# <u>インターネット VPN 対応ルータ</u>

FutureNet XR シリーズ

インターネット VPN 設定例集

IPsec 編

Ver 1.3.0

センチュリー・システムズ株式会社

# 目次

	······ ··· ··· ··· ··· ··· ··· ··· ···
改版履歴	6
1. 様々な接続形態での IPsec 接続例	7
1-1. 構成例	7
1-2. 要件	
1-3. 設定例	
センタールータ (XR_A)	
拠点1ルータ (XR_B)	
拠点 $2 \mu - \varphi$ (XR_C)	
拠点3PC (PC)	30
2. IPsec を利用したセンター経由インターネット接続例	40
2-1. 構成例	40
2-2. 要件	41
2-3. 設定例	
センタールータ $(XR_A)$	
拠点1ルータ (XR_B)	51
拠点 $2 \mu - \varphi (XR_C)$	55
3. 複数セグメントでの IPsec 設定例	59
3-1. 構成例	59
3-2. 要件	60
3-3. 設定例	
(h) $(h)$ $(h)$ $(h)$	
$\mathcal{V} \mathcal{V} \mathcal{Y} \stackrel{\frown}{\longrightarrow} \mathcal{V} \stackrel{\frown}{\longrightarrow} (XR_A)$	<i>c</i> 0
センタールータ $(XR_A)$ センタールータ 2 $(XR_A2)$	
センタールータ (XR_A) センタールータ2 (XR_A2) 拠点ルータ (XR_B)	
センタールータ $(XR_A)$ センタールータ 2 $(XR_A2)$ 拠点ルータ $(XR_B)$ 4. IPsec での NAT 利用例	
センタールータ (XR_A) センタールータ 2 (XR_A2) 拠点ルータ (XR_B) 4. IPsec での NAT 利用例 4-1. 構成例	
センタールータ (XR_A) センタールータ 2 (XR_A2) 拠点ルータ (XR_B) 4. IPsec での NAT 利用例 4-1. 構成例 4-2. 要件	
<ul> <li>センタールータ (XR_A)</li> <li>センタールータ 2 (XR_A2)</li> <li>拠点ルータ (XR_B)</li> </ul> 4. IPsec での NAT 利用例 4-1. 構成例 4-2. 要件 4-3. 設定例	
<ul> <li>センタールータ (XR_A)</li> <li>センタールータ 2 (XR_A2)</li> <li>拠点ルータ (XR_B)</li> </ul> 4. IPsec での NAT 利用例 4-1. 構成例 4-2. 要件 4-3. 設定例 センタールータ (XR_A)	
センタールータ $(XR_A)$ センタールータ $2$ $(XR_A2)$ 拠点ルータ $(XR_B)$ 4. IPsec での NAT 利用例 4-1. 構成例 4-2. 要件 4-3. 設定例 センタールータ $(XR_A)$ 拠点ルータ $(XR_B)$	
センタールータ $(XR_A)$ センタールータ $2$ $(XR_A2)$ 拠点ルータ $(XR_B)$ 4. IPsec での NAT 利用例 4-1. 構成例 4-2. 要件 4-3. 設定例 センタールータ $(XR_A)$ 拠点ルータ $(XR_B)$ 5. GRE over IPsec 設定例	
センタールータ $(XR_A)$ センタールータ $2(XR_A2)$ 拠点ルータ $(XR_B)$ 4. IPsec での NAT 利用例 4-1. 構成例 4-2. 要件 4-3. 設定例 $t = 2 (XR_A)$ $j = 2 (XR_A)$ $j = 2 (XR_B)$ 5. GRE over IPsec 設定例 5-1. 構成例	
センタールータ $(XR_A)$ $t \ge y - n - y 2 (XR_A 2)$ 拠点ルータ $(XR_B)$ 4. IPsec での NAT 利用例 4-1. 構成例 4-2. 要件 4-3. 設定例 $t \ge y - n - y (XR_A)$ 拠点 $n - y (XR_B)$ 5. GRE over IPsec 設定例 5-1. 構成例 5-2. 要件	

センタールーダ ( $XR_A$ )       94         炭点ルーダ ( $XR_B$ )       99         6. <b>IPsec NAT Traversal 設定例 1</b> 104         6-1. 構成例       104         6-2. 要件       105         6-3. 設定例       109 $z > g - h - g$ ( $XR_A$ )       109 $das 1 h - g$ ( $XR_B$ )       116         漫点 $2 PC$ ( $PC$ )       116         NAT $\lambda - g$ 128         7. <b>IPsec NAP Traversal 設定例 2</b> 129         7-1. 構成例       129         7-2. 要件       130         7-3. 設定例       134 $z > J - h - g$ ( $XR_A$ )       134 $z > J - h - g$ ( $XR_A$ )       134 $das 2 - g - h - g$ ( $XR_A$ )       134 $das 2 - g (XR_B)$ 144         NAT $h - g$ 132         8. <b>IPsec backupSA 機能 (IPsec</b> 冗長化) 利用例       163         8-1. 構成例       163         8-2. 要件       164         8-3. 設定例       159 $z > g - h - g (XR_A)       159         z > g - h - g (XR_A)       159         z > g - h - g (XR_A)       159         z > g - h - g (XR_A)       159         z > g - h - g (XR_A)       169         9. ISDN を利用 した回線パック ア$	5-3. 設定例	
超点ルータ (XR_B)       99         6. IPsec NATTraversal 設定例1       104         6-1. 構成例       104         6-2. 要件       105         6-3. 設定例       109 $t \sim J = -h - 9$ (XR_A)       109 $d \sim J = -h - 9$ (XR_A)       109 $d \sim J = -h - 9$ (XR_B)       116         超点 2 PC (PC)       119         NAT $h - 9$ (XR_B)       128         7. IPsec NATTraversal 設定例 2       129         7.1. 構成例       129         7.2. 要件       130         7.3. 設定例       134 $t \sim J = -h - 9$ (XR_A)       134 $d \sim J = -h - 9$ (XR_A)       134 $d \sim J = -h - 9$ (XR_A)       134 $d \sim J = -h - 9$ (XR_A)       134 $d \sim J = -h - 9$ (XR_A)       134 $d \sim J = -h - 9$ (XR_A)       134 $d \sim J = -h - 9$ (XR_A)       135         8. IPsec backupSA 機能 (Psec $T E (L)$ 利用例       153         8.1. 構成例       153         8.2. 要th       154         8.3. 設定例       159 $t \sim J = -h - 9 1$ (XR_A)       159 $t \sim J = -h - 9 1$ (XR_A)       169 $d \sim J = -h - 9 1$ (XR_A)       164	センタールータ (XR_A)	
<ul> <li>6. IPsec NAT'Traversal 設定例 1</li></ul>	拠点ルータ (XR_B)	
6・1.構成例       104         6・2. 要件       105         6・3. 設定例       109 $t \ge y = -t = g'$ (XR_A)       109 $d \ge x \ge y = -t = g'$ (XR_B)       116         選点 $1 t = g'$ (XR_B)       116         選点 $2 PC$ (PC)       119         NAT $t = g'$ 128         7. Psec NAT Traversal 設定例 2       129         7.1. 構成例       129         7.2. 要件       130         7.3. 設定例       134 $t \ge y = -h = g'$ (XR_A)       134 $d \ge x = -g'$ (XR_B)       141         PC (懲点)       144         NAT $h = g'$ (XR_B)       144         PC (懲点)       144         NAT $h = g'$ (XR_B)       144         PC (懲点)       144         NAT $h = g'$ (XR_B)       144         PC (懲点)       144         NAT $h = g'$ (XR_B)       145         8. Psee backupSA 機能 (Psec 冗長化) 利用例       153         8.1. 構成例       153         8.2. 要th       154         8.3. 設定例       159 $t \ge y = -t = g'$ (XR_A)       169 $t \ge y = -t = g'$ (XR_A)       169         9. ISDN を利用した回線バックアップダその1 (メーク       175	6. IPsec NAT Traversal 設定例 1	104
6・2. 要件       105         6・3. 設定例       109 $t \sim y = \lambda - \beta$ (XR_A)       109 $dx \leq 1 \lambda - \beta$ (XR_B)       116         遡点 $2 PC$ (PC)       119         NAT $\lambda - \beta$ 128         7. IPsec NAT'Traversal 設定例 2       129         7.1. 構成例       129         7.2. 要件       130         7.3. 設定例       134 $t \sim y = -\lambda \beta$ (XR_A)       134 $dx \leq \lambda \beta$ (XR_A)       134 $dx \leq \lambda \beta$ (XR_A)       134 $dx = \lambda \beta$ (XR_A)       135         8. IPsec backupSA 機能 (IPsec 冗長化)       144 $NAT \beta$ 135         8. IPsec backupSA 機能 (IPsec 冗長化)       153         8. $2$ 要件       164         8. $3$ 設定例       153 $dx = \lambda \beta$ (XR_A)       159 $t \sim y \beta$ (XR_A)       164	6-1. 構成例	104
6·3. 設定例       109 $t \ge y = y - y = (XR_A)$ 109         遡点 1 $u = g$ (XR_B)       116         遡点 2 PC (PC)       119         NAT $u = g$ 128         7. IPsec NAP Traversal 設定例 2       129         7.1. 構成例       129         7.2. 要件       130         7.3. 設定例       134 $t \ge y = u - g (XR_A)$ 134 $t \ge y = u - g (XR_A)$ 134 $t \ge y = u - g (XR_A)$ 134 $t \ge y = u - g (XR_A)$ 134 $t \ge y = u - g (XR_A)$ 134 $t \ge y = u - g (XR_A)$ 134 $t \ge y = u - g (XR_B)$ 141         PC (遡点)       152         8. IPsec backupSA 機能 (IPsec 冗長化) 利用例       153         8.2. 要件       153         8.3. 設定例       159 $t \ge g - u - g 1$ ( $XR_A$ )       159 $t \ge y - u - g 2$ ( $XR_A$ )       169 $t \ge y - u - g 2$ ( $XR_A$ )       169 $t \ge y - u - g 2$ ( $XR_A$ )       169         9. ISDN を利用した回線 パックフップ例その1 ( $y 4$ ン回線 IPsec)       175         9.1. 構成例       175         9.2. 要性       160 $t \ge y - u - g (XR_A)$ 180 <td>6-2. 要件</td> <td> 105</td>	6-2. 要件	105
センタールータ (XR_A)       109         趣点 1 ルータ (XR_B)       116         拠点 2 PC (PC)       119         NATルータ       128         7. IPsec NAT Traversal 設定例 2       129         7.1. 構成例       129         7.2. 要件       130         7.3. 設定例       134 $t \ge y - \mu - g$ (XR_A)       134 $t \ge y - \mu - g$ (XR_A)       134 $t \ge y - \mu - g$ (XR_A)       134 $t \ge y - \mu - g$ (XR_A)       134 $t \ge y - \mu - g$ (XR_A)       134 $t \ge y - \mu - g$ (XR_A)       134 $t \ge y - \mu - g$ (XR_A)       134 $t \ge y - \mu - g$ (XR_A)       134 $h = 0$ (Mg)       141 $NAT \mu - g$ 152         8. IPsec backupSA 機能 (IPsec 冗長化) 利用例       153         8-1. 構成例       153         8-2. 要件       154         8-3. 設定例       159 $t \ge y - \mu - g 2$ (XR_A)       169 $t \ge y - \mu - g 2$ (XR_A)       169 $t \ge y - \mu - g 2$ (XR_A)       169 $t \ge y - \mu - g 2$ (XR_A)       169 $g = 1$ 175         9-1. 構成例       175         9-2. 要件       169	6-3. 設定例	
總点 1 ハータ (XR_B)       116         總点 2 PC (PC)       119         NAT ハータ       128         7. IPsec NAT Traversal 設定例 2       129         7-1. 構成例       129         7-2. 要件       130         7-3. 設定例       134         センターハータ (XR_A)       134         地点ハータ (XR_B)       141         PC (拠点)       153         8. IPsec backupSA 機能 (IPsec 冗長化) 利用例       163         8-1. 構成例       153         8-2. 要件       154         8-3. 設定例       159 $t > y - n - y = (XR_A)$ 164 $wax - y = (XR_A)$ 165         9. ISDN を利用した回線パックアップ例その1 (メイン回線 IPsec)       175         9.2. 要件       176         9.3. 設定例       180 $t > y - n - y = (XR_A)$ 180 $v > y - n - y = (XR_A)$ 180 $v > y - n - y = (XR_A)$ 189         9. ISDN を利用した回線パックアップ例その1 (メイン回線 IPsec)       175         9.2. 要件       180         10. ISDN を利用した回線パックアップ例その2 (メイン回線 IPsec)       191         10-1. 構成例       191         10-2. 要件       192	センタールータ (XR_A)	109
趣点 2 PC (PC)       119         NAT ルータ       128         7. IPsec NAT Traversal 設定例 2       129         7-1. 構成例       129         7-2. 要件       130         7-3. 設定例       134         センタールータ (XR_A)       134         地点ルータ (XR_B)       141         PC (拠点)       153         8. IPsec backupSA 機能 (IPsec 冗長化) 利用例       153         8.1. 構成例       153         8.2. 要件       154         8.3. 設定例       159         センタールータ1 (XR_A)       169         センタールータ (XR_A)       169         センタールータ (XR_B)       169         9. ISDN を利用した回線パックアップ例その1 (メイン回線 IPsec)       175         9.2. 要件       176         9.3. 設定例       180         センタールータ (XR_A)       180         センタールータ (XR_B)       181         10. ISDN を利用した回線パックアップ例その2 (メイン回線 IPsec)       191         10-1. 構成例       191         10-2. 要件       192	拠点1ルータ (XR_B)	116
NAT ルータ       128         7. IPsec NAT Traversal 設定例 2       129         7.1. 構成例       129         7.2. 要件       130         7.3. 設定例       134         センタールータ (XR_A)       134         増点ルータ (XR_B)       141         PC (拠点)       144         NAT ルータ       152         8. IPsec backupSA 機能 (IPsec 冗長化) 利用例       153         8-1. 構成例       153         8-2. 要件       154         8-3. 設定例       159         センタールータ1 (XR_A)       159         センタールータ2 (XR_A2)       164         拠点ルータ (XR_B)       169         9. ISDN を利用した回線パックアップ例その1 (メイン回線 IPsec)       175         9-2. 要件       176         9-3. 設定例       180         ゼンタールータ (XR_A)       180         ゼンタールータ (XR_A)       180         ゼンタールータ (XR_A)       180         ガンタールータ (XR_A)       180         ウンタールータ (XR_A)       180         ガンタールータ (XR_A)       180         ガンタールータ (XR_B)       180         10. ISDN を利用した回線パックアップ例その2 (メイン回線 IPsec)       191         10-1. 構成例       191         10-2. 要件       192	拠点2PC (PC)	
7. IPsec NAT Traversal 設定例 2       129         7-1. 構成例       129         7-2. 要件       130         7-3. 設定例       134         センタールータ (XR_A)       134         地点ルータ (XR_B)       141         PC (逆点)       144         NAT ルータ       152         8. IPsec backupSA 機能 (IPsec 冗長化) 利用例       153         8-1. 構成例       153         8-2. 要件       154         8-3. 設定例       159         センタールータ1 (XR_A)       159         センタールータ2 (XR_A2)       164         拠点ルータ (XR_B)       169         9. ISDN を利用した回線パックアップ例その1 (メイン回線 IPsec)       175         9-2. 要件       176         9-3. 設定例       180         ゼンタールータ (XR_A)       180         ゼンタールータ (XR_A)       180         センタールータ (XR_B)       180         10. ISDN を利用した回線パックアップ例その2 (メイン回線 IPsec)       191         10-1. 構成例       191         10-2. 要件       192	NATルーダ	128
7-1.構成例       129         7-2.要件       130         7-3. 設定例       134         センタールータ (XR_A)       134         地点ルータ (XR_B)       141         PC (拠点)       144         NAT ルータ       152         8. IPsec backupSA 機能 (IPsec 冗長化) 利用例       153         8-1.構成例       153         8-2.要件       154         8-3. 設定例       159         センタールータ1 (XR_A)       159         センタールータ2 (XR_A2)       164         拠点ルータ (XR_B)       169         9. ISDN を利用した回線パックアップ例その1 (メイン回線 IPsec)       175         9-1.構成例       176         9-3. 設定例       180         センタールータ (XR_A)       180         センタールータ (XR_B)       180         164       180         ウインータ (XR_B)       180         165       180         センタールータ (XR_A)       180         センタールータ (XR_B)       180         175       180         180       180         センタールータ (XR_B)       180         180       180         センタールータ (XR_B)       180         180       180         191       10-1.         10-1	7. IPsec NAT Traversal 設定例 2	129
7-2. 要件       130         7-3. 設定例       134         センタールータ (XR_A)       134         燃点ルータ (XR_B)       141         PC (拠点)       144         NAT ルータ       152         8. IPsec backupSA 機能 (IPsec 冗長化) 利用例       153         8-1. 構成例       153         8-2. 要件       154         8-3. 設定例       159         センタールータ1 (XR_A)       159         センタールータ2 (XR_A2)       164         拠点ルータ (XR_B)       169         9. ISDN を利用した回線パックアップ例その1 (メイン回線 IPsec)       175         9-2. 要件       176         9-3. 設定例       180         センタールータ (XR_A)       180         燃点ルータ (XR_B)       180         10. ISDN を利用した回線パックアップ例その2 (メイン回線 IPsec)       191         10-1. 構成例       191         10-2. 要件       192	7-1. 構成例	
7-3. 設定例       134         センタールータ (XR_A)       134         拠点ルータ (XR_B)       141         PC (拠点)       144         NAT ルータ       152         8. IPsec backupSA 機能 (IPsec 冗長化) 利用例       153         8-1. 構成例       153         8-2. 要件       154         8-3. 設定例       159         センタールータ1 (XR_A)       159         センタールータ2 (XR_A2)       164         拠点ルータ (XR_B)       169         9. ISDN を利用した回線パックアップ例その1 (メイン回線 IPsec)       175         9-2. 要件       176         9-3. 設定例       180         センタールータ (XR_B)       180         センタールータ (XR_B)       180         175       9-2. 要件         9-1. 構成例       180         センタールータ (XR_B)       180         176       9-3. 設定例       180         センタールータ (XR_B)       185         10. ISDN を利用した回線パックアップ例その2 (メイン回線 IPsec)       191         10-1. 構成例       191         10-2. 要件       192	7-2. 要件	
センタールータ (XR_A)       134         拠点ルータ (XR_B)       141         PC (拠点)       144         NAT ルータ       152         8. IPsec backupSA 機能 (IPsec 冗長化) 利用例       153         8-1. 構成例       153         8-2. 要件       154         8-3. 設定例       159         センタールータ1 (XR_A)       159         センタールータ2 (XR_A)       164         拠点ルータ (XR_B)       169         9. ISDN を利用した回線バックアップ例その1 (メイン回線 IPsec)       175         9-2. 要件       176         9-3. 設定例       180         センタールータ (XR_A)       180         センタールータ (XR_A)       180         175       9-2. 要件       176         9-3. 設定例       180         10. ISDN を利用した回線バックアップ例その2 (メイン回線 IPsec)       191         10-1. 構成例       191         10-2. 要件       192	7-3. 設定例	
<ul> <li>拠点ルータ (XR_B)</li></ul>	センタールータ (XR_A)	134
PC (拠点)       144         NAT ルータ       152         8. IPsec backupSA 機能 (IPsec 冗長化) 利用例       153         8-1. 構成例       153         8-2. 要件       154         8-3. 設定例       159         センタールータ1 (XR_A)       159         センタールータ2 (XR_A2)       164         拠点ルータ (XR_B)       169         9. ISDN を利用した回線バックアップ例その1 (メイン回線 IPsec)       175         9-1. 構成例       175         9-2. 要件       176         9-3. 設定例       180         センタールータ (XR_A)       180         センタールータ (XR_B)       180         10. ISDN を利用した回線パックアップ例その2 (メイン回線 IPsec)       191         10-1. 構成例       191         10-2. 要件       192	拠点ルータ (XR_B)	141
NAT ルータ	PC (拠点)	
<ul> <li>8. IPsec backupSA 機能 (IPsec 冗長化) 利用例</li></ul>	$NAT \wedge - \beta$	
8-1.構成例       153         8-2.要件       154         8-3.設定例       159         センタールータ1 (XR_A)       159         センタールータ2 (XR_A2)       164         拠点ルータ (XR_B)       169         9. ISDN を利用した回線バックアップ例その1 (メイン回線 IPsec)       175         9-1.構成例       175         9-2.要件       176         9-3.設定例       180         センタールータ (XR_A)       180         拠点ルータ (XR_B)       185         10. ISDN を利用した回線バックアップ例その2 (メイン回線 IPsec)       191         10-1.構成例       191         10-2.要件       192	8. IPsec backupSA 機能(IPsec 冗長化)利用例	153
<ul> <li>8-2. 要件</li></ul>	8-1. 構成例	153
<ul> <li>8-3. 設定例</li></ul>	8-2. 要件	
<ul> <li>センタールータ1 (XR_A)</li></ul>	8-3. 設定例	
センタールータ2 (XR_A2)       164         拠点ルータ (XR_B)       169         9. ISDN を利用した回線バックアップ例その1 (メイン回線 IPsec)       175         9-1. 構成例       175         9-2. 要件       176         9-3. 設定例       180         センタールータ (XR_A)       180         拠点ルータ (XR_B)       185         10. ISDN を利用した回線バックアップ例その2 (メイン回線 IPsec)       191         10-1. 構成例       191         10-2. 要件       192	センタールータ1 (XR_A)	159
<ul> <li>拠点ルータ (XR_B)</li></ul>	センタールータ2(XR_A2)	
9. ISDN を利用した回線バックアップ例その1(メイン回線 IPsec)       175         9-1. 構成例       175         9-2. 要件       176         9-3. 設定例       180         センタールータ(XR_A)       180         拠点ルータ(XR_B)       185         10. ISDN を利用した回線バックアップ例その2(メイン回線 IPsec)       191         10-1. 構成例       191         10-2. 要件       192	拠点ルータ (XR_B)	
9-1. 構成例       175         9-2. 要件       176         9-3. 設定例       180         センタールータ (XR_A)       180         拠点ルータ (XR_B)       185         10. ISDN を利用した回線バックアップ例その2 (メイン回線 IPsec)       191         10-1. 構成例       191         10-2. 要件       192	9. ISDN を利用した回線バックアップ例その1(メイン回線 IPsec)	
9-2. 要件       176         9-3. 設定例       180         センタールータ (XR_A)       180         拠点ルータ (XR_B)       185         10. ISDN を利用した回線バックアップ例その2 (メイン回線 IPsec)       191         10-1. 構成例       191         10-2. 要件       192	9-1. 構成例	
9-3. 設定例       180         センタールータ (XR_A)       180         拠点ルータ (XR_B)       185         10. ISDN を利用した回線バックアップ例その2 (メイン回線 IPsec)       191         10-1. 構成例       191         10-2. 要件       192	9-2. 要件	
<ul> <li>センタールータ (XR_A)</li></ul>	9-3. 設定例	
<i>拠点ルータ(XR_B)</i>	センタールータ (XR_A)	180
10. ISDN を利用した回線バックアップ例その2(メイン回線 IPsec)       191         10-1. 構成例       191         10-2. 要件       192	拠点ルータ (XR_B)	
10-1.       構成例	10. ISDN を利用した回線バックアップ例その2(メイン回線 IPsec)	191
10-2. 要件	10-1. 構成例	191
	10-2. 要件	

