BROADBAND GATE

インターネット VPN 対応ブロードバンドルータ



FutureNet XR VPN Client 接続設定ガイド

センチュリー・システムズ 株式会社

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 XR VPN Client 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 Sentinel およびSSH Accession 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。

SSH Sentinel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、オンラインヘルプ「SSH Sentinel1.4 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
- ・XR-1000 Ver2.0 以降
- XR-1000/TX4

接続環境例

<u>ネットワーク構成</u>	接続条件
XR をセンター、SSH Sentinel 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。	・PSK(共通鍵)方式で認証します。
	・agressiveモードで接続します。
192.168.0.0/24	・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 (センター)	・XR 側は PPPoE 接続するものとします。
192.168.120.1	・IPアドレス等は図中の表記を使うものとします。
Internet	・IPsec設定で使用するパラメータ値は以下の通り とします。
Dynamic IP SSH (拠点) ID = "ssh"	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。

XRの設定

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ipsec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 ④ 使用しない
Virtual Private設定	
鐘の表示	
本装置のRSA22 (PSKを使用する場合は 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」

[本装置の設定1]

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

[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	
 PSKを使用する RSAを使用する (X509を使用する場合は RSAに設定してください) 	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)	X

- ・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」 ・・・(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 "0"を付けますが、
 Sentinel 側では、"0"を付けない形式で設定してください。SSH Sentinel でも "0"を付けて設定すると接続できません。

[IPsecポリシーの設定]

〇 使用する	○ 使用しない	Responderとして使用する	〇 On-Demandで使用する

使用するIKEポリシー名の選択	(ŭK E1) ▼
本装置側のLAN側のネットワークアドレス	192.168.0.0/24 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.100.1/32 (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
SADライフタイム	28800 秒 (1081~86400秒まで)

- ・「Responder として使用する」
- ・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

^r192.168.0.0/24 J

- ・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」 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」

(2)ここで設定したアドレスと同じ値を、SSH Sentinel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。

SSL Sentinelの設定

ポリシーエディタを開いて設定します。

<u>1. 仮共有鍵の設定</u>

📲 SSH Sentinel ポリシー エディタ	? ×
セキュリティ ポリシー 鍵管理	
日 信頼されたポリシー サーバ 日 (言頼されたポリシー サーバ 日 (言頼された君田書) 田 (二) 見てした ホスト 田 (二) リモート ホスト 日 (二) リモート ホスト 日 (二) リモート ホスト 田 (二)	C CENTURY SYSTEMS
(追加(1)) 前除(12)	ブロパティ(2) 表示(2)
- 説明 □ーカル ホストの認証に使用される翁	ect.
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。 「事前共有鍵を作成する」を選択して「次へ」ボタ ンをクリックしてください。

		×
	4h	ssh
照するための名前を付けます。入力ミ ントを使用して、実際にシークレットを3	スを防かために共有シークレットを 2 表示せずに通信相手とシークレットを	
ssh to xr		

1): 01bc 4b2f		
< 戻る(日) 完了 キャン	セル
	ださい。 	ださい。 (たろの) 完了 キャン

「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、事前共有鍵を入力して「完了」をク リックします。

■ SSH Sentinel ポリシー エディタ	? ×
セキュリティ ポリシー 鍵管理	
 ● ② 信頼されたポリシー サーバ ● ③ 信頼された起印書 ● ④ 認証局 ● ④ 認証局 ● ● ○ 記証局 ● ● ○ ホルトリ サービス ● ● ○ ホルトレ サービス ● ● ○ ホルトレ キー ● ● ○ ○ ホルト キー ● ● ○ ○ ホルト キー ● ● ● ○ ○ ホルト キー ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	CENTURY SYSTEMS
<u>追加(D)</u> 削除(<u>R</u>)	
前204 事前共有鍵	
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、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。

<u>2.IDの設定</u>

事前共有鍵		? ×
プロパティ(ID	\supset	
	「前共有鍵認証は、 「行われます。	当事者のみが知る共有シークレットに基づい
事前共有鍵情	₩ ₩ ₩ ₩ ₩ ₩ ₩ ₩	
并	ろ前: 建 ID:	ssh to xr
共有シークレッ	۶ <u> </u>	
÷	も有シークレット:	kokokokok
3	ノークレットの確認	****
フィンガープリン 0	∙⊩ 1bc 4b2f	
	→般的な語句は辞書 -クレットとしては使用	■攻撃に対する脆弱性があるため、共有シ しないでください。
		OK キャンセル

「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」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)。

