 接続す る場合は、XR の「Virtual Private 設定」を次のように設 定します。

(何)%v4:192.168.10.0/24,%v4:192.168.20.0/24 ,%v4:192.168.30.0/24

LAN ごとの Virtual Private 設定を"カンマ"で区切り設 定していきます(例ではレイアウトの都合上改行していま すが、実際の設定では続けて設定してください)。

またファームウェアのバージョンによっては、GUI 上で最 大 4 つまで Virutal Private 設定ができるようになってい ます。

<u>7-7-1. バックアップテキストでの設定</u> 以下の項目で設定します。

・[IPsec 本装置、本装置側の設定 1] VIRTUALPRIVATE= ;Virtual Private

項目で、"VIRTUALPRIVATE="に続いて上記(例)のよう に入力します。

バックアップテキストで設定したときには、設定の復帰 時に XR 本体が自動的に再起動されます。 NAT トラバーサルによる IPsec 接続と、通常の IPsec 接続 を同時におこなうための設定です。

# 7-1. ネットワーク構成



(site host)

<u>7-2. 運用条件</u>

・R1、R2、R3 ともに PPPoE 接続をします。

- ・R1 は固定 IP アドレス、R2 と R3 は動的 IP アドレス とします。
- ・R2 は通常の NAT ルータでの動作とします。
- ・R1 と PC は、NAT トラバーサルによって IPsec 接続を おこないます。
- ・R1 と R3 は aggressive モードで IPsec 接続をおこな います。
- それぞれのLANは以下の設定とします。
  LAN A : 192.168.10.0/24
  LAN B : 192.168.100.0/24
  LAN C : 192.168.0.0/24
- 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 192.168.50.1/ 255.255.255.0 とします。

7-	-3.XR の設定			
<u>7-</u> [:	<u>·3–1. #1 の設定</u> 本装置側の設定 1]			
	インターフェー スのIPアドレス	10.10.1	0.1	
ĺ	上位ルータのIPアドレス	Жррр0		
	インターフェースのID			(例:@xr.centurysys)
[:	本装置の設定]			
	NAT Traversal		● 使用する ○ 使用しない	

NAT Traversal	◎ 使用する ◎ 使用しない
Virtual Private設定	%v4:192.168.50.0/24

NAT-T の設定をおこないます。

#### [IPsec ポリシーの設定 1] ○使用する ○使用しない ● Responderとして使用する ○ On-Demandで使用する 使用するIKEポリシー名の選択 (IKE1) 💌 本装置側のLAN側のネットワークアドレス 192.168.10.0/24 (第):192.168.0.0/24) 相手側のLAN側のネットワークアドレス 192.168.0.0/24 (第1:192.168.0.0/24) PH2のTransFormの選択 すべてを送信する 💌 PFS ● 使用する ○ 使用しない DH Groupの選択(PFS使用時に有効) 指定しない 💌 SAのライフタイム 28800 秒 (1081~86400秒まで)

# [IPsec ポリシーの設定 2]

DISTANCE

○ 使用する ○ 使用しない ◎ Responderとして使用する ○ On-Demandで使用する

1

(1~255まで)

使用するIKEポリシー名の選択	(IKE2)
本装置側のLAN側のネットワークアドレス	192.168.10.0/24 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	vhost:%priv (例:192.168.0.0/24)
PH2のTransFormの選択	すべてを送信する 💌
PFS	◉ 使用する ○ 使用しない
DH Groupの選択(PFS使用時に有効)	指定しない
SAのライフタイム	28800 秒 (1081~86400秒まで)
DISTANCE	1 (1~255まで)

#### [IKE/ISAKMP ポリシーの設定 1]

IKE/ISAKMPポリシー名	
接続する本装置側の設定	本装置側の設定1 ▼
インターフェー スのIPアドレス	0.0.0.0
上位ルータのIPアドレス	
インターフェー スのID	@branch (例:@xr.centurysys)
モードの設定	aggressive モード 💌
transformの設定	1番目 group2-3des-sha1 2番目 使用しない 3番目 使用しない 4番目 使用しない ▼
IKEのライフタイム	3600 秒 (1081~28800秒まで)
鍵の設定	
<ul> <li>PSKを使用する</li> <li>RSAを使用する</li> <li>(X509を使用する場合は RSAに設定してください)</li> </ul>	test