10-3.	設定例	
センタ	$\gamma - \mu - \not > 1  (XR_A)  \dots$	
センタ	$T - \mathcal{W} - \mathcal{F} 2  (XR_A2)$	
拠点儿	~—\$\angle (XR_B)	
11. ISD	N を利用した回線バックアップ例その3(メイン回線 IPsec)	
11-1.	構成例	
11-2.	要件	
11-3.	設定例	
センタ	マールータ1 (XR_A)	
センタ	$\gamma - \mu - \not{P} 2  (XR_A2)  \dots$	
拠点川	ν—\$\\$\\$\\$ (XR_B)	

# はじめに

本書はXRシリーズを利用した設定例集になります。 本書を利用する際は、各製品のユーザーズガイドも合わせてご利用下さい。

# 注意事項

- 本書の内容の一部または全部を無断で転載することを禁止しています。
- 本書の内容については、将来予告なしに変更することがあります。
- 本書の内容については万全を期しておりますが、ご不審な点や誤り、記載漏れ等お気づきの点がありましたらお手数ですが、ご一報下さいますようお願い致します。
- ■本書はXR-510/C, XR-540/C Ver3.2.0をベースに作成しております。IPsec および IPsec KeepAlive において、ご使用されている製品およびファームウェアのバージョンによっては、一部機能および 設定画面が異なっている場合もありますので、その場合は各製品のユーザーズガイドを参考に、適 宜読みかえてご参照および設定を行って下さい。
- 本書を利用し運用した結果発生した問題に関しましては、責任を負いかねますのでご了承下さい。

# 改版履歴

Version	更新内容
1. 1. 0	初版
1. 2. 0	NAT-Traversal 設定例2追加
	設定例構成図変更
1.2.0	複数セグメントでの IPsec 設定例追加
1. 3. 0	IPsec での NAT 利用例追加

# 1. 様々な接続形態での IPsec 接続例

この例は、PPPoE や DHCP クライアントでの接続で IPsec によるインターネット VPN を実現する設定例で す。また PC にインストールして使用する VPN クライアント「FutureNet VPN Client/Net-G」を利用する ことにより、外出先などのリモートからも IPsec によるインターネット VPN が利用可能です。この例で は、PPP 回線を利用した VPN クライアントによるリモートアクセスを実現しています。

### 1-1. 構成例



## 1-2. 要件

- ▶ インタフェースおよび PPPoE
  - XR\_A(センター), XR\_B(拠点 1)はインターネットに PPPoE で接続します。
  - XR\_C(拠点 2)はインターネットに Ether (DHCP クライアント)で接続します。
  - PC(拠点 3)はインターネットに PPP で接続します。
  - PPPoE 接続は、自動再接続するように設定しています。
  - WAN 側インタフェースの IP マスカレード, ステートフルパケットインスペクション は「有効」にしています。

主なインタフェースおよび PPPoE のパラメータ

	XR_A(センター)	XR_B(拠点1)	XR_C(拠点 2)	PC(拠点3)
LAN 側インタフェース	Ether0	Ether0	Ether0	_
LAN 側 IP アドレス	192. 168. 10. 1	192. 168. 20. 1	192.168.30.1	
WAN 側インタフェース	Ether1[ppp0]	Ether1[ppp0]	Ether1	-
WAN 側 IP アドレス	10. 10. 10. 1	10. 10. 20. 1	動的 IP	動的 IP
PPPoE ユーザ名	test1@centurysys	test2@centurysys	-	test3
PPPoE パスワード	test1pass	test2pass	-	test3
接続回線	PPPoE 接続	PPPoE 接続	Ether 接続	PPP 接続

▶ IPsec

- 鍵交換モードは XR\_A <-> XR\_B はメインモード, XR\_A <-> XR\_C, XR\_A <-> PC はア グレッシブモードを使用しています。
- XR\_A(センター)は 192.168.10.0/24 <-> 192.168.20.0/24, 192.168.30.0/24, 192.168.40.1/32の時に IPsec を適用します。
- XR\_B(拠点 1)は 192.168.20.0/24 <-> 192.168.10.0/24 の時に IPsec を適用します。
- XR\_C(拠点 2)は 192.168.30.0/24 <-> 192.168.10.0/24 の時に IPsec を適用します。
- PC(拠点 3)は192.168.40.1/32 <-> 192.168.10.0/24の時に IPsec を適用します。
- IPsec KeepAlive は拠点のみ(PC 拠点3は除く)に使用しています。

本装置側のパラメータ

	XR_A(センター)	XR_B(拠点1)	XR_C(拠点 2)
インタフェースの IP アドレス	10. 10. 10. 1	10. 10. 20. 1	%eth1
上位ルータの IP アドレス	%ppp0	%ppp0	
インタフェースの ID			@ipsec2

		XR_A(センター)	
対向拠点	XR_B(拠点1)	XR_C(拠点 2)	PC(拠点3)
IKE/ISAKMP ポリシー名	XR_B	XR_C	PC
リモート IP アドレス	10. 10. 20. 1	0. 0. 0. 0	0. 0. 0. 0
インタフェースの ID		@ipsec2	@vpnclient
モード	Main	Aggressive	Aggressive
暗号化アルゴリズム	AES-128	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1	SHA1
DH グループ	Group2	Group2	Group2
ライフタイム	3600(秒)	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey2	ipseckey3

IKE/ISAKMP ポリシーのパラメータ(1) 「XR\_A(センター)」

IPsec ポリシーのパラメータ(1) 「XR\_A(センター)」

		XR_A(センター)	
対向拠点	XR_B(拠点1)	XR_C(拠点 2)	PC(拠点3)
使用する IKE ポリシー名	XR_B(IKE1)	XR_C(IKE2)	PC(IKE3)
本装置の LAN 側のネットワーク	192.168.10.0/24	192.168.10.0/24	192. 168. 10. 0/24
アドレス			
相手側の LAN 側のネットワーク	192.168.20.0/24	192. 168. 30. 0/24	192. 168. 40. 1/32
アドレス			
暗号化アルゴリズム	AES-128	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1	SHA1
PFS (DH グループ)	使用する(Group2)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)	28800(秒)
DISTANCE	1	1	1

	XR_B(拠点1)	XR_C(拠点 2)
対向拠点	XR_A(センター)	XR_A(センター)
IKE/ISAKMP ポリシー名	XR_A	XR_A
リモート IP アドレス	10. 10. 10. 1	10. 10. 10. 1
モード	Main	Aggressive
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
DH グループ	Group2	Group2
ライフタイム	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey2

IKE/ISAKMP ポリシーのパラメータ(2) 「XR\_B(拠点 1), XR\_C(拠点 2)」

IPsec ポリシーのパラメータ(2) 「XR\_B(拠点 1), XR\_C(拠点 2)」

	XR_B(拠点1)	XR_C(拠点 2)
対向拠点	XR_A(センター)	XR_A(センター)
使用する IKE ポリシー名	XR_A(IKE1)	XR_A(IKE1)
本装置の LAN 側のネットワークアドレス	192.168.20.0/24	192.168.30.0/24
相手側の LAN 側のネットワークアドレス	192.168.10.0/24	192.168.10.0/24
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
PFS (DH グループ)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)
DISTANCE	1	1

IPsec Keepalive のパラメータ

	XR_A(センター)	XR_B(拠点1)	XR_C(拠点 2)
対向拠点	XR_B(拠点1)	XR_A(センター)	XR_A(センター)
Policy No.	1	1	1
source address	192. 168. 10. 1	192. 168. 20. 1	192. 168. 30. 1
destination address	192. 168. 20. 1	192. 168. 10. 1	192. 168. 10. 1
interval(sec)	30	45	45
watch count	3	3	3
timeout/delay(sec)	60	60	60
動作option	1	1	2
interface	ipsec0	ipsec0	ipsec6

#### 1-3. 設定例

#### センタールータ (XR\_A)

#### ポイント

拠点1~3と IPsec 接続するための設定を行います。

拠点 2,3 は動的 IP のため、アグレッシブモードを使用しています。

#### <<インタフェース設定>>

[Ethernet0の設定]

<ol> <li>固定アド</li> </ol>	レスで使用
ℙアドレス	192.168.10.1
ネットマスク	255.255.255.0
MTU	1500

Ethernet0 に関する設定をします。

※IPアドレスの設定を変更した場合、その設定した IPアドレスが即反映されます。

[Ethernet1の設定]

<ol> <li>固定アド</li> </ol>	レスで使用	
IP アドレス	0	
ネットマスク	255.255.25	5.0
MTU	1500	

Ethernet1 に関する設定をします。

PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

#### <<PPP/PPPoE 設定>>

[接続先設定1]

ユーザロ	test1@centurysys	]
パスワード	test1pass	

PPPoE 接続で使用するユーザ ID,パスワードを登録します。

[接続設定]

接続先の選択	●接號先1 ●接読先2 ●接號先3 ●接號先4 ●接読先5
接続ポート	O Ether0 • Ether1 • Ether2 • ERI(64K) • ERI MP(128K) • RS2320
接統形態	○ 手動接続 ○ 常時接続 ○ スケジューラ接続
RS232C/BRI接続タイプ	<ul> <li>● 通常</li> <li>○ On-Demand接続</li> </ul>
ドマスカレード	○無効 ● 有効
ステートフルパケット インスペウション	○無効 ○有効 □DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ● 有効

PPPoE 接続するインタフェース、および接続形態を選択します。 ※この例では、ルータ経由でのインターネットアクセスも可能になっています。



PPPoEの再接続性を高めるために、PPPoE 特殊オプションを設定しています。

#### <<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ррр0	パケオ受信時	許可 💌	udp 💌		500		500	
рррО	パケオ受信時	許可 💌	esp 💌					

IKE パケット, ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

# <<各種サービスの設定>>

#### <IPsec サーバ>

[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	%ррр0
インターフェー スのID	(例:@xr.centurysys)

XR\_A(センター)のWAN側インタフェースのIPアドレス,および上位ルータのIPアドレスを設定します。 PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。

[IKE/ISAKMPの設定1]

IKE/ISAKMP ポリシーのパラメータは以下のとおりです。

設定項目	パラメータ
IKE/ISAKMP ポリシー名	XR_B
リモート IP アドレス	10. 10. 20. 1
モード	Main
暗号化アルゴリズム	AES-128
認証アルゴリズム	SHA1
DHグループ	Group2
ライフタイム	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1

IKE/ISAKMPポリシー名	XR_B
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	10.10.20.1
上位ルータのIPアドレス	
インターフェー スのЮ	(例:@xr.centurysys)
モードの設定	main モード
	1番目 group2-aes128-sha1 💌
two of two OP	2番目 使用しない 🔽
(ransionno)ague	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 料 (1081~28800秒まで)

XR\_B(拠点1)に対する IKE/ISAKMP ポリシーを設定します。

鍵の設定	
<ul> <li>PSKを使用する</li> <li>RSAを使用する</li> <li>(509を使用する場合は</li> <li>RSAに設定してください)</li> </ul>	ipseckey1