事前共有鍵	? ×
プロパティ ID	
通常は、ID モードでは、	を指定する必要はありません。ただし、IKE アグレッシブ 両方の ID を指定する必要があります。
ローカル プライマリ ID: ホスト ドメイン名:	島 ホスト ドメイン名 🔹
リモート プライマリ ID:	👰 ID &L
警告 <u> 達</u> 選択した I	D は、IKE メイン モードでは使用できません。
	OK キャンセル

 "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。

■SSH Sentinel ポリシー エディタ セキュリティ ポリシー 鍵管理	? 🗙
 ● ② 信頼されたポリシー サーバ ● ② 信頼された記明書 ● ③ 記録声局 ● ● リモート ホスト ● ③ ディレクトリ サービス ● ● 自分の鍵 ● ○ 加点 ● ○ 読む to xr ● ○ 追加。 	CENTURY SYSTEMS
道加(D)	ロパティ(D) 美示(y)
ОК	キャンセル 適用

「OK」ボタンをクリックすると「鍵管理」画面に戻 ります。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. セキュリティポリシーの設定

規
E II
则
評
価
川直
序
0
₩斤(<u>D</u>)

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」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1.事前共有鍵の設定で登録した仮共 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。

「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。

名前を後 定義されたネットワー	で使用して規則 .ヵ	を作成できます。	
名前	- IP アドレス	サブネット マスク	
any xr−lan	0.0.0.0 192.168.0.0	0.0.0.0 255.255.255.0	
		新規(<u>N</u>)	削除(<u>R</u>)
ネットローカタ・	xr-lan	新規(N)	肖邶余(<u>R</u>)
ネットワーク名: IP アドレス:	xr-lan	新規(<u>N</u>)	削除(R)
ネットワーク名: IP アドレス: サゴネット マスル	xr-lan 192 255	新規(N) 168 0 255 255	削除(E) 0 3



規則のプロパティ ? × 全般詳細 リモート エンドポイント セキュリティ ゲートウェイ: 192 ΙP 168 120 1 リモート ネットワーク: xr-lan • ... IPSec / IKE 候補 🥐 i21148 🐖 ssh to xr • legacy -候補テンプレート 設定... 仮想 IP アドレスを取得する
 仮想 IP アドレスは、内部ネットワークのアドレス
 です。 設定. □ 拡張認証 VPN ゲートウェイでは、IKE XAuth、RADIUS、 または CHAP 認証が必要となる場合がありま す。 設定. - || 党印月 変更(<u>C</u>)... キャンセル OK

「ネットワークエディタ」画面が開きます。

「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、XR に接続 している LAN について入力し、「OK」をクリックし ます。

「セキュリティーポリシー」画面に戻ります。 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、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。

引き続いて、登録した設定の「プロパティ」を開 いてください。

「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、一番上のボタンを クリックします。

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)	-

則のプロパ 全般	ティ ¥細 】		3
リモート:	・ エンドポイント —		
	セキュリティ ゲートウェイ:	192 168	120 1 <u>I</u> P
Simu	リモート ネットワーク:	xr-lan	▼
IPSec /	IKE 候補		
?	認証鍵	🐖 ssh to xr	-
•	候補テンプレート	legacy	•
▼ 仮想 ↓~■	見 IP アドレスを取得する 仮想 IP アドレスは、内部 です。	ネットワークのアドレス	atte
□ 拡張	WZ証 VPN ゲートウェイでは、IKI または CHAP 認証が必要 す。	E XAuth、RADIUS、 要となる場合がありま	
		OK	キャンセル

- 🔄 לםגםוע — — — — — — – – – – – – – – – – – – –					
○ IPSec 経由の DHCP	^o (Dynami	c Host C	>onfigura	tion Proto	ocol)
C L2TP (Layer Two T	unneling F	rotocol)			
 ● IKE 設定モニト ● 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	
ー DNS サーバと WINS	サーバを指	定する:			
DNS サーバ					
WINS サーバ					

「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。

「OK」ボタンをクリックして「規則のプロパティ」 画面に戻ります。

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ま す。

「仮想 IP アドレス」画面が開きます。 ここでは XR に IPsec 接続する際に、この PC が使用 する仮想的な IP アドレスを設定します。

「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 ビットマスクとします。

ここまで設定できましたら、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(操作方法はオンラインヘルプをご参照 ください)。

IPsec 接続とインターネット接続を同時に行う設定

前セクションまでの設定では、SSH Sentinel 側は IPsec とインターネットに同時 に接続できません。SSH Sentinel で Ipsec レスを取得する」にはチェックを入れま を確立しているときは IPsec のみ通信可能 せん。 となります。