# [IKE/ISAKMP ポリシーの設定 2]

IKE/ISAKMPポリシー名	
接続する本装置側の設定	本装置側の設定1 👤
インターフェー スのIPアドレス	0.0.0.0
上位ルータのIPアドレス	
インターフェー スのID	@client (P):@vr.centurysys)
モードの設定	aggressive モード ▼
transformの設定	1番目 group2-3des-sha1 ▼ 2番目 使用しない ▼ 3番目 使用しない ▼ 4番目 使用しない ▼
IKEのライフタイム	3600 秒 (1081~28800秒まで)
鍵の設定	
<ul> <li>PSKを使用する</li> <li>RSAを使用する</li> <li>(X509を使用する場合は RSAに設定してくだれい)</li> </ul>	test2

[ パケットフィルタ設定 ] 入力フィルタで以下の設定を加えます。

a. 「インタフェース」外部接続しているポートを選択 「gre No.」 空欄 「方向」 パケット受信時 「動作」 許可 「プロトコル」 udp 「送信元アドレス」 空欄 「送信元ポート」 空欄 「あて先アドレス」 500 「あて先ポート」 空欄

#### b.

「インタフェース」外部接続しているポートを選択 「gre No.」 空欄 「方向」 パケット受信時 「動作」 許可 「プロトコル」 udp 「送信元アドレス」 空欄 「送信元ポート」 空欄 「あて先アドレス」 4500 「あて先ポート」 空欄

#### C.

「インタフェース」外部接続しているポートを選択 「gre No.」 空欄 「方向」 パケット受信時 「動作」 許可 「プロトコル」 esp 「送信元アドレス」 空欄 「送信元ポート」 空欄 「あて先アドレス」 空欄 [パケットフィルタ設定時の注意点] NAT ルータ配下の複数の VPN Client から同時に IPsec 接続 する場合は、XR の入力フィルタ設定を以下のようにしてく ださい。

#### a.

「インタフェース」外部接続しているポートを選択 「gre No.」 空欄 「方向」 パケット受信時 「動作」 許可 「プロトコル」 udp 「送信元アドレス」 空欄 「送信元ポート」 空欄 「あて先アドレス」 空欄

# b.

「インタフェース」外部接続しているポートを選択 「gre No.」 空欄 「方向」 パケット受信時 「動作」 許可 「プロトコル」 esp 「送信元アドレス」 空欄 「送信元ポート」 空欄 「あて先アドレス」 空欄

7. 接続設定例 ~ NAT トラバーサルを用いた接続 2~

# <u>7-3-2.#2の設定</u> [本装置側の設定 1]

インターフェー スのIPアドレス	ЖрррО	
上位ルータのIPアドレス		
インターフェー スのID	@branch	(例:@xr.centurysys)

# [本装置の設定]

設定の必要はありませんが、MTU 値については適宜変更できます。

[IKE/ISAKMP ポリシーの設定 1]

IKE/ISAKMPポリシー名	
接続する本装置側の設定	本装置側の設定1 👤
インターフェー スのIPアドレス	10.10.10.1
上位ルータのIPアドレス	
インターフェー スのID	(例:@vr.centurysys)
モードの設定	aggressive モード 💌
transformの設定	1番目 group2-3des-sha1 2番目 使用しない 3番目 使用しない 4番目 使用しない ▼
IKEのライフタイム	3600 秒 (1081~28800秒まで)
纏の設定	
<ul> <li>PSKを使用する</li> <li>RSAを使用する</li> <li>(X509を使用する場合は RSAに設定してください)</li> </ul>	test 💌

#### [IPsec ポリシーの設定 1]

● 使用する ○ 使用しない ○ Resp	onderとして使用する 🛛 On-Demandで使用する
使用するIKEポリシー名の選択	(IKE1)
本装置側のLAN側のネットワークアドレス	192.168.0.0/24 (M):192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.10.0/24 (M):192.168.0.0/24)
PH2のTransFormの選択	すべてを送信する
PFS	● 使用する ○ 使用しない
DH Groupの選択(PFS使用時に有効)	指定しない
SADライフタイム	28800 秒 (1081~86400秒まで)
DISTANCE	1 (1~255まで)

[パケットフィルタ設定]

入力フィルタ設定で、「udp/500 番ポート」と「esp プロト コル」を解放してください。

# <u>7-4.VPN Clinentの設定</u>

[規則のプロパティく全般>設定]