事前共有鍵(PSK)として「ipseckey1」を設定しています。

[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-Dermandで使用する

XR\_B(拠点 1)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

IPsec ポリシーのパラメータは以下のとおりです。

設定項目	パラメータ
使用する IKE ポリシー名	XR_B(IKE1)
本装置の 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	192.168.20.0/24
暗号化アルゴリズム	AES-128
認証アルゴリズム	SHA1
PFS (DH グループ)	使用する(Group2)
ライフタイム	28800(秒)
DISTANCE	1

使用するIKEポリシー名の選択	XR_B (IKE1) 💌
本装置側のLAN側のネオワークアドレス	192.168.10.0/24 (第1:192.168.00/24)
相手側のLAN側のネットワークアドレス	192.168.20.0/24 (約:192.168.00/24)
FH2のTransFormの選択	aes128-sha1 💌
PFS	<ul> <li>● 使用する ○ 使用しない</li> </ul>
DH Groupの選択(PFS使用時に有効)	eroup2 💌
SAのライフタイム	28800 彩 (1081~86400秒まで)
DISTANCE	1 (1~255まで)

XR\_B(拠点1)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

### [IKE/ISAKMPの設定 2]

IKE/ISAKMP ポリシーのパラメータは以下のとおりです。

設定項目	パラメータ
IKE/ISAKMP ポリシー名	XR_C
リモート IP アドレス	0. 0. 0. 0
インタフェースの ID	@ipsec2
モード	Aggressive
暗号化アルゴリズム	AES-128
認証アルゴリズム	SHA1
DH グループ	Group2
ライフタイム	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey2

IKE/ISAKMPポリシー名	XR_C
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	@ipsec2 (例:@xr.centurysys)
モードの設定	aggressive モード 💌
	1番目 group2-aes128-sha1 🔽
	2番目 使用しない 🔽
TRADSTERTOLLISE &	
(Internet to Appendix	3番目 使用しない 🔽
CONSIGNIO/BEE	3番目 使用しない <ul> <li>◆</li> <li>4番目 使用しない </li> </ul>

XR\_C(拠点 2)に対する IKE/ISAKMP ポリシーの設定を行います。

縺の設定	
<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 RSAL設定してください)</li> </ul>	ipseckey2

事前共有鍵(PSK)として「ipseckey2」を設定します。

[IPsec ポリシーの設定 2]

🔿 使用する 🔿 使用しない 📀 Responderとして使用する 🔿 On-Dermandで使用する

XR\_C(拠点 2)の IP アドレスが不定のため、「Responder として使用する」を選択します。

IPsec ポリシーのパラメータは以下のとおりです。

設定項目	パラメータ
使用する IKE ポリシー名	XR_C(IKE2)
本装置の 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	192.168.30.0/24
暗号化アルゴリズム	AES-128
認証アルゴリズム	SHA1
PFS (DH グループ)	使用する(Group2)
ライフタイム	28800(秒)
DISTANCE	1

使用するIKEポリシー名の選択	XR_C (IKE2)
本装置側のL4N側のネットワークアドレス	192.168.10.0/24 (79):192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.30.0/24 (7):192.168.0.0/24)
FH2のTransFormの選択	aes128-sha1 💌
PFS	<ul> <li>● 使用する</li> <li>● 使用しない</li> </ul>
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)
DISTANCE	1 (1~255まで)

XR\_C(拠点 2)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

#### [IKE/ISAKMPの設定3]

IKE/ISAKMP ポリシーのパラメータは以下のとおりです。

設定項目	パラメータ
IKE/ISAKMP ポリシー名	PC
リモート IP アドレス	0. 0. 0. 0
インタフェースの ID	@vpnclient
モード	Aggressive
暗号化アルゴリズム	AES-128
認証アルゴリズム	SHA1
DH グループ	Group2
ライフタイム	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey3

IKE/ISAKMPポリシー名	PC
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	@vpnclient (例:@xr.centurysys)
モードの設定	aggressive モード 💌
	1番目 group2-aes128-sha1 🔽
two cfum OPP	2番目 使用しない 🛛 👻
transform() as a	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)

PC(拠点3)に対する IKE/ISAKMP ポリシーの設定を行います。

鍵の設定	
<ul> <li>PSKを使用する</li> <li>RSAを使用する</li> <li>(X500を使用する場合は RSAに設定してください)</li> </ul>	ipseckey3

事前共有鍵(PSK)として「ipseckey3」を設定します。

[IPsec ポリシーの設定 3]

🕐 使用する 🔷 使用しない 💿 Responderとして使用する 🔷 On-Dermandで使用する

PC(拠点3)の IP アドレスが不定のため、「Responder として使用する」を選択します。

設定項目	パラメータ
使用する IKE ポリシー名	PC(IKE3)
本装置の 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	192. 168. 40. 1/32
暗号化アルゴリズム	AES-128
認証アルゴリズム	SHA1
PFS (DH グループ)	使用する(Group2)
ライフタイム	28800(秒)
DISTANCE	1

使用するIKEポリシー名の選択	PC (IKE3) 💌
本装置側のL4N側のネオワークアドレス	192.168.10.0/24 (期:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.40.1/32 (別:192.168.0.0/24)
FH2のTransFormの選択	aes128-sha1 💌
PFS	<ol> <li>使用する</li> <li>使用しない</li> </ol>
DH Groupの選択(PFS使用時に有効)	eroup2
SADライフタイム	28800 秒 (1081~86400秒まで)
DISTANCE	1 (1~255まで)

PC(拠点3)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

[IPsec Keep-Alive 設定]

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1 <u>米</u>	動作option 2 <u>米</u>	interface	backup SA
1		192.168.10.1	192.168.20.1	30	3	60			ipsec0 💌	

XR\_B(拠点1)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

<u>IPsecサーバ</u>

○停止 ⊙起動

IPsec サーバ機能を起動します。

#### 拠点1ルータ(XR\_B)

#### ポイント

XR\_A(センター)に対して IPsec 接続を行います。XR\_A, XR\_B ともに WAN 側 IP アドレスが固定 IP アドレ スであるため、鍵交換モードとして「Main モード」を使用しています。

#### <<インタフェース設定>>

[Ethernet0の設定]

<ol> <li>固定アド</li> </ol>	レスで使用	
₽₽Ÿ₽₽ス	192.168.20.1	
ネットマスク	255.255.255.0	
MTU	1500	

Ethernet0の設定をします。

※IPアドレスの設定を変更した場合、その設定した IPアドレスが即反映されます。

[Ethernet1の設定]

● 固定アドレスで使用		
ℙアドレス	0	
ネットマスク	255.255.255.0	
MTU	1500	

PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

#### <<PPP/PPPoE 設定>>

[接続先設定1]

ユーザロ	test2@centurysys
パスワード	test2pass

PPPoE 接続で使用するユーザ ID,パスワードを登録します。

[接続設定]

接続先の選択	●接號先1 ●接読先2 ●接號先3 ●接號先4 ●接読先5
接続ポート	O Ether0 • Ether1 • Ether2 • ERI(64K) • ERI MP(128K) • RS2320
接統形態	○ 手動接続 ○ 常時接続 ○ スケジューラ接続
RS232C/BRI接続タイプ	<ul> <li>● 通常</li> <li>○ On-Demand接続</li> </ul>
ドマスカレード	○無効 ● 有効
ステートフルパケット インスペウション	○無効 ○有効 □DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ● 有効

PPPoE 接続するインタフェース、および接続形態を選択します。 ※この例では、ルータ経由でのインターネットアクセスも可能になっています。



PPPoEの再接続性を高めるために、PPPoE 特殊オプションを設定しています。

#### <<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ррр0	パケ水受信時	許可 🔽	udp 💌		500		500	
ррр0	パケット受信時	許可 💌	esp 💌					

IKE パケット, ESP パケットの「許可」を設定します。

# <<各種サービスの設定>>

# <IPsec サーバ>

[本装置側の設定 1]

インターフェースのIPアドレス	10.10.20.1
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

WAN 側インタフェースの IP アドレス,および上位ルータの IP アドレスを設定します。

[IKE/ISAKMPの設定1]

IKE/ISAKMPポリシー名	XRA
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	(預:@xr.centurysys)
モードの設定	main モード 💌
	1∰目 group2-aes128-sha1 💌
	1番目 group2-aes128-sha1 💌 2番目 使用しない 💌
transformの設定	1番目 group2-aes128-sha1 V 2番目 使用しない V 3番目 使用しない V
transformの設定	1番目 group2-aes128-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 ♥

XR\_A(センター)に対する ISAKMP ポリシーの設定を行います。

鍵の設定	
<ul> <li>PSKを使用する</li> <li>RSAを使用する</li> <li>0509を使用する場合は</li> <li>RSAに設定してください)</li> </ul>	ipseckey1

事前共有鍵(PSK)として「ipseckey1」を設定します。

[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-Dermandで使用する

XR\_A(センター)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

使用するIKEポリシー名の選択	XR_A (IKE1) 💌
本装置側のL4N側のネ・オワークアドレス	192.168.20.0/24 (期: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 (期:192.168.00/24)
FH2のTransFormの選択	aes128-sha1 💌
PFS	💿 使用する 🔘 使用しない
DH Groupの選択(PFS使用時に有効)	eroup2 💌
SADライフタイム	28800 秒 (1081~86400秒まで)
DISTANCE	1 (1~255まで)

XR\_A(センター)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

[IPsec Keep-Alive 設定]

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1 <u>米</u>	動作option 2 <u>米</u>	interface	backup SA
1		192.168.20.1	192.168.10.1	45	3	60			ipsec0 💌	

XR\_A(センター)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

#### 【IPsec サーバ】

IPsecサーバ	○停止	⊙起動	

IPsec サーバ機能を起動します。

#### 拠点2ルータ(XR\_C)

#### ポイント

XR\_A(センター)に対して IPsec 接続を行います。WAN 側 IP アドレスが動的 IP アドレスであるため、鍵 交換モードとして「Aggressive モード」を使用しています。

#### <<インタフェース設定>>

[Ethernet0の設定]

<ol> <li>固定アド</li> </ol>	レスで使用	
⊫rFレス	192.168.30.1	
ネットマスク	255.255.255.0	
MTU	1500	

Ethernet0の設定をします。

※IPアドレスの設定を変更した場合、その設定した IPアドレスが即反映されます。

[Ethernet1の設定]

● DHCPサーバから取得						
ホスト名						
мастрыл						

DHCP サーバから IP アドレスを取得するため、「DHCP サーバから取得」を選択します。

ビマスカレード(p masq)     (このポートで使用するIPアドレスに変換して通信を行います)
🔽 ステートフルパケットインスペクション(spi)

ルータ経由でインターネットアクセスを行う場合、IPマスカレード設定を「有効」にしています。ステ ートフルパケットインスペクション(SPI)を「有効」に設定します。

#### <<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
eth1	パケット受信時	許可 🔽	udp 💌		500		500	
eth1	パケ水受信時	許可 💌	esp 💌					

IKE パケット, ESP パケットの「許可」を設定します。

# <<各種サービスの設定>>

#### <IPsec サーバ>

[本装置側の設定1]

インターフェー スのIPアドレス	%eth1	
上位ルータのIPアドレス		
インターフェースのID	@ipsec2	(例:@xr.centurysys)

Ethernet 接続(DHCP クライアント)で WAN 側(Ether1)インタフェースの IP アドレスが不定のためインタフェースの IP アドレスに「%eth1」、インタフェースの ID として「@ipsec2」を設定します。

[IKE/ISAKMPの設定1]

IKE/ISAKMPポリシー名	XR_A
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 💌
	1╋目 group2-aes128-sha1 💌
	2番目 使用しない 🔽
transformu) ag æ	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)

XR\_A(センター)に対する IKE/ISAKMP ポリシーの設定を行います。

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>	ipseckey2

事前共有鍵(PSK)として「ipseckey2」を設定します。

[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-Dermandで使用する

XR\_A(センター)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

使用するIKEポリシー名の選択	XR_A (KE1) 💌
本装置側のL4N側のネットワークアドレス	192.168.30.0/24 (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 (M:192.168.0.0/24)
FH2のTransFormの選択	aes128-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)
DISTANCE	1 (1~255まで)

XR\_A(センター)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

[IPsec Keep-Alive 設定]

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1 <u>米</u>	動作option 2 <u>米</u>	interface	backup SA
1		192.168.30.1	192.168.10.1	45	3	60			ipsecő 💌	

XR\_A(センター)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

#### 【IPsec サーバ】

IPsecサーバ	○停止	⊙起動	

IPsec サーバ機能を起動します。

#### 拠点3PC(PC)

#### ポイント

拠点3は「FutureNet VPN Client/NET-G」をインストールした PC からの IPsec 接続になります。この例では、PPP 接続による Internet へのアクセスが可能になっている状態とします。

<<既知共有鍵(Pre shared Key)の設定>>

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
日
<u> 適加(D)</u>
OK キャンセル 適用

「鍵管理」タブをクリックし、「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ので、「既知共有鍵を作成する」を選択し、「次へ」ボタンをク リックして下さい。

既知共有鍵		×
既知共有鍵の作成 共有シークレットを入力してください	Ns	
既知共有鍵に自分だけが参照 回入力します。フィンガーブリント 確認します。 既知共有鍵	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 を使用して、実際にシークレットを表示せずに通信相手とシークレットを	
名前:	新しい既知共有鍵	
共有シークレット	*****	
共有シークレットの確認:	kokookok	
フィンガープリント (SHA-1):	6198 60b9	
	< 戻る( <u>B</u> ) 完了 キャンセ	01

「既知共有鍵の作成」画面が開きます。ここで既知共有鍵を作成します。「名前」には任意の設定名を入 カします。「共有シークレット」「共有シークレットの確認」項目には既知共有鍵を入力し、「完了」ボタ ンをクリックします。

この例では共有シークレットとして「ipseckey3」を設定しています。



「鍵管理」画面に戻ります。既知共有鍵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 リックして下さい。「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。 <<ID の設定>>

既知共有鍵	? ×
プロパティ ID	
(第11) 既知共有鍵認証は で行われます。	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:	新しい既知共有鍵
鍵 ID:	
共有シークレット ――――	
共有シークレット	*okokokokokok
シークレットの確認。	****
フィンガープリント	
6198 6069	
_ <u>警告</u>	
ー般的な語句は辞 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

「鍵管理」画面で、登録した既知共有鍵を選択して「プロパティ」をクリックします。「既知共有鍵」画面が開きますので、「ID」タブをクリックします(この画面では既知共有鍵を変更できます)。

既知共有鍵	? ×
プロパティ ID	
通常は、ID を指定する必要はありません。ただし、IKE アグレッシュ モードでは、両方の ID を指定する必要があります。	"
_ I ー ー ー ー ー ー ー ー ー ー ー ー ー ー ー ー ー ー	
プライマリ ID: 📴 ホスト ドメイン名 👤	
ホストドメイン名: vpnclient	
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。	

「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 サーバ「IKE/ISAKMP の設定」における「インタフェー ス ID」と同じ ID を設定します。

※ただしこの時、ホストドメイン名には"@"をつけないで設定して下さい。

セキュリティポリシー 鍵管理
<ul> <li>□ 信頼されたポリシー サーバ</li> <li>□ 信頼された証明書</li> <li>□ 認証局</li> <li>□ リモート ホスト</li> <li>□ アート ホスト</li> <li>□ アート ホスト</li> <li>□ アート ホスト</li> <li>□ アート ホスト</li> <li>□ コート ホスト</li> <li>□ コート</li> <li>□ コート</li></ul>
<u>     通知(位)</u> 削除(13) ブロバティ(中)… 表示(い)… - 説明
ローカル ホストのは24世に使用される鍵です。
OK 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下さい。「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。 <<セキュリティポリシーの設定>>

	<u>? ×</u>
セキュリティ ホリシー   鍵管理	
ポリシー: 1 デフォルト 🔽	
田····································	_
由 🔝 セキュアな接続	規則
■ ③ デフォルト応答	の
	評
	川直
	序
	0
追加(A) 削除(B) ブロパティ(P)	12世斤( <u>D</u> )
<ul> <li>ローカル ホストがセキュリティ ゲートウェイ経由でリモート 一クへの IPSec 接続を確立するときに、仮想プライベート</li> </ul>	プライベート ネットワ
ঠনাৱৰ.	
	1 28 FF
UK 4+9527	

ポリシーエディタの「セキュリティポリシー」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	?	×	
	ゲートウェイ IP アドレス:	10.10.10.1	7	
- P 📃	リモート ネットワーク:	any 💌	]	
	認証鍵	☞ 新しい既知共有鍵	•	
		🔲 レガシ候補を使用する(U)		
i診断(D) (プロパティ(P) OK キャンセル				

「VPN 接続を追加」画面が開きます。「ゲートウェイ IP アドレス」で右端の"IP"をクリックし、XR\_A(センター)の WAN 側 IP アドレスを設定します。