IPsec とインターネットに同時に接続する には、以下のように設定してください。

仮想 IP アドレスを使わない方法

XR 側の設定

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	(m):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	(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)	eroup2
SAのライフタイム	28800 秒 (1081~86400秒まで)

(画面は設定例です)

SSH Sentinel 側の設定

「規則のプロパティ」画面の「仮想 IP アド

規則のプロパ	<u>ਰ</u> ੋਮ			? ×
全般計	飾田			
リモートコ	こンドポイント ――			_
	セキュリティ ゲートウェイ:	192 168	120 1	IP
Suma	リモート ネットワーク:	xr-lan	•	
IPSec /	IKE 候補			
?	認証鍵	🐖 ssh to xr		-
	候補テンプレート:	legacy		•
-				
(仮想	IP アドレスを取得する			=
41-1	100.00 11 アドレスは、141804 です。	ドットノークのアトレス		
□ 拡張	121 1			
	- VPN ゲートウェイでは、IKE または CHAP 認証が必要	、XAuth、RADIUS、 となる場合がありま	設定	
_=====	ब .			
6/L ⁴ /1			変更(C)	1
				-
			territe	
		UK		.70

(画面は設定例です)

この2点以外については、前セクションま でと同様に設定してください。

この設定では、VPN クライアント(が動作 している PC)自身が保持するグローバル IP アドレスを使って VPN 接続します。

<この設定での注意点>

SSH Sentinel 側が動的 IP 側の場合、 IPsec 接続中に SSH Sentinel 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

仮想 IP アドレスを使う方法

前セクションの設定はそのままで、さら に以下の設定をしてください。

SSH Sentinel 側の設定

「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。

規則のフロパティ ?×
全般 詳細
セキュリティの関連付けの有効期間
IPSec セキュリティと IKE セキュリティの関連付 けの有効期間を設定します。
監査オブション
○ この規則を監査する(A)
詳細オブション
 IP 圧縮を適用する① PMTU (Path Maximum Transfer Unit) を発見する(M) NAT 装置を経由する NAT 装置を経由する NAT-T (Network: Address Translation Traversal) ボート(:適用する UDP カブセル(上: 2746 起動時に間K (S) 分割トンネリングを拒否する
OK キャンセル

この設定では、VPN クライアント側で設定 した仮想 IP アドレスを使って VPN 接続し ます。

すべてセンター経由で IPsec 接続を行う設定

<u>ネットワーク構成</u> SSH Sentinel クライアントは、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、SSH SentinelとXR #1間、XR #2とXR #1間で生成します。

<u>SSH Sentinel 側の設定</u>

P.3からの設定通りに設定します。 ただし以下の項目については

・「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)

のように設定をしてください。

センター: 192.168.100.0/24

XR #1

固定 IP

<u>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。

¹192.168.0.0/24 ¹

Internet		a.(SSH Sentinel 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 「0.0.0.0/0」 相手側のLAN側のネットワークアドレス 「SSH Sentinelの仮想 IPアドレス /32」
IP	動的 IP	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
	XR #2	
		相手側のLAN側のネットワークアドレス

石子回のこれ原のイク

SSH Sentinel

動的 IP

拠点:192.168.0.0/24

XR #2(拠点側)の設定

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、SSH Sentinel 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 ルータを経由して IPsec 接続をする場合の設定

<u>ネットワーク構成</u>

XR #2をセンター、SSH Sentinelを拠点とします。 SSH Sentinel とLAN Bをセキュアに通信可能とし ます。ただし、XR #1はNATルータとして機能する ものとします。

この構成では、IPsec設定につきましては当ガイド P.3からの設定通りに設定します。

さらに XR #1(NAT ルータ)において、以下のように バーチャルサーバ設定とパケットフィルタ設定を してください。

<u>バーチャルサーバ設定</u>

以下の2つの設定を加えます。

	LAN B	以下の2つの設定を加えます。
XR #2		a. 「サーバのアドレス」SSH SentinelのIPアドレス 「公開するグローバルアドレス」空欄 「プロトコル」udp 「ポート」500 「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
Ineternet	IPsec	b. 「サーバのアドレス」SSH SentinelのIPアドレス 「公開するグローバルアドレス」空欄 「プロトコル」esp 「ポート」空欄 「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

XR #1 NAT

SSH Sentinel

<u>パケットフィルタ設定</u>

転送フィルタで以下の2つの設定を加えます。

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」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
- 「あて先ポート」空欄