規則のフロ	パティ		<u>? ×</u>
全般	羊糸田 】		
リモート	エンドポイント		
	セキュリティ ゲートウェイ:	<b>1</b> 10.10.10.1	P
Sum	リモート ネットワーク:	192.168.10.0/24	
IPSec /	IKE 候補		
	認証鍵:	🛩 test key	-
0	候補テンプレート	legacy	•
			設定
↓ 仮想	見 IP アドレスを取得する		
-1	仮想IPアドレスは、内留 です。	Pネットワークのアトレス	
□ 拡引			
	VPN ゲートウェイでは、IP または CHAP 認証が必 す。	(E XAuth、 RADIUS、 要となる場合がありま	
- 記日月 -			<b>杰</b> 軍(0) 【
			<u>&amp;</u>
		OK	キャンセル

「仮想 IP アドレスを取得する」にチェックします。

#### [仮想 IP アドレス画面]

仮想 IP アドレス	? ×
● 仮想 IP アドレスに割り当てるプロトコルを選択するか、手動で ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	設定を
לעבאסל	
C IPSec 経田()) DHCP (Dynamic Host Configuration Protocol)	
() L2TP (Layer Two Tunneling Protocol)	
192168501	
IP DELOCION	
サブネットマスク: 255.255.255.0	
DNS サーバと WINS サーバを指定する:	
DNS サーバ:	
WINS サーバ	
[OK] ≠γ≻/	セル



VPN Client は NAT-T によって IPsec 接続をおこないます ので、「NAT 装置を経由する」と「NAT-T」にチェックを入 れてください。

[パラメータ候補画面]

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 (group 2)	-
PSec 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)	-

[事前共有鍵 < プロパティ > 画面]

既知共有鍵	? ×
プロパティ   ID	
の日本 既知共有鍵認証は て行われます。	は、当事者のみが知る共有シークレットに基づい
既知共有鍵情報	
名前:	test key
鍵 ID:	ssh
共有シークレット	
共有シークレット	****
シークレットの確認	kokokok
フィンガープリント f090 669e	
警告 一般的な語句は辞 ークレットとしては使	書攻撃に対する脆弱性があるため、共有シ 用しないでください。
	OK キャンセル

#### [事前共有鍵 <ID> 画面]

既知共有鏈	<u>? ×</u>
לםואדא ID	
通常は、ID を モードでは、両	措定する必要はありません。ただし、IKE アグレッシブ 前方の ID を指定する必要があります。
_□-カル	1
プライマリ ID:	🔁 ホスト ドメイン名
ホスト ドメイン名:	client
 J£~ト	
プライマリ ID:	🕵 ID なし 📃
「警告」 選択した ID	は、IKE メイン モードでは使用できません。
	キャンセル

# 8. VPN Client のログについて

VPN Client では「IKE のログウィンドウ」を表示させることで、Ipsec の状態を把握することができます。

万が一 IPsec が確立できない場合もログを確認することで、ある程度の原因追及が可能です。

ここでは、IPsec が確立できないときの主なログの読み方 を説明します。 [正常に接続できたときのログ表示例]

0.0.0.0:500 (Initiator) <-> xxx.xxx.xxx.xxx:500 { bee8ab89 5a000003 - 647c30a6 94998148 [-1] / 0x00000000 } Aggr: MESSAGE: Phase 1 version = 1.0, auth\_method = Pre shared keys, cipher = 3des-cbc, hash = sha1, prf = hmac-sha1, life = 0 kB / 14400 sec, key len = 0, group = 2

Phase-1 [initiator] between fqdn(udp:500, [0..2]=ssh) and ipv4(any:0, [0..3]=xxx.xxx.xxx.xxx) done.

0.0.0.0:500 (Initiator)  $\langle - \rangle xxx.xxx.xxx.xxx.xxx:500$ { bee8ab89 5a000003 - 647c30a6 94998148 [0] / 0xbaf3de8e } QM; MESSAGE: Phase 2 connection succeeded, Using PFS, group = 2

0.0.0.0:500 (Initiator) <-> xxx.xxx.xxx.xxx:500 { bee8ab89 5a000003 - 647c30a6 94998148 [0] / 0xbaf3de8e } QM; MESSAGE: SA[0][0] = ESP 3des, life = 409600 kB/3600 sec, group = 2, tunnel, hmacsha1-96, key len = 0, key rounds = 0

Phase-2 [initiator] done bundle 2 with 2 SA's by rule 21:`ipsec [IKE フェーズ1が確立できないときのログ表示 例 その1]

0.0.0.0:500 (Initiator) <-> xxx.xxx.xxx.xxx:500 { a2196204 1e000003 - 00000000 00000000 [-1] / 0x00000000 } Aggr; Connection timed out or error, calling callback

Phase-1 [initiator] between fqdn(udp:500, [0..2]=ssh) and ipv4(udp:500, [0..3]=xxx.xxx.xxx.xxx) failed; Timeout.