「認証鍵」は、既知共有鍵の設定で登録した既知共有鍵の設定名を選択します。 「リモートネットワーク」については右端にある"・・・"をクリックして下さい。

ットワーク エディタ			?)
100 ネットワー 1000 名前を後	りおよびサブネットワ で使用して相則たり	ークに独自の名前を FRAできます。	付けます。この
~u <sup>™</sup> <u>■</u> ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	сылысыла 5	PARCENTO	
名前	IP アドレス	サブネット マスク	
any any6	0.0.0.0 0::0	0.0.0.0 0::0	
LAN_A	192.168.10.0	200.200.205.0	
		新規(N)	削除( <u>R</u> )
ネットワーク名:	LAN_A		
IP アドレス:	192.168.10.0		<b>N</b>
サブネット マスク:	255.255.255.0		
		OK	キャンセル

「ネットワークエディタ」画面が開きます。

「ネットワーク名」は任意の名前を設定することができます。

「IPアドレス」「サブネットマスク」はXRに接続しているLANについて設定し(ここではLAN\_A[センター側のネットワーク]の値を設定しています)、「OK」をクリックします。

VPN 接続	を追加		? X
	ゲートウェイ IP アドレス:	10.10.10.1	IP
₩₫,	リモート ネットワーク:	LAN_A	·
	認証鍵	🐖 新しい既知共有鍵	-
		□ レガシ候補を使用する	(U)
	( <u>D</u> ) プロパティ(P).	. OK ++>	セル

リモートネットワーク設定後、「VPN 接続を追加」画面が開きますので、続いてプロパティをクリックします。

規則のプロパ	रिन्द		? ×
全般	羊細		
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	IP
Simut	リモート ネットワーク:	LAN_A	<b>•</b>
IPSec /	IKE 候補		
- 🌮	認証鍵	☞ 新しい既知共有	ī键 ▼
v	候補テンプレート:	normal	•
匚 仮想	見IP アドレスを取得する		[] [[]]][[]]][[]]][[]]][[]]][[
- P-	仮想 IP アドレスは、内部 です。	ネットワークのアドレス	
	<sup>観</sup> 忍証 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
a/L=/]		ļ	変更( <u>C</u> )
		OK	キャンセル

「規則のプロパティ」画面が開きます。ここで 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		? ×
😵 IKE 候補と IPSec 修	実補の各パラメータ値を設定します。	
∛ ┌IKE 候補		
暗号化アルゴリズム:	AES-128	•
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:	AES-128	•
整合性関数:	HMAC-SHA-1	•
IPSec モード:	tunnel	~
PFS グループ:	MODP 1024 (group 2)	-
「「 避快」た使のPaた候類(Thr	173	
● 通知(いた)直(いの)を)大性的にの	1/2	
	( OK キャン	セル

「パラメータ候補画面」が開きます。ここで暗号化方式などを設定します。IKE モードは「aggressive mode」を設定します。また「選択した値のみを候補に加える」にチェックをいれます。
規則のプロパ	<del>ティ</del>		? ×
全般	É約田		
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	IP
Similar	リモート ネットワーク:	LAN_A	<b>•</b>
IPSec /	IKE 候補		
P	認証鍵:	🐖 新しい既知共有	键 🔽
Ň	候補テンプレート	normal	•
			設定
☑ 仮想	見IP アドレスを取得する		
- <b>1</b> -	仮想 IP アドレスは、内部オ です。	ミットワークのアドレス	
□ 拡張	121 <b>1</b>		
	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	
- 記四月-			<b>本</b> 更(0) 1
		_	<u>&amp; E \U/</u>
		C OK	キャンセル

「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、「設定」ボタンをクリックします。

仮想 IP アドレス		? ×
画 仮想 IP アドレス 小画 行います。	なに割り当てるプロトコルを選択するか、手動で	設定を
לסלים אבר אבר		
C IPSec 経田の DHCH	' (Dynamic Host Configuration Protocol)	
C L2TP (Layer Two Ti	unneling Protocol)	
○ IKE 設定モード		
┌● 手動で指定:		
IP アドレス:	192.168.40.1	
サブネット マスク:	255.255.255.0	
ーロ DNS サーバと WINS	サーバを指定する:	
DNS サーバ		
WINS サーバ		
	0K ++>t	211

「仮想 IP アドレス」画面が開きます。

ここでは XR に接続する際に使用するこの PC の仮想的な 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 サーバにおける「IPsec ポリシーの設定」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。この例では、サブネットマスクは 24 ビットマスクとしています。

※XR\_A(センター)の IPsec ポリシーで設定したサブネットと異なるので注意して下さい。

(32 ビットマスクは設定することができません。)

これで設定は完了です。

続いて IPsec 接続を行います。



タスクバーの中にある FutureNet Net-G VPNclient のアイコンを右クリックします。そして「VPN を選択」の指定し、作成した IPsec ポリシーを選択します。

VPN 接続の状態		×
次の場所への VPN 接続を開いてい	います 10.10.10.1 (LAN_A)	
		「キャンセル」

選択後、IKEのネゴシエーションを行う画面が表示されます。



IPsec が正常に確立した場合、「VPN 接続は正常に確立しました」という画面が表示されます。

これで IPsec 接続は完了です。

なおこの設定例では、IPsec 接続時の Internet へのアクセスは拒否になっています。

IPsec 接続と Internet へのアクセスを両方同時に利用したい場合には、以下の設定を行って下さい。

規則のプロパティ
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)
詳細オプション
<ul> <li>○ IP 圧縮を適用する Q</li> <li>○ PMTU (Path Maximum Transfer Unit) を発見する (M)</li> <li>○ NAT 装置を経由する</li> <li>○ NAT-T (Network Address Translation Traversal)</li> <li>○ ボート(ご適用する UDP カフセルビ: 2746</li> <li>□ 起動時に開く (S)</li> <li>□ 分割トンネリングを拒否する</li> </ul>
のK キャンセル

「規則のプロパティ」画面を開き、「詳細タブ」をクリックします。ここで詳細オプションにある「分割 トンネリングを拒否する」のチェックボックスのチェックを外します。

# 2. IPsec を利用したセンター経由インターネット接続例

この例は、PPPoE や Ether での接続で IPsec によるインターネット VPN を行い、拠点の端末はインター ネットアクセスする場合、センターの XR 経由でアクセスするというものです。 またこの例では、センター<->拠点間の通信だけではなく、拠点間通信も可能になっています。

## 2-1. 構成例



## 2-2. 要件

- ▶ インタフェースおよび PPPoE
  - XR\_A(センター), XR\_B(拠点 1)はインターネットに PPPoE で接続します。
  - XR\_C(拠点 2)はインターネットに Ether で接続します。
  - PPPoE 接続は、自動再接続するように設定しています。
  - WAN 側インタフェースの IP マスカレードは「無効」、ステートフルパケットインスペクションは「有効」にしています。

主なインタフェースおよび PPPoE のパラメータ

	XR_A(センター)	XR_B(拠点1)	XR_C(拠点 2)
LAN 側インタフェース	Ether0	Ether0	Ether0
LAN 側 IP アドレス	192. 168. 10. 1	192. 168. 20. 1	192. 168. 30. 1
WAN 側インタフェース	Ether1[ppp0]	Ether1[ppp0]	Ether1
WAN 側 IP アドレス	10. 10. 10. 1	動的 IP	10. 10. 30. 1
PPPoE ユーザ名	test1@centurysys	test2@centurysys	_
PPPoE パスワード	test1pass	test2pass	_
接続回線	PPPoE 接続	PPPoE 接続	Ether 接続

≻ IPsec

- 鍵交換モードは XR\_A <-> XR\_B はアグレッシブモード, XR\_A <-> XR\_C はメインモードを使用しています。
- XR\_A(センター)は 0.0.0.0/0 <-> 192.168.20.0/24, 192.168.30.0/24 の時に IPsec を適用します。
- XR\_B(拠点 1)は 192. 168. 20. 0/24 <-> 0. 0. 0. 0/0 の時に IPsec を適用します。
- XR\_C(拠点 2)は192.168.30.0/24 <-> 0.0.0.0/0の時に IPsec を適用します。
- XR\_A(センター)は、XR\_C(拠点 2)に対してのみ IPsec KeepAlive を使用しています。
- XR\_B(拠点 1)は、XR\_A(センター)に対して IPsec KeepAlive を使用しています。
- XR\_C(拠点 2)は、XR\_A(センター)に対して IPsec KeepAlive を使用しています。

本装置側のパラメータ

	XR_A(センター)	XR_B(拠点1)	XR_C(拠点 2)
インタフェースの IP アドレス	10. 10. 10. 1	%ppp0	10. 10. 30. 1
上位ルータの IP アドレス	%ppp0		10. 10. 30. 254
インタフェースの ID		@ipsec1	

	XR_A(センター)	
対向拠点	XR_B(拠点 1)	XR_C(拠点 2)
IKE/ISAKMP ポリシー名	XR_B	XR_C
リモート IP アドレス	0. 0. 0. 0	10. 10. 10. 1
インタフェースの ID	@ipsec1	
モード	Aggressive	Main
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
DH グループ	Group2	Group2
ライフタイム	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey2

IKE/ISAKMP ポリシーのパラメータ(1) 「XR\_A(センター)」

IPsec ポリシーのパラメータ(1) 「XR\_A(センター)」

	XR_A(センター)		
対向拠点	XR_B(拠点1)	XR_C(拠点 2)	
使用する IKE ポリシー名	XR_B(IKE1)	XR_C(IKE2)	
本装置の LAN 側のネットワークアドレス	0.0.0.0/0	0.0.0/0	
相手側の LAN 側のネットワークアドレス	192. 168. 20. 0/24	192. 168. 30. 0/24	
暗号化アルゴリズム	AES-128	AES-128	
認証アルゴリズム	SHA1	SHA1	
PFS (DH グループ)	使用する(Group2)	使用する(Group2)	
ライフタイム	28800(秒)	28800(秒)	
DISTANCE	1	1	

	XR_B(拠点 1)	XR_C(拠点 2)
対向拠点	XR_A(センター)	XR_A(センター)
IKE/ISAKMP ポリシー名	XR_A	XR_A
リモート IP アドレス	10. 10. 10. 1	10. 10. 10. 1
モード	Aggressive	Main
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
DH グループ	Group2	Group2
ライフタイム	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey2

IKE/ISAKMP ポリシーのパラメータ(2) 「XR\_B(拠点 1), XR\_C(拠点 2)」

IPsec ポリシーのパラメータ(2) 「XR\_B(拠点 1), XR\_C(拠点 2)」

	XR_B(拠点 1)	XR_C(拠点 2)
対向拠点	XR_A(センター)	XR_A(センター)
使用する IKE ポリシー名	XR_A(IKE1)	XR_A(IKE1)
本装置の LAN 側のネットワークアドレス	192. 168. 20. 0/24	192. 168. 30. 0/24
相手側の LAN 側のネットワークアドレス	0.0.0.0/0	0.0.0/0
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
PFS (DH グループ)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)
DISTANCE	1	1

IPsec Keepalive のパラメータ

	XR_A(センター)	XR_B(拠点1)	XR_C(拠点 2)
対向拠点	XR_C(拠点2)	XR_A(センター)	XR_A(センター)
Policy No.	2	1	1
source address	192. 168. 10. 1	192. 168. 20. 1	192. 168. 30. 1
destination address	192. 168. 30. 1	192. 168. 10. 1	192. 168. 10. 1
interval(sec)	30	45	45
watch count	3	3	3
timeout/delay(sec)	60	60	60
動作option	1	2	1
interface	ipsec0	ipsec0	ipsec6

## 2-3. 設定例

### センタールータ(XR\_A)

ポイント

拠点 1,2 と IPsec 接続するための設定を行います。

XR\_B(拠点 1)は動的 IP のため、アグレッシブモードを使用しています。

## 〈〈インタフェース設定〉〉

[Ethernet0の設定]

<ol> <li>固定アド</li> </ol>	レスで使用
ℙアドレス	192.168.10.1
ネットマスク	255.255.255.0
MTU	1500

Ethernet0 に関する設定をします。

※IPアドレスの設定を変更した場合、その設定した IPアドレスが即反映されます。

[Ethernet1の設定]

●固定アドレスで使用					
ℙアドレス	0				
ネットマスク	255.255.255.0				
MTU	1500				

Ethernet1 に関する設定をします。

PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

## <<PPP/PPPoE 設定>>

[接続先設定1]

ユーザロ	test1@centurysys	]
パスワード	test1pass	

PPPoE 接続で使用するユーザ ID,パスワードを登録します。

[接続設定]

接続先の選択	●接號先1 ●接號先2 ●接號先3 ●接號先4 ●接読先5
接続ボート	O Ether0 • Ether1 • Ether2 • BRI(64K) • BRI MP(128K) • RS232C
接統形態	○ 手動接続 ○ 常時接続 ○ スケジューラ接続
RS232C/BRI接続タイプ	<ul> <li>● 通常</li> <li>○ On-Demand接続</li> </ul>
ドマスカレード	○無効 ● 有効
ステートフルパケット インスペウション	○ 無効 ● 有効 □ DROP したパケットのLOGを取得
デフォルトルートの設定	○ 無効 ● 有効

PPPoE 接続するインタフェース、および接続形態を選択します。 ※この例では、ルータ経由でのインターネットアクセスも可能になっています。



PPPoEの再接続性を高めるために、PPPoE 特殊オプションを設定しています。

## <<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ррр0	パケ水受信時	許可 🔽	udp 💌		500		500	
ррр0	パケ水受信時	許可 🔽	esp 💌					

IKE パケット, ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

## <<各種サービスの設定>>

#### <IPsec サーバ>

[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	%ррр0	
インターフェー スのID	(例:@xr.centurys)	rs)

XR\_A(センター)のWAN側インタフェースのIPアドレス,および上位ルータのIPアドレスを設定します。 PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。

[IKE/ISAKMPの設定1]

IKE/ISAKMPポリシー名	XR_B					
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	@ipsec1 (例:@xr.centurysys)					
エードの恐定	and the Table 19					
C-PORE	aggressive thr					
C-1:022	aggressive					
	aggressive モート V 1番目 group2-aes128-sha1 V 2番目 使用しない V					
transformの設定	aggressive モート V 1番目 group2-aes128-sha1 V 2番目 使用しない V 3番目 使用しない V					
モードの設定 transformの設定	aggressive モート V 1番目 group2-aes128-sha1 V 2番目 使用しない V 4番目 使用しない V					

XR\_B(拠点 1)に対する IKE/ISAKMP ポリシーを設定します。

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 RSAL設定してください)</li> </ul>	ipseckey1

事前共有鍵(PSK)として「ipseckey1」を設定しています。

[IPsec ポリシーの設定 1]

○ 使用する ○ 使用しない ③ Responderとして使用する ○ On-Dermandで使用する

XR\_B(拠点1)の IP アドレスが不定のため、「Responder として使用する」を選択します。

使用するIKEポリシー名の選択	XR_B (IKE1) 💌
本装置側のL4N側のネオワークアドレス	0.0.0.0/0 (期:192.168.00/24)
相手側のLAN側のネットワークアドレス	192.168.20.0/24 (第:192.168.0.0/24)
FH2のTransFormの選択	aes128-sha1 💌
PFS	<ul> <li>● 使用する</li> <li>● 使用しない</li> </ul>
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)
DISTANCE	1 ()~255まで)

XR\_B(拠点 1)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。

[IKE/ISAKMPの設定 2]

IKE/ISAKMPポリシー名	XR_C					
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	10.10.30.1					
上位ルータのIPアドレス						
インターフェー スのЮ	(預:@xr.centurysys)					
モードの設定	main モード					
	1╋目 group2-aes128-sha1 💌					
	2番目 使用しない 💌					
transform() ag at	3番目 使用しない 🔽					
	4番目 使用しない 🔽					

XR\_C(拠点 2)に対する ISAKMP ポリシーの設定を行います。

鍵の設定	
<ul> <li>PSKを使用する</li> <li>RSAを使用する</li> <li>(X500を使用する場合は RSAに設定してください)</li> </ul>	ipseckey2

事前共有鍵(PSK)として「ipseckey2」を設定します。

[IPsec ポリシーの設定 2]

💿 使用する 🔿 使用しない 🔿 Responderとして使用する 🔿 On-Dermandで使用する

XR\_C (拠点 2)に対して IKE のネゴシエーションを行うため、「使用する」を選択しています。

使用するIKEポリシー名の選択	XR_C ((KE2) 🔽
本装置側のL4M側のネオワークアドレス	0.0.0.0/0 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.30.0/24 (期:192.168.00/24)
PH2のTransFormの選択	aes128-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)
DISTANCE	1 (1~255まで)

XR\_C(拠点 2)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

[IPsec Keep-Alive 設定]

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1 <u>米</u>	動作option 2 <u>米</u>	interface	backup SA
1				30	3	60			ipsec0 💌	
2	<b>V</b>	192.168.10.1	192.168.30.1	30	3	60			ipsec0 💌	

XR\_C(拠点2)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

I <u>Psecサーバ</u>	○停止	⊙起動	

IPsec サーバ機能を起動します。

## 拠点1ルータ(XR\_B)

#### ポイント

XR\_A(センター)に対して IPsec 接続を行います。WAN 側 IP アドレスが動的 IP アドレスであるため、鍵 交換モードとして「Aggressive モード」を使用しています。

### <<インタフェース設定>>

[Ethernet0の設定]

<ol> <li>固定アド</li> </ol>	レスで使用
₽₽Ÿ₽₽ス	192.168.20.1
ネットマスク	255.255.255.0
мти	1500

Ethernet0の設定をします。

※IPアドレスの設定を変更した場合、その設定した IPアドレスが即反映されます。

[Ethernet1の設定]