これらの設定を加えることで、SSH Sentinel は NAT ルータである XR #1 を経由して IPsec 接続が可 能となります。

FutureNet XRシリーズ以外のNATルータを経由する場合は、これに準じた設定をしてください。

SSH Sentinelを使用したいクライアントの台数 分だけのグローバルアドレスが必要となります。

NAT トラバーサルを用いた IPsec 接続 1

<u>ネットワーク構成</u> VD #2 ちちンター SSH Senting」 ち枷 ちとします	<u>接続条件</u>
XK #2をビンター、SSF Sentinelを拠点とします。 SSH Sentinel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	・PSK(共通鍵)方式で認証します。
するものとします。	・agressive モードで接続します。
	・XR 側は PPPoE 接続 / 固定 IP とします。
LAN A	・SSH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。
XR 100.100.100.1	・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 : 192.168.1.0/24
	・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。
Ineternet IPsec	・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」 拠占の ID : ssb
ルータ NAT	

LAN B

SSH Sentinel
(ID = ssh)

<u>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	%ррр0	
インターフェー スのID		(例:@xr.centurysy

[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ipsec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	%v4:192.168.1.0/24
鐘の表示	
本装置のRSA纏 (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 Г インターフェー スのID @ssh (例:@xr.centurysys) aggressive モード ▼ モードの設定 1∰⊟ group2-3des-sha1 💌 2番目 使用しない transformの設定 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 ipseckey . ● PSKを使用する RSAを使用する (X509を使用する場合は RSAに設定してください) Ŧ X509の設定 -接続先の証明書の設定 (X509を使用しない場合は 必要ありません) 7

[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-Dermand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 (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	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)

「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「%v4:192.168.1.0/24」(3)
- ・本装置の RSA 鍵 「空欄」

(3)VPN Client が属しているものと同じネットワーク アドレスを指定します。

また VPN Client が仮想 IP アドレスを使っている場合 は、その仮想 IP アドレス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
 - r 192.168.10.0/24 ر
- ・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」

<u>VPN Clinentの設定</u>

[規則のプロパティ < 全般 > 設定]



- ・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」

[リモートネットワークの設定]

名前	IP アドレス	サブネット マ	スク	
any	0.0.0.0	0.0.0.0		
test	192.168.10.0	255.255.255	0.0	
		新規(<u>N</u>)		判除(<u>R</u>)
	test	新規(<u>N</u>)	Ĕ	削除(<u>R</u>)
、ットワーク名:	test	新規(11)	Ĕ	削除(<u>R</u>)
、ットワーク名: • アドレス:	test 192	新規(<u>N</u>) 168 10	i	削除(<u>R)</u>

・「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」

[パラメータの設定]

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」
- ・PFS グループ 「MODP 1024 (group2)」

[規則のプロパティ < 詳細 > 設定]



詳細オプション項目にある

NAT 装置を経由する

• NAT-T

の2カ所にチェックをしてください。 それ以外については、任意で設定してください。

<u>VPN Clinent の設定で仮想 IP アドレスを使う場合</u>

VPN Clientの設定で、以下のように仮想 IP アドレスを設定したとします。

- ・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」



この場合は、XRの本装置の設定にある「Virtual Private 設定」を以下のように設定してください。

%v4:192.168.20.0/24 (仮想 IP アドレスと同じ ネットワークアドレスを指定します)

Virtual Private設定

%v4:192.168.20.0/24

複数のVPN Clinent を接続する場合

複数の VPN Client から 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。

NAT トラパーサルを用いた IPsec 接続 2

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。	運用条件 ・R1、R2、R3 ともに PPPoE 接続をします。
<u>ネットワーク構成</u>	・R1 は固定 IP アドレス、R2 とR3 は動的 IP アドレ スとします。
LAN A	・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 I Psec 接 続をおこないます。
R1	・R1 とR3 は aggressive モードで IPsec 接続をお こないます。
10.10.10.1(11102)	・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
Internet	・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。
PPPoE PPPoE 動的 IP 動的 IP R3 R2 NAT	・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
PC	・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。

VPN Client

<u>R1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	10.10.10.1	
上位ルータのIPアドレス	ЖрррО	
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	
Virtual Private設定	%v4:192.168.50.0/24	
NAT-Tの設定をおこないます。		

MTU値については適宜設定してください。

[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 ()#]:@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	
 PSKを使用する RSAを使用する (X509を使用する場合は RSAに設定してください) 	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	192.168.10.0/24 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.0.0/24 ()):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)