このログは IKE フェーズ1ネゴシエーションがうまく開始 できていないことを示しています。以下の点をご確認くだ さい。

・IPsec ゲートウェイの IP アドレス設定 XR 側:本装置の設定「インタフェースの IP アドレス」 SSH 側:セキュリティーポリシー「セキュリティーゲート ウェイ」(P.8)

・インタフェース ID

XR 側: IKE/ISAKMP ポリシー設定「インタフェースの ID」 SSH 側:事前共有鍵設定「ID」のホストドメイン名 (P.6) ※ XR 側は <@ID> の入力、SSH 側は <ID> の入力

・モード間違い

XR 側: IKE/ISAKMP ポリシー設定「モードの設定」 SSH 側:規則のプロパティ「パラメータ候補」(P.9) ※どちらも"aggressive モード"で設定します。

・XR 側でステートフルパケットインスペクションが有効に なっていませんか?有効になっているのであれば、無効に するか、IPsec 用のフィルタ設定をしてください。 [IKE フェーズ1が確立できないときのログ表示 例 その2]

0.0.0.0:500 (Initiator) <-> xxx.xxx.xxx.xxx:500 { 878a3c20 b4000000 - 0e6a4ab9 116f8cc3 [-1] / 0x00000000 } Aggr; Hash value mismatch

Phase-1 [initiator] between fqdn(udp:500, [0..2]=ssh) and ipv4(udp:500, [0..3]=xxx.xxx.xxx. xxx) failed; Authentication failed.

0.0.0.0:500 (Initiator) <-> xxx.xxx.xxx.xxx:500 { 878a3c20 b4000000 - 0e6a4ab9 116f8cc3 [-1] / 0x00000000 } Aggr; Error = Authentication failed (24)

このログは IKE フェーズ1ネゴシエーションを始めていま すが、ホスト認証で失敗していることを示しています。共 有鍵設定が間違っている可能性が高いので、以下の点をご 確認ください。

XR 側: IKE/ISAKMP ポリシー設定の「鍵の設定」aggressive モードの場合は PSK 方式のみ使用可能です。

SSH 側: 鍵管理「プロパティ」 (P.6)

※同じ文字列の鍵を入力します。

[IKE フェーズ 2 が確立できないときのログ表示 例]

0.0.0.0:500 (Initiator) <-> xxx.xxx.xxx.xxx:500 { 0202f991 16000008 - 0e6a4ab9 116f8cc3 [-1] / 0x00000000 } Aggr; MESSAGE: Phase 1 version = 1.0, auth\_method = Pre shared keys, cipher = 3des-cbc, hash = sha1, prf = hmac-sha1, life = 0 kB / 14400 sec, key len = 0, group = 2

Phase-1 [initiator] between fqdn(udp:500, [0..2]=ssh) and ipv4(any:0, [0..3]=xxx.xxx.xxx. xxx) done.

0.0.0.0:500 (Initiator) <-> xxx.xxx.xxx.xxx:500 { 0202f991 16000008 - 0e6a4ab9 116f8cc3 [0] / 0xb-00c7f69 } QM; Connection timed out or error, calling callback

Phase-2 [initiator] for ipv4(icmp:0, [0..3]=192.168. 100.1) and ipv4(icmp:0, [0..3]=192.168.1.1) failed; Timeout.

このログは IKE フェーズ 2 ネゴシエーションがうまくでき ていないことを示しています。以下の点をご確認ください。

- XR 側: IPsec ポリシー設定 「本装置側の LAN 側のネットワー クアドレス」と「相手側の LAN 側のネットワーク アドレス」
- SSH 側: セキュリティーポリシー「ネットワークエディタ」 と規則のプロパティ「仮想 IP アドレス」(P.9)

FutureNet VPN Client/NET-G 接続設定ガイド v1.1.1 2006 年 8 月版 発行 センチュリー・システムズ株式会社 2006 CENTURYSYSTEMS, INC. All rights reserved.