● 固定アドレスで使用					
ℙアドレス	0				
ネットマスク	255.255.255.0				
MTU	1500				

PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

### <<PPP/PPPoE 設定>>

[接続先設定1]

ユーザロ	test2@centurysys
パスワード	test2pass

PPPoE 接続で使用するユーザ ID,パスワードを登録します。

[接続設定]

接続先の選択	●接號先1 ●接號先2 ●接號先3 ●接號先4 ●接読先5
接続ボート	O Ether0 • Ether1 • Ether2 • BRI(64K) • BRI MP(128K) • RS232C
接統形態	○ 手動接続 ○ 常時接続 ○ スケジューラ接続
RS232C/BRI接続タイプ	<ul> <li>● 通常</li> <li>○ On-Demand接続</li> </ul>
IPマスカレード	⊙ 無効 ○ 有効
ステートフルパケット インスペウション	○ 無効 ○ 有効 □ DROP したパケットのLOGを取得
デフォルトルートの設定	○ 無効 ● 有効

PPPoE 接続するインタフェース、および接続形態を選択します。

インターネットアクセスはセンター経由で行うため、IPマスカレード設定を「無効」にしています。



PPPoEの再接続性を高めるために、PPPoE 特殊オプションを設定しています。

## <<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ррр0	パケ水受信時	許可 🔽	udp 💌		500		500	
рррО	パケット受信時	許可 🔽	esp 💌					

IKE パケット, ESP パケットの「許可」を設定します。

## <<各種サービスの設定>>

#### <IPsec サーバ>

[本装置側の設定 1]

インターフェー スのIPアドレス	%рррО	
上位ルータのIPアドレス		
インターフェースのID	@ipsec1	(例:@xr.centurysys)

PPPoE 接続で WAN 側(ppp0)インタフェースの IP アドレスが不定のため「%ppp0」, インタフェースの ID として「@ipsec1」を設定します。

[IKE/ISAKMPの設定1]

IKE/ISAKMPポリシー名	XR_A
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Ю	(例:@xr.centurysys)
モードの設定	aggressive モード 💌
	1∰目 group2-aes128-sha1 💌
	2番目 使用しない 🔽
(ransiormo) ague	3番目 使用しない 💌
	4番目 使用しない 🔽

XR\_A(センター)に対する ISAKMP ポリシーの設定を行います。

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 RSAL設定してください)</li> </ul>	ipseckey1

事前共有鍵(PSK)として「ipseckey1」を設定します。

[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-Dermandで使用する

XR\_A(センター)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

使用するIKEポリシー名の選択	XR_A (IKE1) 💌
本装置側のL4N側のネットワークアドレス	192.168.20.0/24 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	0.0.0.0/0 (期:192.168.0.0/24)
FH2のTransFormの選択	aes128-sha1 💌
PFS	<ul> <li>● 使用する</li> <li>● 使用しない</li> </ul>
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)
DISTANCE	1 (1~255まで)

XR\_A(センター)に対して IPsec 通信を行う IP アドレスの範囲を設定します。 この例では、IPsec 通信を行う宛先 IP アドレスを「0.0.0.0/0」に設定しています。

[IPsec Keep-Alive 設定]

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1 <u>米</u>	動作option 2 <u>米</u>	interface	backup SA
1		192.168.20.1	192.168.10.1	45	3	60			ipsec0 💌	

XR\_A(センター)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

<u>IPsecサーバ</u>	○停止	⊙起動	
-----------------	-----	-----	--

IPsec サーバ機能を起動します。

## 拠点2ルータ(XR\_C)

### ポイント

XR\_A(センター)に対して IPsec 接続を行います。XR\_A, XR\_C の WAN 側 IP アドレスが固定 IP アドレスで あるため、鍵交換モードとして「Main モード」を使用しています。

### <<インタフェース設定>>

[Ethernet0の設定]

<ol> <li></li></ol>	レスで使用	
ℙアドレス	192.168.30.1	
ネットマスク	255.255.255.0	
MTU	1500	

Ethernet0の設定をします。

※IPアドレスの設定を変更した場合、その設定した IPアドレスが即反映されます。

[Ethernet1の設定]

◎固定アド		
IP アドレス	10.10.30.1	
ネットマスク	255.255.255.0	]
мти	1500	

WAN 側 IP アドレスの設定をします。

	IPマスカレード(pimasq) (このポートで使用するIPアドレスに変換して通信を行います)	
$\checkmark$	ステートフルパケットインスペウション(spi)	

インターネットアクセスはセンター経由で行うため、IPマスカレード設定を「無効」にしています。ス テートフルパケットインスペクション(SPI)を「有効」に設定します。

#### <<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
eth1	パケット受信時	許可 💌	udp 💌		500		500	
eth1	パケット受信時	許可 🔽	esp 💌					

IKE パケット, ESP パケットの「許可」を設定します。

#### <<各種サービスの設定>>

#### <IPsec サーバ>

[本装置側の設定 1]

インターフェー スのIPアドレス	10.10.30.1
上位ルータのIPアドレス	10.10.30.254
インターフェー スのゆ	(例:@xr.centurysys)

XR\_A(センター)のWAN 側インタフェースのIPアドレス,および上位ルータのIPアドレスを設定します。 ※Ether 接続でWAN 側 IP アドレスが固定 IP の場合、「上位ルータの IP アドレス」は「%eth1」と設定 することはできません。 [IKE/ISAKMPの設定1]

IKE/ISAKMPポリシー名	XR_A
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Ю	(例:@xr.centurysys)
モードの設定	main モード
	1╋目 group2-aes128-sha1 💌
	2番目 使用しない 🛛 👻
transformu) ag je	3番目 使用しない 🛛 👻
	4番目 使用しない 💌

XR\_A(センター)に対する ISAKMP ポリシーの設定を行います。

鍵の設定	
<ul> <li>PSKを使用する</li> <li>RSAを使用する</li> <li>(X500を使用する場合は</li> <li>RSAに設定してください)</li> </ul>	ipseckey2

事前共有鍵(PSK)として「ipseckey2」を設定します。

[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-Dermandで使用する

XR\_A(センター)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

使用するIKEポリシー名の選択	XR_A (KE1) 💌
本装置側のL4N側のネットワークアドレス	192.168.30.0/24 (期: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 (₩:192.168.0.0/24)
FH2のTransFormの選択	aes128-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)
DISTANCE	1 (1~255まで)

XR\_A(センター)に対して IPsec 通信を行う IP アドレスの範囲を設定します。 この例では、IPsec 通信を行う宛先 IP アドレスを「0.0.0.0/0」に設定しています。

[IPsec Keep-Alive 設定]

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1 <u>米</u>	動作option 2 <u>米</u>	interface	backup SA
1		192.168.30.1	192.168.10.1	45	3	60			ipsecő 💌	

XR\_A(センター)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

<u>IPsecサーバ</u>	○停止	⊙起動	
-----------------	-----	-----	--

IPsec サーバ機能を起動します。

# 3. 複数セグメントでの IPsec 設定例

IPsec を行っている XR 配下に複数のセグメントがあった場合の IPsec 設定例になります。 この例では、センター側にある2つのセグメントに対して IPsec ポリシーを2つ作成しています。

## 3-1. 構成例



## 3-2. 要件

- ▶ インタフェースおよび PPPoE
  - XR\_A(センター1), XR\_B(拠点)はインターネットに PPPoE で接続します。
  - XR\_A2(センター2)はローカルルータになります。
  - PPPoE 接続は、自動再接続するように設定しています。
  - XR\_A(センター1), XR\_B(拠点)の WAN 側インタフェースの IP マスカレードは「有効」, ステートフルパケットインスペクションは「有効」にしています。

主なインタフェースおよび PPPoE のパラメータ(1)

	XR_A(センター)	XR_B(拠点)
LAN 側インタフェース	Ether0	Ether0
LAN 側 IP アドレス	192. 168. 110. 1	192. 168. 20. 1
WAN 側インタフェース	Ether1[ppp0]	Ether1[ppp0]
WAN 側 IP アドレス	10. 10. 10. 1	動的 IP
PPPoE ユーザ名	test1@centurysys	test2@centurysys
PPPoE パスワード	test1pass	test2pass
接続回線	PPPoE 接続	PPPoE 接続

主なインタフェースおよび PPP/PPPoE のパラメータ(2)

	XR_A2(センター2)
LAN 側インタフェース	Ether0
LAN 側 IP アドレス	192. 168. 10. 1
WAN 側インタフェース	Ether1
WAN 側 IP アドレス	192. 168. 110. 254
デフォルトゲートウェイ	192. 168. 110. 1

➢ IPsec

- 鍵交換モードは XR\_A <-> XR\_B はアグレッシブモードを使用しています。
- XR\_A(センター1)は 192.168.10.0/24, 192.168.110.0/24 <-> 192.168.20.0/24 の時 に IPsec を適用します。
- XR\_B(拠点)は 192.168.20.0/24 <-> 192.168.10.0/24, 192.168.110.0/24 の時に IPsec を適用します。
- XR\_B(拠点)は、XR\_A(センター)に対して IPsec KeepAlive を使用しています。

本装置側のパラメータ

	XR_A(センター1)	XR_B(拠点)
インタフェースの IP アドレス	10. 10. 10. 1	%ppp0
上位ルータの IP アドレス	%ppp0	
インタフェースの ID		@ipsec1

IKE/ISAKMP ポリシーのパラメータ 「XR\_A(センター1), XR\_B(拠点)」

	XR_A(センター1)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター1)
IKE/ISAKMP ポリシー名	XR_B	XR_A
リモート IP アドレス	0. 0. 0. 0	10. 10. 10. 1
インタフェースの ID	@ipsec1	
モード	Aggressive	Aggressive
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
DHグループ	Group2	Group2
ライフタイム	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey1

IPsec ポリシーのパラメータ(1) 「XR\_A(センター1)」

	XR_A(セ	ンター1)
対向拠点	XR_B (	[拠点]
使用する IKE ポリシー名	XR_B(IKE1)	XR_B(IKE1)
本装置の LAN 側のネットワークアドレス	192. 168. 10. 0/24	192. 168. 110. 0/24
相手側の LAN 側のネットワークアドレス	192. 168. 20. 0/24	192. 168. 20. 0/24
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
PFS (DH グループ)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)
DISTANCE	1	1

IPsec ポリシーのパラメータ(2) 「XR\_B(拠点)」

	XR_B(拠点)		
対向拠点	XR_A(センター)		
使用する IKE ポリシー名	XR_A(IKE1)	XR_A(IKE1)	
本装置の LAN 側のネットワークアドレス	192. 168. 20. 0/24	192. 168. 20. 0/24	
相手側の LAN 側のネットワークアドレス	192. 168. 10. 0/24	192. 168. 110. 0/24	
暗号化アルゴリズム	AES-128	AES-128	
認証アルゴリズム	SHA1	SHA1	
PFS (DH グループ)	使用する(Group2)	使用する(Group2)	
ライフタイム	28800(秒)	28800(秒)	
DISTANCE	1	1	

IPsec Keepalive のパラメータ

	XR_B(拠点)		
対向拠点	XR_A(センター)		
Policy No.	1	2	
source address	192. 168. 20. 1	192. 168. 20. 1	
destination address	192. 168. 10. 254	192. 168. 110. 1	
Interval(sec)	45	60	
watch count	3	3	
timeout/delay(sec)	60	60	
動作option	2	2	
interface	ipsec0	ipsec0	

- ▶ その他
- XR\_A(センター1)では、XR\_B(拠点)の IPsec 192.168.20.0/24 <-> 192.168.10.0/24
   の IPsec KeepAlive 応答用に仮想インタフェース設定で「192.168.10.254」を設定しています。

#### 3-3. 設定例

#### センタールータ (XR\_A)

ポイント

拠点と IPsec 接続するための設定を行います。

XR\_B(拠点)は動的 IP のため、アグレッシブモードを使用しています。

「192.168.10.0/24」,「192.168.110.0/24」の二つのセグメントで IPsec を使用しますので、IPsec ポ リシーを二つ設定しています。

XR\_B(拠点)の IPsec 192.168.20.0/24 <-> 192.168.10.0/24 の IPsec KeepAlive 応答用に仮想インタフ ェース設定で「192.168.10.254」を設定しています。

#### <<インタフェース設定>>

[Ethernet0の設定]

<ol> <li>固定アド</li> </ol>	レスで使用	
IP 7F レス	192.168.110.1	
ネットマスク	255.255.255.0	
мти	1500	

Ethernet0 に関する設定をします。

※IPアドレスの設定を変更した場合、その設定した IPアドレスが即反映されます。

[Ethernet1の設定]

<ol> <li>固定アド</li> </ol>	レスで使用	
₽₽Fレス	0	
ネットマスク	255.255.255.0	
мти	1500	

Ethernet1 に関する設定をします。 PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

#### <<PPP/PPPoE 設定>>

[接続先設定1]

ユーザロ	test1@centurysys	
パスワード	test1pass	

PPPoE 接続で使用するユーザ ID,パスワードを登録します。

[接続設定]

接続先の選択	●接號先1 ●接読先2 ●接號先3 ●接號先4 ●接読先5
接続ボート	O Ether0 • Ether1 • Ether2 • BRI(64K) • BRI MP(128K) • RS232C
接統形態	○ 手動接続 ○ 常時接続 ○ スケジューラ接続
RS232C/BRI接続タイプ	<ul> <li>● 通常</li> <li>● On-Demand接続</li> </ul>
ドマスカレード	○無効 ● 有効
ステートフルパケット インスペウション	○無効 ○有効 □DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ● 有効

PPPoE 接続するインタフェース、および接続形態を選択します。 ※この例では、ルータ経由でのインターネットアクセスも可能になっています。



PPPoEの再接続性を高めるために、PPPoE 特殊オプションを設定しています。

## <<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ррр0	パケオ受信時	許可 🚩	udp 💌		500		500	
рррО	パケオ受信時	許可 🚩	esp 💌					

IKE パケット, ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

## <<スタティックルート設定>>

アドレス	ネットマスク	インターフェー ス/ゲートウェイ	ディスタンス (1-255>
192.168.10.0	255.255.255.0	192.168.110.254	1

LAN A(192.168.10.0/24)宛のパケットを XR\_A2 へ転送するための設定をしています。

## <<各種サービスの設定>>

#### <IPsec サーバ>

[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	%ррр0
インターフェー スのID	(例:@xr.centurysys)

XR\_A(センター)のWAN側インタフェースのIPアドレス,および上位ルータのIPアドレスを設定します。 PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。

[IKE/ISAKMPの設定1]

IKE/ISAKMPポリシー名	XR_B
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	@ipsec1 (例:@xr.centurysys)
モードの設定	aggressive モード 💌
	1番目 group2-aes128-sha1 💌
	1番目 group2-aes128-sha1 👻 2番目 使用しない 🛛 👻
transformの設定	1番目 group2-aes128-sha1 ♥ 2番目 使用しない ♥ 3番目 使用しない ♥
transformの設定	1番目 group2-aes128-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 ♥

XR\_B(拠点 1)に対する IKE/ISAKMP ポリシーを設定します。

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 RSAL設定してください)</li> </ul>	ipseckey1

事前共有鍵(PSK)として「ipseckey1」を設定しています。

[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-Dermandで使用する

XR\_B(拠点)の IP アドレスが不定のため、「Responder として使用する」を選択します。

使用するIKEポリシー名の選択	XR_B (IKE1) 💌
本装置側のL4V側のネットワークアドレス	192.168.10.0/24 (例:192.168.00/24)
相手側のLAN側のネットワークアドレス	192.168.20.0/24 (M):192.168.0.0/24)
FH2のTransFormの選択	aes128-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)
DISTANCE	1 ()~255まで)

XR\_B(拠点)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。

この IPsec ポリシーは、192.168.10.0/24 <-> 192.168.20.0/24 の通信に適用されます。

[IPsec ポリシーの設定 2]

🕐 使用する 🔷 使用しない 📀 Responderとして使用する 🔷 On-Demandで使用する

XR\_B(拠点)の IP アドレスが不定のため、「Responder として使用する」を選択します。

使用するIKEポリシー名の選択	XR_B (IKE1) 💌
本装置側のL4N側のネットワークアドレス	192.168.110.0/24 (第1:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.20.0/24 (第1:192.168.0.0/24)
PH2のTransFormの選択	aes128-sha1 💌
PFS	<ul> <li>● 使用する</li> <li>● 使用しない</li> </ul>
DH Groupの選択(PFS使用時に有効)	group2
SADライフタイム	28800 彩 (1081~86400秒まで)
DISTANCE	1 0~255まで)

XR\_B(拠点)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。

この IPsec ポリシーは、192.168.110.0/24 <-> 192.168.20.0/24 の通信に適用されます。

#### 【IPsec サーバ】



IPsec サーバ機能を起動します。

<<仮想インタフェース設定>>

インターフェース	仮想L/F番号	IPアドレス	ネットマスク	
lo	1	192.168.10.254	255.255.255.255	

仮想インタフェース設定で「lo」インタフェースを設定します。

このインタフェースは XR\_B(拠点)の IPsec 192.168.20.0/24 <-> 192.168.10.0/24 の IPsec KeepAlive 応答用に設定しています。