[IPsecポリシーの設定2]

○ 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	(1) The second s
本装置側のLAN側のネットワークアドレス	192.168.10.0/24 (M:192.168.0.0/24)
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
SAD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
上位ルータのIPアドレス	
インターフェー スのID	@client (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	
 PSKを使用する RSAを使用する (X509を使用する場合は RSAに設定してくだれい) 	test2

<u>R3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	%ррр0	
上位ルータのIPアドレス		
インターフェー スのID	@branch	(例:@>r.centurysys)

[本装置の設定]

とくに設定するところはありません。 MTU値については適宜設定してください。

[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:@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	
 PSKを使用する RSAを使用する (X509を使用する場合は RSAに設定してください) 	test 💌

[IPsecポリシーの設定1]

「使用する」 使用しない い Resp	onderとし(使用する 🤍 Un-Demand C1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 (例: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 (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)

<u>VPN Clinentの設定</u>

[規則のプロパティ < 全般 > 設定]

則のプロ	パティ		?)
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:	10 10	10 1 <u>I</u> P
Sumi	リモート ネットワーク:	192.168.10.0/24	▼
IPSec /	IKE 候補		
**	認証鍵	🥯 test	-
U	候補テンプレート:	normal	•
			設定
	見IP アドレスを取得する 仮想 IP アドレスは、内部 です。	ネットワークのアドレス	
	観烈証 VPN ゲートウェイでは、IKI または CHAP 認証が必要 す。	E XAuth、RADIUS、 見となる場合がありま	設定
			変更(<u>C</u>)
		C 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					? ×
した 仮想 IP アドレス 行います。	なに割り当て	こるプロト:	コルを選択	てするか、手	動で設定を
プロトコル 〇 IPSec 経由の DHCF	o (Dynami	c Host C	>onfigura	tion Proto	col)
C L2TP (Layer Two Tr	unneling F	Protocol)			
 ○ IKE 設定モード ○ 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	サーバを指	定する:			
DNS サーバ					
WINS サーバ					
		[ок	+	ャンセル

[規則のプロパティ < 詳細 > 設定]



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]

事前共有鍵	<u>? ×</u>
プロパティ ID	
●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●	、当事者のみが知る共有シークレットに基づい
事前共有鍵情報 -	
名前:	test
鍵 ID:	test
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	****
フィンガーブリント	
109f 4b3c	
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 利しないでください。
	OK キャンセル

[事前共有鍵 <ID> 画面]

事前共有鍵	<u>?×</u>
ว่อパティ ID	
通常は、IDを指 モードでは、両方	定する必要はありません。ただし、IKE アグレッシブ の ID を指定する必要があります。
プライマリ ID:	■ ホストドメイン名
ホスト ドメイン名:	client
プライマリ ID:	🕵 ID なし 📃
警告 建択した ID は	. IKE メイン モードでは使用できません。
	OK キャンセル

SSH Sentinel のログについて

SSH Sentinel 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 = hmacsha1, 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) done.

0.0.0.0:500 (Initiator) <-> 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, hmac-sha1-96, key len = 0, key rounds = 0

Phase-2 [initiator] done bundle 2 with 2 SA's
by rule 21:`ipsec ipv4(any:0,[0..3]
=192.168.100.1)<->ipv4_subnet(any:0,[0..7]
=192.168.1.0/24)(gw:ipv4(any:0,[0..3]
=xxx.xxx.xxx.xxx))'

SA ESP[be022262] alg [3des-cbc/24]+hmac[hmacsha1-96] bundle [2,0] pri 0 opts src=ipv4 (any:0,[0..3]=192.168.100.1) dst=ipv4_subnet (any:0,[0..7]=192.168.1.0/24)

SA ESP[491547c3] alg [3des-cbc/24]+hmac[hmacsha1-96] bundle [2,0] pri 0 opts src=ipv4_subnet(any:0,[0..7]=192.168.1.0/24) dst=ipv4(any:0,[0..3]=192.168.100.1)

SSH Sentinelのログについて

[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.) 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) 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。

SSH Sentinelのログについて

[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 = hmacsha1, 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) done.

0.0.0.0:500 (Initiator) <-> xxx.xxx.xxx.xxx: 500 { 0202f991 16000008 - 0e6a4ab9 116f8cc3 [0] / 0xb00c7f69 } 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)

2004年5月版 発行 センチュリー・システムズ株式会社 2001-2004 CENTURYSYSTEMS,INC. All rights reserved.