この設定を行うことにより、「192.168.10.254」宛のパケットを XR\_A(センター1)で受信した場合は、 XR\_A(センター1)が応答を返すようになります。 センタールータ 2(XR\_A2)

## ポイント

この設定例では、センタールータ2(XR\_A2)の設定例は記載していません。 センタールータ2(XR\_A2)の主な必要な要件は以下のとおりです。

・宛先 192.168.20.0/24 ゲートウェイ 192.168.110.1のスタティックルートが設定され ていること

## 拠点ルータ(XR\_B)

ポイント

XR\_A(センター1)に対して IPsec 接続を行います。WAN 側 IP アドレスが動的 IP アドレスであるため、鍵 交換モードとして「Aggressive モード」を使用しています。

IPsec 通信の宛先として 192. 168. 10. 0/24, 192. 168. 110. 0/24 がありますので、IPsec ポリシーを 2 つ設 定しています。

## 〈〈インタフェース設定〉〉

[Ethernet0の設定]

<ul> <li>固定アド</li> </ul>	レスで使用
ℙアドレス	192.168.20.1
ネットマスク	255.255.255.0
MTU	1500

Ethernet0の設定をします。

※IPアドレスの設定を変更した場合、その設定した IPアドレスが即反映されます。

[Ethernet1の設定]

<ol> <li>固定アド</li> </ol>	レスで使用	
IPアドレス	0	
ネットマスク	255.255.255.0	
MTU	1500	

PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

#### <<PPP/PPPoE 設定>>

[接続先設定1]

ユーザロ	test2@centurysys
パスワード	test2pass

PPPoE 接続で使用するユーザ ID,パスワードを登録します。

[接続設定]

接続先の選択	●接號先1 ●接読先2 ●接號先3 ●接號先4 ●接読先5
接続ポート	O Ether0 • Ether1 • Ether2 • ERI(64K) • ERI MP(128K) • RS2320
接統形態	○ 手動接続 ○ 常時接続 ○ スケジューラ接続
RS232C/BRI接続タイプ	<ul> <li>● 通常</li> <li>○ On-Demand接続</li> </ul>
ドマスカレード	○無効 ● 有効
ステートフルパケット インスペウション	○無効 ○有効 □DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ● 有効

PPPoE 接続するインタフェース、および接続形態を選択します。 ※この例では、ルータ経由でのインターネットアクセスも可能になっています。



PPPoEの再接続性を高めるために、PPPoE 特殊オプションを設定しています。

## <<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ррр0	パケ水受信時	許可 🔽	udp 💌		500		500	
рррО	パケット受信時	許可 💌	esp 💌					

IKE パケット, ESP パケットの「許可」を設定します。

<<各種サービスの設定>>

<IPsec サーバ>

[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	@ipsec1	(例:@xr.centurysys)

PPPoE 接続で WAN 側(ppp0)インタフェースの IP アドレスが不定のため「%ppp0」, インタフェースの ID として「@ipsec1」を設定します。

[IKE/ISAKMPの設定1]

IKE/ISAKMPポリシー名	XR_A
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Ю	(例:@xr.centurysys)
モードの設定	aggressive モード 💌
	1∰目 group2-aes128-sha1 💌
	2番目 使用しない 💌
(ransiorno)ag a	3番目 使用しない 🛛 👻
	4番目 使用しない 🔽

XR\_A(センター1)に対する ISAKMP ポリシーの設定を行います。

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 RSAL設定してください)</li> </ul>	ipseckey1

事前共有鍵(PSK)として「ipseckey1」を設定します。
[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-Dermandで使用する

XR\_A(センター1)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

使用するIKEポリシー名の選択	XR_A (IKE1) 💌
本装置側のL4N側のネオワークアドレス	192.168.20.0/24 (例:192.168.00/24)
相手側のLAN側のネットワークアドレス	192.168.10.0/24 (例:192.168.00/24)
FH2のTransFormの選択	aes128-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)
DISTANCE	1 (1~255まで)

XR\_A(センター1)に対して IPsec 通信を行う IP アドレスの範囲を設定します。 この IPsec ポリシーは、192.168.20.0/24 <-> 192.168.10.0/24 の通信に適用されます。

```
[IPsec ポリシーの設定 2]
```

💿 使用する – 使用しない 🦳 Responderとして使用する 🦳 On-Dermandで使用する

XR\_A(センター1)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

使用するIKEポリシー名の選択	XR_A (IKE1) 💌
本装置側のL4M側のネオワークアドレス	192.168.20.0/24 (例:192.168.00/24)
相手側のLAN側のネットワークアドレス	192.168.110.0/24 (例:192.168.00/24)
FH2のTransFormの選択	aes128-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)
DISTANCE	1 (1~255まで)

XR\_A(センター1)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

この IPsec ポリシーは、192.168.20.0/24 <-> 192.168.110.0/24 の通信に適用されます。

[IPsec Keep-Alive 設定]

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option1 <u>米</u>	動作option 2 <u>米</u>	interface	backup SA
1	<b>v</b>	192.168.20.1	192.168.10.254	45	3	60			ipsec0 💌	
2	<b>V</b>	192.168.20.1	192.168.110.1	60	3	60			ipsec0 💌	

XR\_A(センター1)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。 IPsec ポリシー1 の宛先として XR\_A(センター1)で設定している仮想インタフェースの IP アドレスを指 定しています。

【IPsec サーバ】

|--|

IPsec サーバ機能を起動します。

# 4. IPsec での NAT 利用例

通常同一のネットワークアドレスを利用している拠点間では、IPsec による通信はできませんが、IPsec での NAT を利用することにより、同一ネットワークアドレスを利用している拠点間の特定の機器同士で IPsec による通信を利用できます。

## 4-1. 構成例



## 4-2. 要件

- ▶ インタフェースおよび PPP/PPPoE
  - インターネットに PPPoE で接続します。
  - PPPoE 接続は、自動再接続するように設定しています。
  - WAN 側インタフェースの IP マスカレード、ステートフルパケットインスペクションは「有効」にしています。

主なインタフェースおよび PPP/PPPoE のパラメータ

	XR_A(センター)	XR_B(拠点)
LAN 側インタフェース	Ether0	Ether0
LAN 側 IP アドレス	192. 168. 10. 1	192. 168. 10. 2
WAN 側インタフェース	Ether1[ppp0]	Ether1[ppp0]
WAN 側 IP アドレス	10. 10. 10. 1	動的 IP
PPPoE ユーザ名	test1@centurysys	test2@centurysys
PPPoE パスワード	test1pass	test2pass
WAN 側接続回線	PPPoE 接続	PPPoE 接続

≻ IPsec

- 鍵交換モードはアグレッシブモードを使用しています。
- XR\_A(センター)は172.16.10.0/24 <-> 172.16.20.0/24 の時に IPsec を適用します。
- XR\_B(拠点)は172.16.20.0/24 <-> 172.16.10.0/24の時に IPsec を適用します。

本装置側のパラメータ

	XR_A(センター)	XR_B(拠点)
インタフェースの IP アドレス	10. 10. 10. 1	%ppp0
上位ルータの IP アドレス	%ppp0	
インタフェースの ID		@ipsec1

	XR_A(センター)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター)
IKE/ISAKMP ポリシー名	XR_B	XR_A
リモート IP アドレス	0. 0. 0. 0	10. 10. 10. 1
インタフェースの ID	@ipsec1	
モード	Aggressive	Aggressive
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
DH グループ	Group2	Group2
ライフタイム	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey1

IKE/ISAKMP ポリシーのパラメータ「XR\_A(センター), XR\_B(拠点)」

IPsec ポリシーのパラメータ「XR\_A(センター), XR\_B(拠点)」

	XR_A(センター)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター)
使用する IKE ポリシー名	XR_B(IKE1)	XR_A(IKE1)
本装置の LAN 側のネットワークアドレス	172.16.10.0/24	172. 16. 20. 0/24
相手側の LAN 側のネットワークアドレス	172. 16. 20. 0/24	172.16.10.0/24
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
PFS (DH グループ)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)
DISTANCE	1	1

IPsec Keepalive のパラメータ

	XR_B(拠点)
対向拠点	XR_A(センター)
Policy No.	1
source address	172. 16. 20. 1
destination address	172. 16. 10. 1
interval(sec)	45
watch count	3
timeout/delay(sec)	60
動作option	2
interface	ipsec0

≻ NAT

- XR\_A(センター)では IPsec を経由して「172.16.10.1」宛のパケットを受信した場合には宛先を「192.168.10.1」に変換し、「172.16.10.2」宛のパケットを受信した場合には宛先を「192.168.10.100」に変換します。
   また IPsec を経由して送信元「192.168.10.1」のパケットを送信する場合には、送信元を「172.16.10.1」に変換し、送信元「192.168.10.100」のパケットを送信する場合には、送信元を「172.16.10.1」に変換し、送信元「192.168.10.100」のパケットを送信する場合には、送信元を「172.16.10.2」に変換します。
- XR\_B(拠点)では IPsec を経由して「172.16.20.1」宛のパケットを受信した場合には 宛先を「192.168.10.2」に変換し、「172.16.20.2」宛のパケットを受信した場合には 宛先を「192.168.10.200」に変換します。
   また IPsec を経由して送信元「192.168.10.2」のパケットを送信する場合には、送信 元を「172.16.20.1」に変換し、送信元「192.168.10.200」のパケットを送信する場 合には、送信元を「172.16.20.2」に変換します。

	XR_A(センター)		XR_B(拠点)	
サーバのアドレス	192. 168. 10. 1	192. 168. 10. 100	192. 168. 10. 2	192. 168. 10. 200
公開するグローバルアドレス	172. 16. 10. 1	172. 16. 10. 2	172.16.20.1	172.16.20.2
プロトコル	全て	全て	全て	全て
ポート				
インタフェース	ipsec0	ipsec0	ipsec0	ipsec0

バーチャルサーバのパラメータ「XR\_A(センター), XR\_B(拠点)」

IPsec 設定例 IPsec での NAT 利用例

送信元 NAT のパラメータ「XR\_A(センター), XR\_B(拠点)」

	XR_A(センター)		XR_B (	拠点)
送信元のプライベート アドレス	192. 168. 10. 1	192. 168. 10. 100	192. 168. 10. 2	192. 168. 10. 200
変換後のグローバル アドレス	172. 16. 10. 1	172. 16. 10. 2	172. 16. 20. 1	172. 16. 20. 2
インタフェース	ipsec0	ipsec0	ipsec0	ipsec0

#### 4-3. 設定例

センタールータ(XR\_A)

ポイント

XR\_B(拠点)と IPsec で接続するための設定を行います。

IPsec の鍵交換モードはアグレッシブモードを使用します。

IPsec でのNAT を利用するため、バーチャルサーバ,送信元NAT を設定しています。

#### <<インタフェース設定>>

[Ethernet0の設定]

<ul> <li>固定アド</li> </ul>	レスで使用
ℙアドレス	192.168.10.1
ネットマスク	255.255.255.0
мти	1500

Ethernet0 に関する設定をします。

※IPアドレスの設定を変更した場合、その設定した IPアドレスが即反映されます。

[Ethernet1の設定]

<ul> <li>         ・         ・         ・</li></ul>	レスで使用	
IPアドレス	0	
ネットマスク	255.255.255.0	
мти	1500	

Ethernet1 に関する設定をします。

PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

#### <<PPP/PPPoE 設定>>

[接続先設定1]

ユーザロ	test1@centurysys	
パスワード	test1pass	

PPPoE 接続で使用するユーザ ID,パスワードを登録します。

[接続設定]

接続先の選択	●接號先1 ●接読先2 ●接號先3 ●接號先4 ●接読先5
接続ボート	O Ether0 • Ether1 • Ether2 • BRI(64K) • BRI MP(128K) • RS232C
接統形態	○ 手動接続 ○ 常時接続 ○ スケジューラ接続
RS232C/BRI接続タイプ	<ul> <li>● 通常</li> <li>● On-Demand接続</li> </ul>
ドマスカレード	○無効 ● 有効
ステートフルパケット インスペウション	○無効 ○有効 □DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ● 有効

PPPoE 接続するインタフェース、および接続形態を選択します。 ※この例では、ルータ経由でのインターネットアクセスも可能になっています。



PPPoEの再接続性を高めるために、PPPoE 特殊オプションを設定しています。

### <<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ррр0	パケ水受信時	許可 🔽	udp 💌		500		500	
ррр0	パケ水受信時	許可 🔽	esp 💌					

IKE パケット, ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

<<各種サービスの設定>>

<IPsec サーバ>

[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	%ppp0
インターフェー スのЮ	(例:@xr.centurysys)

XR\_A(センター)のWAN側インタフェースのIPアドレス,および上位ルータのIPアドレスを設定します。 PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。

[IKE/ISAKMPの設定1]

IKE/ISAKMPポリシー名	XR_B
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	@ipsec1 (例:@xr.centurysys)
モードの恐安	remain To K w
C T OVARAC	aggressive t - r
C T WARKE	aggressive t - r ♥ 1番目 group2-aes128-sha1 ♥
	ageressive モード V 1番目 group2-aes128-sha1 V 2番目 使用しない V
transformの設定	ageressive モード V 1番目 group2-aes128-sha1 V 2番目 使用しない V 3番目 使用しない V
transformの設定	aeeressive モード V 1番目 group2-aes128-sha1 V 2番目 使用しない V 4番目 使用しない V

XR\_B(拠点)に対する IKE/ISAKMP ポリシーを設定します。

鍵の設定	
<ul> <li>PSKを使用する</li> <li>RSAを使用する</li> <li>(0509を使用する場合は RSAL設定してください)</li> </ul>	ipseckey1

事前共有鍵(PSK)として「ipseckey1」を設定しています。

[IPsec ポリシーの設定 1]

○ 使用する ○ 使用しない ③ Responderとして使用する ○ On-Demandで使用する

XR\_B(拠点)の IP アドレスが不定のため、「Responder として使用する」を選択します。

使用するIKEポリシー名の選択	XR_B (KE1) 💌
本装置側のL4N側のネットワークアドレス	172.16.10.0/24 (第:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	172.16.20.0/24 (朔:192.168.0.0/24)
FH2のTransFormの選択	aes128-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 彩 (1081~86400秒まで)
DISTANCE	1 (1~255まで)

XR\_B(拠点)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。

この例では、本装置側の仮想ネットワーク「172.16.10.0/24」と対向の仮想ネットワーク「172.16.20.0/24」の通信に対して IPsec を適用します。

【IPsec サーバ】



IPsec サーバ機能を起動します。

#### <<NAT 設定>>

[バーチャルサーバ]

サーバのアドレス	公開するグローバルアドレス	プロトコル	ボート	インターフェー ス
192.168.10.1	172.16.10.1	全て 🔽		ipsec0
192.168.10.100	172.16.10.2	全て 🔽		ipsec0

IPsec を経由して「172.16.10.1」宛のパケットを受信した場合には宛先を「192.168.10.1」に変換し、「172.16.10.2」宛のパケットを受信した場合には宛先を「192.168.10.100」に変換します。

[送信元 NAT]

送信元のプライベートアドレス	変換後のグローバルアドレス	インターフェース
192.168.10.1	172.16.10.1	ipsec0
192.168.10.100	172.16.10.2	ipsec0

IPsec を経由して送信元「192.168.10.1」のパケットを送信する場合には、送信元を「172.16.10.1」に 変換し、送信元「192.168.10.100」のパケットを送信する場合には、送信元を「172.16.10.2」に変換し ます。 拠点ルータ(XR\_B)

ポイント

XR\_A(センター)と IPsec で接続するための設定を行います。

IPsec の鍵交換モードはアグレッシブモードを使用します。

IPsec でのNATを利用するため、バーチャルサーバ,送信元NATを設定しています。

#### <<インタフェース設定>>

[Ethernet0の設定]

<ul> <li>固定アド</li> </ul>	レスで使用
IP アドレス	192.168.10.2
ネットマスク	255.255.255.0
мти	1500

Ethernet0 に関する設定をします。

※IPアドレスの設定を変更した場合、その設定した IPアドレスが即反映されます。

[Ethernet1の設定]

<ol> <li>固定アド</li> </ol>	レスで使用
IP アドレス	0
ネットマスク	255.255.255.0
мτυ	1500

Ethernet1 に関する設定をします。

PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

### <<PPP/PPPoE 設定>>

[接続先設定1]

ユーザロ	test2@centurysys	
パスワード	test2pass	

PPPoE 接続で使用するユーザ ID,パスワードを登録します。

[接続設定]

接続先の選択	●接號先1 ●接號先2 ●接號先3 ●接號先4 ●接読先5
接続ポート	O Ether0 • Ether1 • Ether2 • BRI(64K) • BRI MP(128K) • RS232C
接統形態	○ 手動接続 ○ 常時接続 ○ スケジューラ接続
RS232C/BRI接続タイプ	<ul> <li>● 通常</li> <li>○ On-Demand接続</li> </ul>
<b>₽マス</b> カレード	○ 無効 ● 有効
ステートフルパケット インスペウション	○ 無効 ● 有効 □ DROP したパケットのLOGを取得
デフォルトルートの設定	○ 無効 ● 有効

PPPoE 接続するインタフェース、および接続形態を選択します。 ※この例では、ルータ経由でのインターネットアクセスも可能になっています。



PPPoEの再接続性を高めるために、PPPoE 特殊オプションを設定しています。

### <<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ррр0	パケ水受信時	許可 🔽	udp 💌		500		500	
ррр0	パケ水受信時	許可 🔽	esp 💌					

IKE パケット, ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

<<各種サービスの設定>>

<IPsec サーバ>

[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	@ipsec1	(例:@xr.centurysys

WAN 側インタフェースの IP アドレス,および上位ルータの IP アドレスを設定します。

[IKE/ISAKMPの設定1]

IKE/ISAKMPポリシー名	XRA
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 💌
	1╋目 group2-aes128-sha1 💌
かったこの改定	1番目 group2-aes128-sha1 🔽 2番目 使用しない 🔽
transformの設定	1番目 group2-aes128-sha1 マ 2番目 使用しない マ 3番目 使用しない マ
transformの設定	1番目 group2-aes128-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 ♥

XR\_A(センター)に対する ISAKMP ポリシーの設定を行います。

鍵の設定	
<ul> <li>PSKを使用する</li> <li>RSAを使用する</li> <li>0509を使用する場合は</li> <li>RSAに設定してください)</li> </ul>	ipseckey1

事前共有鍵(PSK)として「ipseckey1」を設定します。

[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-Dermandで使用する

XR\_A(センター)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

使用するIKEポリシー名の選択	XR_A (KE1) 💌
本装置側のL4N側のネットワークアドレス	172.16.20.0/24 (第1:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	172.16.10.0/24 (期:192.168.00/24)
FH2のTransFormの選択	aes128-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)
DISTANCE	1 (1~255まで)

XR\_A(センター)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。

この例では、本装置側の仮想ネットワーク「172.16.20.0/24」と対向の仮想ネットワーク「172.16.10.0/24」の通信に対して IPsec を適用します。

[IPsec Keep-Alive 設定]

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option1 <u>米</u>	動作option 2 <u>米</u>	interface	backup SA
1		192.168.10.2	172.16.10.1	45	3	60			ipsec0 💌	

XR\_A(センター)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。 この設定例では、IPsec KeepAlive パケットが送信時に送信元 NAT で変換されるのを利用しているため、 source address が「192.168.10.2」と設定されています。

### 【IPsec サーバ】

<u>Psecty − /í</u> ○停止 ⊙起動

IPsec サーバ機能を起動します。

#### <<NAT 設定>>

[バーチャルサーバ]

サーバのアドレス	公開するグローバルアドレス	プロトコル	ボート	インターフェース
192.168.10.2	172.16.20.1	全て 🔽		ipsec0
192.168.10.200	172.16.20.2	全て 🔽		ipsec0

IPsec を経由して「172.16.20.1」宛のパケットを受信した場合には宛先を「192.168.10.2」に変換し、「172.16.20.2」宛のパケットを受信した場合には宛先を「192.168.10.200」に変換します。

[送信元 NAT]

送信元のプライベートアドレス	変換後のグローバルアドレス	インターフェース	
192.168.10.2	172.16.20.1	ipsec0	
192.168.10.200	172.16.20.2	ipsec0	

IPsec を経由して送信元「192.168.10.2」のパケットを送信する場合には、送信元を「172.16.20.1」に 変換し、送信元「192.168.10.200」のパケットを送信する場合には、送信元を「172.16.20.2」に変換し ます。

## 5. GRE over IPsec 設定例

この例は、GRE over IPsec の設定例です。GRE だけでは通信内容を暗号化できませんでしたが、IPsec を併用することにより暗号化することができます。

なお GRE over IPsec は WAN 側 IP アドレスが固定 IP アドレスの場合のみ利用可能です。

### 5-1. 構成例



## 5-2. 要件

- ▶ インタフェースおよび PPP/PPPoE
  - インターネットに PPPoE で接続します。
  - PPPoE 接続は、自動再接続するように設定しています。
  - WAN 側インタフェースの IP マスカレード、ステートフルパケットインスペクションは「有効」にしています。

主なインタフェースおよび PPP/PPPoE のパラメータ

	XR_A(センター)	XR_B(拠点)
LAN 側インタフェース	Ether0	Ether0
LAN 側 IP アドレス	192.168.10.1	192. 168. 20. 1
WAN 側インタフェース	Ether1[ppp0]	Ether1[ppp0]
WAN 側 IP アドレス	10. 10. 10. 1	10. 10. 20. 1
PPPoE ユーザ名	test1@centurysys	test2@centurysys
PPPoE パスワード	test1pass	test2pass
WAN 側接続回線	PPPoE 接続	PPPoE 接続

≻ IPsec

- 鍵交換モードはメインモードを使用しています。
- XR\_A(センター)は10.10.10.1/32 <-> 10.10.20.1/32 の時に IPsec を適用します。
- XR\_B(拠点)は10.10.20.1/32 <-> 10.10.1/32 の時に IPsec を適用します。
- IPsec KeepAlive は XR\_A(センター), XR\_B(拠点)で動作オプション1で使用しています。

本装置側のパラメータ

	XR_A(センター)	XR_B(拠点)
インタフェースの IP アドレス	10. 10. 10. 1	10. 10. 20. 1
上位ルータの IP アドレス	%ppp0	%ppp0
インタフェースの ID		

	XR_A(センター)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター)
IKE/ISAKMP ポリシー名	XR_B	XR_A
リモート IP アドレス	10. 10. 20. 1	10. 10. 10. 1
インタフェースの ID		
モード	Main	Main
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
DH グループ	Group2	Group2
ライフタイム	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey1

IKE/ISAKMP ポリシーのパラメータ「XR\_A(センター), XR\_B(拠点)」

IPsec ポリシーのパラメータ「XR\_A(センター), XR\_B(拠点)」

	XR_A(センター)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター)
使用する IKE ポリシー名	XR_B(IKE1)	XR_A(IKE1)
本装置の LAN 側のネットワークアドレス	10. 10. 10. 1/32	10. 10. 20. 1/32
相手側の LAN 側のネットワークアドレス	10. 10. 20. 1/32	10. 10. 10. 1/32
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
PFS (DH グループ)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)
DISTANCE	1	1

IPsec Keepalive のパラメータ

	XR_A(センター)	XR_B(拠点 1)
対向拠点	XR_B(拠点 1)	XR_A(センター)
Policy No.	1	1
source address	10. 10. 10. 1	10. 10. 20. 1
destination address	10. 10. 20. 1	10. 10. 10. 1
interval(sec)	30	45
watch count	3	3
timeout/delay(sec)	60	60
動作option	1	1
interface	ipsec0	ipsec0

#### ≻ GRE

- XR\_A(センター)のインタフェースアドレスを「172.16.0.1」と設定しています。
- XR\_B(拠点)のインタフェースアドレスを「172.16.0.2」と設定しています。
- GRE over IPsec を使用するを選択し、IPsec インタフェースを指定します。

主な GRE のパラメータ

	XR_A(センター)	XR_B(拠点)
インタフェースアドレス	172. 16. 0. 1/30	172. 16. 0. 2/30
リモート(宛先)アドレス	10. 10. 20. 1	10. 10. 10. 1
ローカル(送信元)アドレス	10. 10. 10. 1	10. 10. 20. 1
PEER アドレス	172. 16. 0. 2/30	172. 16. 0. 1/30
GREoverIPsec	使用する[ipsec0]	使用する[ipsec0]

### ▶ その他

- XR\_A(センター)では拠点側へのルートをスタティックルートでインタフェース 「gre1」で設定しています。
- XR\_B(拠点)ではセンター側へのルートをスタティックルートでインタフェース 「gre1」で設定しています。

#### 5-3. 設定例

#### センタールータ(XR\_A)

#### ポイント

XR\_B(拠点)と GRE over IPsec で接続するための設定を行います。

IPsec の鍵交換モードはメインモードを使用します。

拠点側への通信が GRE トンネルを通るようにスタティックルートで GRE インタフェースを指定しています。

#### <<インタフェース設定>>

[Ethernet0の設定]

<ol> <li>固定アド</li> </ol>	レスで使用
IP アドレス	192.168.10.1
ネットマスク	255.255.255.0
MTU	1500

Ethernet0 に関する設定をします。

※IPアドレスの設定を変更した場合、その設定した IPアドレスが即反映されます。

[Ethernet1の設定]

<ol> <li>固定アド</li> </ol>	レスで使用
IP アドレス	0
ネットマスク	255.255.255.0
мти	1500

Ethernet1 に関する設定をします。

PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

#### <<PPP/PPPoE 設定>>

[接続先設定1]

ユーザロ	test1@centurysys	
パスワード	test1pass	

PPPoE 接続で使用するユーザ ID, パスワードを登録します。

[接続設定]

接続先の選択	◎接統先1 ◎接統先2 ◎接統先3 ◎接統先4 ◎接統先5
接続ポート	O Ether0 O Ether1 O Ether2 O BRI(64K) O BRI MP(128K) O RS2320
接続形態	○ 手動接続 ● 常時接続 ○ スケジューラ接続
RS232C/BRI接続タイプ	<ul> <li>● 通常</li> <li>○ On-Demand接続</li> </ul>
ドマスカレード	○無効 ⊙ 有効
ステートフルバケット インスペウション	○無効 ○ 有効 □ DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ⊙ 有効

PPPoE 接続するインタフェース、および接続形態を選択します。 ※この例では、ルータ経由でのインターネットアクセスも可能になっています。



PPPoEの再接続性を高めるために、PPPoE 特殊オプションを設定しています。

### <<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ррр0	パケ水受信時	許可 🔽	udp 💌		500		500	
ррр0	パケ水受信時	許可 🔽	esp 💌					

IKE パケット, ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

<<各種サービスの設定>>

<IPsec サーバ>

[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	%ррр0
インターフェー スのID	(例:@xr.centurysys)

XR\_A(センター)のWAN側インタフェースのIPアドレス,および上位ルータのIPアドレスを設定します。 PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。

[IKE/ISAKMPの設定1]

IKE/ISAKMPポリシー名	XR_B
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	10.10.20.1
上位ルータのIPアドレス	
インターフェー スのЮ	(例:@xr.centurysys)
モードの設定	main モード 💌
	1番目 group2-aes128-sha1 💌
	2番目 使用しない 🔽
(ranstormu) ag æ	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)

XR\_B(拠点)に対する IKE/ISAKMP ポリシーを設定します。

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 RSAL設定してください)</li> </ul>	ipseckey1

事前共有鍵(PSK)として「ipseckey1」を設定しています。

[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-Dermandで使用する

XR\_B(拠点)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

使用するIKEポリシー名の選択	XR_B (KE1) 💌
本装置側のL4N側のネオワークアドレス	10.10.10.1/32 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	10.10.20.1/32 (第:192.168.0.0/24)
PH2のTransFormの選択	aes128-sha1 💌
PFS	<ul> <li>● 使用する ○ 使用しない</li> </ul>
DH Groupの選択(PFS使用時に有効)	group2 💌
SADライフタイム	28800 彩 (1081~86400映まで)
DISTANCE	1 0~255まで)

XR\_B(拠点)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。

この例では GRE over IPsec を使用しているため、XR\_A(センター)と XR\_B(拠点)の WAN 側 IP アドレスを それぞれ指定しています。

※ 本装置のLAN 側ネットワークアドレス,および相手のLAN 側ネットワークアドレスの項目に関しては、 この項目に「空欄」を設定した場合、WAN 側 IP アドレスを設定したのと同じ意味になります。

[IPsec Keep-Alive 設定]

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1 <u>米</u>	動作option 2 <u>米</u>	interface	backup SA
1		1010101	1010201	30	3	60			ipsec0 💌	

XR\_B(拠点)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

I <u>Psecサーバ</u>	○停止 ⊙起動
------------------	---------

IPsec サーバ機能を起動します。

<<GRE 設定>>

インタフェー スアド レス	172.16.0.1/30 (例:192.168.0.1/30)
リモート(宛先)アドレス	10.10.20.1 (例:192.168.1.1)
ローカルG差信元)アドレス	10.10.10.1 (例:192.168.2.1)
PEER7F U.A	172.16.0.2/30 (例:192.168.02/30)

XR\_B(拠点)とのGRE トンネルを設定します。

GREover/PSec   ・ 使用する ipsec 0  ・ Routing Tableに依存		
O Routing Table门放存	GREaverIPSec	⊙ 使用する ipsec0
	anzovennseo	〇 Routing Tableに依存

この例では GRE over IPsec を使用しますので、「使用する」を選択し、インタフェースとして「ipsec0」 を設定しています。

#### <<スタティックルート設定>>

アドレス	ネットマスク	インターフェー	- ス/ゲートウェイ	ディスタンス (1-255>
192.168.20.0	255.255.255.0	gre1		1

拠点側への通信が GRE トンネルを通るように GRE インタフェースを指定しています。

拠点ルータ(XR\_B)

ポイント

XR\_A(センター)とGRE over IPsec で接続するための設定を行います。

IPsec の鍵交換モードはメインモードを使用します。

拠点側への通信が GRE トンネルを通るようにスタティックルートで GRE インタフェースを指定しています。

### 〈〈インタフェース設定〉〉

[Ethernet0の設定]

<ul> <li>         ・         ・         ・</li></ul>				
₽₽Fレス	192.168.20.1			
ネットマスク	255.255.255.0			
мти	1500			

Ethernet0 に関する設定をします。

※IPアドレスの設定を変更した場合、その設定した IPアドレスが即反映されます。

[Ethernet1の設定]

<ul> <li>         ・         ・         ・</li></ul>	レスで使用	
IPアドレス	0	
ネットマスク	255.255.255.0	
мти	1500	

Ethernet1 に関する設定をします。

PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

### <<PPP/PPPoE 設定>>

[接続先設定1]

ユーザロ	test2@centurysys	
パスワード	test2pass	

PPPoE 接続で使用するユーザ ID, パスワードを登録します。

[接続設定]

接続先の選択	●接號先1 ●接號先2 ●接號先3 ●接號先4 ●接號先5
接続ボート	O Ether0 • Ether1 • Ether2 • BRI(64K) • BRI MP(128K) • RS232C
接続形態	○ 手動接続 ○ 常時接続 ○ スケジューラ接続
RS232C/BRI接続タイプ	<ul> <li>● 通常</li> <li>● On-Demand接続</li> </ul>
ドマスカレード	○無効 ● 有効
ステートフルパケット インスペウション	○無効 ○有効 □DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ● 有効

PPPoE 接続するインタフェース、および接続形態を選択します。 ※この例では、ルータ経由でのインターネットアクセスも可能になっています。



PPPoEの再接続性を高めるために、PPPoE 特殊オプションを設定しています。

### <<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ррр0	パケ水受信時	許可 🔽	udp 💌		500		500	
ррр0	パケ水受信時	許可 🔽	esp 💌					

IKE パケット, ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

## <<各種サービスの設定>>

#### <IPsec サーバ>

[本装置側の設定 1]

インターフェースのIPアドレス	10.10.20.1
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

WAN 側インタフェースの IP アドレス,および上位ルータの IP アドレスを設定します。

[IKE/ISAKMPの設定1]

IKE/ISAKMPポリシー名	XRA
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	(預:@xr.centurysys)
モードの設定	main モード 💌
	1∰目 group2-aes128-sha1 💌
	1番目 group2-aes128-sha1 💌 2番目 使用しない 💌
transformの設定	1番目 group2-aes128-sha1 V 2番目 使用しない V 3番目 使用しない V
transformの設定	1番目 group2-aes128-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 ♥

XR\_A(センター)に対する ISAKMP ポリシーの設定を行います。

鍵の設定	
<ul> <li>PSKを使用する</li> <li>RSAを使用する</li> <li>(X500を使用する場合は RSAL設定してください)</li> </ul>	ipseckey1

事前共有鍵(PSK)として「ipseckey1」を設定します。

[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-Dermandで使用する

XR\_A(センター)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

使用するIKEポリシー名の選択	XR_A (1KE1) 💌
本装置側のL4N側のネオワークアドレス	10.10.20.1/32 (第:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	10.10.10.1/32 (第:192.168.0.0/24)
FH2のTransFormの選択	aes128-sha1 💌
PFS	<ul> <li>● 使用する</li> <li>● 使用しない</li> </ul>
DH Groupの選択(PFS使用時に有効)	group2 💌
SADライフタイム	28800 彩(1081~86400秒まで)
DISTANCE	1 ()~255まで)

XR\_A(センター)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

この例では GRE over IPsec を使用しているため、XR\_B(拠点)と XR\_A(センター)との WAN 側 IP アドレス をそれぞれ指定しています。

※ 本装置のLAN 側ネットワークアドレス,および相手のLAN 側ネットワークアドレスの項目に関しては、 この項目に「空欄」を設定した場合、WAN 側 IP アドレスを設定したのと同じ意味になります。

[IPsec Keep-Alive 設定]

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1 <u>米</u>	動作option 2 <u>米</u>	interface	backup SA
1		1010201	1010101	45	3	60			ipsec0 💌	

⊙起動

XR\_A(センター)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

Psect-バ O停止

IPsec サーバ機能を起動します。

<<GRE 設定>>

インタフェー スアド レス	172.16.0.2/30 (例:192.168.0.1/30)
リモート(宛先)アドレス	10.10.10.1 (例:192.168.1.1)
ローカルG差信元)アドレス	10.10.20.1 (例:192.168.2.1)
PEER7F U.A	172.16.0.1/30 (例:192.168.02/30)

XR\_A(センター)との GRE トンネルを設定します。

GEGorardBCoo	<ul> <li>● 使用する ipsec0</li> </ul>
anzovennoed	〇 Routing Table口做存

この例では GRE over IPsec を使用しますので、「使用する」を選択し、インタフェースとして「ipsec0」を設定しています。

#### <<スタティックルート設定>>

アドレス	ネットマスク	インターフェー	- ス/ゲートウェイ	ディスタンス (1-255>
192.168.10.0	255.255.255.0	gre1		1

センター側への通信が GRE トンネルを通るように GRE インタフェースを指定しています。

# 6. IPsec NAT-Traversal 設定例 1

この例は、IPsec NAT-Traversal を利用した IPsec 接続の設定例です。拠点側にインターネットアクセ ス用の NAT ルータがあり、その配下に IPsec 接続をするルータや VPN クライアントが存在する構成です。

## 6-1. 構成例



## 6-2. 要件

- ▶ インタフェースおよび PPP/PPPoE
  - インターネットに PPPoE で接続します。
  - PPPoE 接続は、自動再接続するように設定しています。
  - WAN 側インタフェースの IP マスカレード、ステートフルパケットインスペクションは「有効」にしています。
  - XR\_B(拠点 1)はローカルルータの設定をします。

主なインタフェースおよび PPP/PPPoE のパラメータ(1)

	XR_A(センター)	XR_B2(拠点1)	XR_C2(拠点 2)
LAN 側インタフェース	Ether0	Ether0	Ether0
LAN 側 IP アドレス	192. 168. 10. 1	192. 168. 120. 254	192. 168. 130. 254
WAN 側インタフェース	Ether1[ppp0]	Ether1[ppp0]	Ether1[ppp0]
WAN 側 IP アドレス	10. 10. 10. 1	動的 IP	動的 IP
PPPoE ユーザ名	test1@centurysys	test2@centurysys	test3@centurysys
PPPoE パスワード	test1pass	test2pass	test3pass
WAN 側接続回線	PPPoE 接続	PPPoE 接続	PPPoE 接続

主なインタフェースおよび PPP/PPPoE のパラメータ(2)

	XR_B(拠点1)	PC(拠点 2)
LAN 側インタフェース	Ether0	_
LAN 側 IP アドレス	192. 168. 20. 1	-
WAN 側インタフェース	Ether1	_
WAN 側 IP アドレス	192. 168. 120. 1	192. 168. 130. 1
デフォルトゲートウェイ	192. 168. 120. 254	192. 168. 130. 254

#### ≻ IPsec

- 鍵交換モードはアグレッシブモードを使用しています。
- XR\_A(センター)は 192.168.10.0/24 <-> 192.168.20.0/24, 192.168.10.0/24 <-> 192.168.30.1/32の時に IPsec を適用します。
- XR\_B(拠点 1)は 192. 168. 20. 0/24 <-> 192. 168. 10. 0/24 の時に IPsec を適用します。
- PC(拠点 2)は192.168.30.1/32 <-> 192.168.10.0/24の時に IPsec を適用します。
- XR\_A(センター)は、IPsec NAT-TraversalのResponder 側になるため、NAT-TraversalのVirtual Private 設定を行っています。
- XR\_B(拠点 1)は、IPsec NAT-Traversal の Initiator 側になるため、NAT-Traversal を「使用する」を選択し、Virtual Private 設定を行っていません。
- IPsec KeepAlive は XR\_B(拠点)が動作オプション2で使用しています。

	XR_A(センター)	XR_B(拠点 1)
NAT Traversal	使用する	使用する
Virtual Private 設定	192.168.20.0/24	
Virtual Private 設定 2	192. 168. 30. 1/32	
インタフェースの IP アドレス	10. 10. 10. 1	192. 168. 120. 1
上位ルータの IP アドレス	%ppp0	192. 168. 120. 254
インタフェースの ID		@ipsec1

本装置側のパラメータ

	XR_A(センター)		XR_B(拠点 1)
対向拠点	XR_B(拠点 1)	PC(拠点 2)	XR_A(センター)
IKE/ISAKMP ポリシー名	XR_B	PC	XR_A
リモート IP アドレス	0. 0. 0. 0	0. 0. 0. 0	10. 10. 10. 1
インタフェースの ID	@ipsec1	@vpnclient	
モード	Aggressive	Aggressive	Aggressive
暗号化アルゴリズム	AES-128	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1	SHA1
DHグループ	Group2	Group2	Group2
ライフタイム	3600(秒)	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey2	ipseckey1

IKE/ISAKMP ポリシーのパラメータ「XR\_A(センター), XR\_B(拠点1)」

IPsec ポリシーのパラメータ「XR\_A(センター), XR\_B(拠点 1)」

	XR_A(センター)		XR_B(拠点)
対向拠点	XR_B(拠点1)	PC(拠点 2)	XR_A(センター)
使用する IKE ポリシー名	XR_B(IKE1)	PC(IKE2)	XR_A(IKE1)
本装置の LAN 側のネットワークアドレス	192.168.10.0/24	192.168.10.0/24	192.168.20.0/24
相手側の LAN 側のネットワークアドレス	vnet:%priv	vhost:%priv	192.168.10.0/24
暗号化アルゴリズム	AES-128	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1	SHA1
PFS (DH グループ)	使用する(Group2)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)	28800(秒)
DISTANCE	1	1	1

IPsec Keepalive のパラメータ

	XR_B(拠点1)
対向拠点	XR_A(センター)
Policy No.	1
source address	192. 168. 20. 1
destination address	192. 168. 10. 1
interval(sec)	45
watch count	3
timeout/delay(sec)	60
動作option	2
interface	ipsec6

## ▶ その他

● 本設定例では、NAT ルータとして XR を使用しています。
## 6-3. 設定例

### センタールータ (XR\_A)

ポイント

XR\_B(拠点1)とPC(拠点2)とIPsec NAT-Traversal で接続するための設定を行います。

IPsec の鍵交換モードはアグレッシブモードを使用します。

XR\_A(センター)は、IPsec NAT-Traversal の Responder 側になるため、NAT-Traversal の Virtual Private 設定を行っています。

IPsec NAT-Traversal で使用する UDP のポート番号をフィルタで許可しています。

## 〈〈インタフェース設定〉〉

[Ethernet0の設定]

● 固定アドレスで使用		
₽₽Fレス	192.168.10.1	
ネットマスク	255.255.255.0	
мτυ	1500	

Ethernet0 に関する設定をします。

※IPアドレスの設定を変更した場合、その設定した IPアドレスが即反映されます。

[Ethernet1の設定]

<ol> <li>固定アド</li> </ol>		
IP アドレス	0	
ネットマスク	255.255.255.0	
мти	1500	

Ethernet1に関する設定をします。 PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

## <<PPP/PPPoE 設定>>

[接続先設定1]

ユーザロ	test1@centurysys	
パスワード	test1pass	

PPPoE 接続で使用するユーザ ID, パスワードを登録します。

[接続設定]

接続先の選択	●接統先1 ●接統先2 ●接統先3 ●接統先4 ●接統先5
接続ポート	O Ether0 • Ether1 • Ether2 • BRI(64K) • BRI MP(128K) • RS232C
接続形態	○ 手動接続 ○ 常時接続 ○ スケジューラ接続
RS232C/BRI接続タイプ	<ul> <li>● 通常</li> <li>● On-Demand接続</li> </ul>
ドマスカレード	○無効 ● 有効
ステートフルバケット インスペウション	○無効 ○有効 □DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ● 有効

PPPoE 接続するインタフェース、および接続形態を選択します。 ※この例では、ルータ経由でのインターネットアクセスも可能になっています。



PPPoEの再接続性を高めるために、PPPoE 特殊オプションを設定しています。

## <<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ррр0	パケオ受信時	許可 🚩	udp 💌		500		500	
рррО	パケ水受信時	許可 🚩	udp 💌		4500		4500	

IKE パケット, NAT-Traversal 使用時にカプセル化する UDP ポート「4500」のパケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

#### <<各種サービスの設定>>

<IPsec サーバ>

[本装置の設定]

NAT Traversal	<ul> <li>● 使用する</li> <li>● 使用しない</li> </ul>
Virtual Private設定	%v4:192.168.20.0/24
Virtual Private設定2	%v4:192.168.30.1/32

NAT Traversal を利用するため、「使用する」を選択します。

Virtual Private 設定では、NAT-Traversal を使用しているルータ配下の LAN または NAT-Traversal を使用している機器のアドレスを設定します。

この例では、XR\_B(拠点 1)の配下の LAN「192.168.20.0/24」と NAT-Traversal を使用している機器「PC(拠 点 2)」のアドレスを設定しています。

[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	%ppp0
インターフェー スのID	(例:@vacenturysys)

XR\_A(センター)のWAN側インタフェースのIPアドレス,および上位ルータのIPアドレスを設定します。 PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。 [IKE/ISAKMPの設定1]

IKE/ISAKMPポリシー名	XR_B
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	@ipsec1 (例:@xr.centurysys)
モードの設定	aggressive モード 💌
モードの設定	aggressive モード 💌 1番目 group2-aes128-sha1 💌
モードの設定	aggressive モード 💌 1番目 group2-aes128-sha1 💌 2番目 使用しない
モードの設定 transformの設定	aggressive モード 💌 1番目 group2-aes128-sha1 💌 2番目 使用しない 🔍 3番目 使用しない
モードの設定 transformの設定	aggressive モード 💌 1番目 group2-aes128-sha1 💌 2番目 使用しない 🔍 3番目 使用しない 🔍

XR\_B(拠点1)に対する IKE/ISAKMP ポリシーを設定します。

鍵の設定	
<ul> <li>PSKを使用する</li> <li>RSAを使用する</li> <li>(X500を使用する場合は</li> <li>RSAに設定してください)</li> </ul>	ipseckey1

事前共有鍵(PSK)として「ipseckey1」を設定しています。

[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-Dermandで使用する

XR\_B(拠点1)の IP アドレスが不定のため、「Responder として使用する」を選択します。

使用するIKEポリシー名の選択	XR_B (IKE1) 💌
本装置側のLAN側のネットワークアドレス	192.168.10.0/24 (約:192.168.00/24)
相手側のLAN側のネットワークアドレス	vnet:%priv (例:192.168.0.0/24)
FH2のTransFormの選択	aes128-sha1 💌
PFS	<ul> <li>● 使用する</li> <li>● 使用しない</li> </ul>
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)
DISTANCE	1 (1~255まで)

XR\_B(拠点 1)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。

NAT-Traversalを使用しているルータ配下のLANを指定する場合は「vnet:%priv」を指定します。

[IKE/ISAKMPの設定2]

IKE/ISAKMPポリシー名	PC
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	@vpnclient (例:@xr.centurysys)
モードの設定	aggressive モード 💌
	1∰目 group2-aes128-sha1 💌
	2番目 使用しない 🗸
Autor Autor の別庁	
transformの設定	3番目 使用しない ▼
transformの設定	3番目 使用しない マ 4番目 使用しない マ

PC(拠点2)に対する IKE/ISAKMP ポリシーを設定します。

鍵の設定	
<ul> <li>PSKを使用する</li> <li>RSAを使用する</li> <li>(X500を使用する場合は</li> <li>RSAに設定してください)</li> </ul>	ipseckey2

事前共有鍵(PSK)として「ipseckey2」を設定しています。

[IPsec ポリシーの設定 2]

🔾 使用する 🔷 使用しない 💿 Responderとして使用する 🔷 On-Demandで使用する

PC(拠点 2)の IP アドレスが不定のため、「Responder として使用する」を選択します。

使用するIKEポリシー名の選択	PC (IKE2)
本装置側のL4N側のネットワークアドレス	192.168.10.0/24 (卿:192.168.00/24)
相手側のLAN側のネットワークアドレス	vhost:%priv (19):192.168.0.0/24)
FH2のTransFormの選択	aes128-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)
DISTANCE	1 (1~255まで)

PC(拠点 2)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。 NAT-Traversal を使用している機器を指定する場合は「vhost:%priv」を指定します。

## 【IPsec サーバ】

<u>IPsecサーバ</u>

○停止 ⊙起動

IPsec サーバ機能を起動します。

### 拠点1ルータ(XR\_B)

ポイント

XR\_A(センター)と IPsec NAT-Traversal で接続するための設定を行います。

IPsec の鍵交換モードはアグレッシブモードを使用します。

XR\_B(拠点 1)は、IPsec NAT-Traversal の Initiator 側になるため、NAT-Traversal を「使用する」を選 択し、Virtual Private 設定を行っていません。

IPsec NAT-Traversal で使用する UDP のポート番号をフィルタで許可しています。

## 〈〈インタフェース設定〉〉

[Ethernet0の設定]

<ol> <li>固定アド</li> </ol>	レスで使用	
ℙアドレス	192.168.20.1	
ネットマスク	255.255.255.0	
мти	1500	

Ethernet0 に関する設定をします。

※IPアドレスの設定を変更した場合、その設定した IPアドレスが即反映されます。

[Ethernet1の設定]

<ul> <li>固定アド</li> </ul>	レスで使用
₽₽Fレス	192.168.120.1
ネットマスク	255.255.255.0
MTU	1500

Ethernet1の IP アドレスの設定をします。



この例では、NAT Traversal を使用するルータの WAN 側では IP マスカレードおよびステートフルパケットインスペクション(spi)は使用していません。

[その他の設定]

デフォルトゲートウェイの設定	
192.168.120.254	

XR\_Bの上位ルータである XR\_B2 をデフォルトゲートウェイとして指定しています。

## <<各種サービスの設定>>

<IPsec サーバ>

[本装置の設定]

NAT Traversal

💿 使用する 🔘 使用しない

NAT Traversal を利用するため、「使用する」を選択します。

[本装置側の設定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	192.168.120.254	
インターフェー スのID	@ipsec1	(例:@xr.centurysys)

WAN 側インタフェースの IP アドレス,および上位ルータの IP アドレスを設定します。 XR\_B は NAT ルータ配下にあるため、「インタフェースの ID」を設定しています。

[IKE/ISAKMPの設定1]

IKE/ISAKMPポリシー名	XR_A
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Ю	(例:@xr.centurysys)
モードの設定	aggressive モード 💌
	1╋目 group2-aes128-sha1 🔽
	2番目 使用しない 🔽
(ransionno)ague	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)

XR\_A(センター)に対する ISAKMP ポリシーの設定を行います。

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>	ipseckey1

事前共有鍵(PSK)として「ipseckey1」を設定します。

[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
-------------------------------------	------------------

XR\_A(センター)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

使用するIKEポリシー名の選択	XR_A ((KE1) 💌
本装置側のL4N側のネオワークアドレス	192.168.20.0/24 (9):192.168.00/24)
相手側のLAN側のネットワークアドレス	192.168.10.0/24 (約:192.168.00/24)
PH2のTransFormの選択	aes128-sha1 💌
PFS	<ul> <li>● 使用する</li> <li>● 使用しない</li> </ul>
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)
DISTANCE	1 (1~255まで)

XR\_A(センター)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

#### [IPsec Keep-Alive 設定]

enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1 <u>米</u>	動作option 2 <u>米</u>	interface	backup SA
	192.168.20.1	192.168.10.1	45	3	60			ipsecő 💌	

XR\_A(センター)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

IPsecサーバ	○停止	⊙起動	
----------	-----	-----	--

IPsec サーバ機能を起動します。

## 拠点2PC(PC)

## ポイント

拠点2は「FutureNet VPN Client/NET-G」をインストールした PC からの IPsec NAT Traversal 接続にな ります。

<<既知共有鍵(Pre shared Key)の設定>>

■ 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	? X
<ul> <li>● ② 信頼されたポリシー サーバ</li> <li>● ④ 信頼された証明書</li> <li>● ▲ 認証局</li> <li>● ④ ワモート ホスト</li> <li>● ● ディレクトリ サービス</li> <li>● ● ● ライルクタ現</li> <li>● ● ● ラの現</li> <li>● ● ● ○ ホスト キー</li> <li>● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●</li></ul>	
<u> </u>	
OK キャンセル 適用	

「鍵管理」タブをクリックし、「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ので、「既知共有鍵を作成する」を選択し、「次へ」ボタンをク リックして下さい。

既知共有鍵		X
<b>既知共有鍵の作成</b> 共有シークレットを入力してくださ	(v.	
既知共有鍵に自分だけが参照 回入力します。フィンガープリン! 確認します。 ┌既知共有鍵	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 を使用して、実際にシークレットを表示せずに通信相手とシークレットを	
名前:	新しい既知共有鏈	
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):	e3c4 c285	
	(戻る(日) 完了 キャンセル	

「既知共有鍵の作成」画面が開きます。ここで既知共有鍵を作成します。「名前」には任意の設定名を入 カします。「共有シークレット」「共有シークレットの確認」項目には既知共有鍵を入力し、「完了」ボタ ンをクリックします。

この例では共有シークレットとして「ipseckey2」を設定しています。



「鍵管理」画面に戻ります。既知共有鍵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 リックして下さい。「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。

#### <<ID の設定>>

既知共有鍵	<u>?</u> ×
プロパティ ID	
びたいます。 既知共有鍵認証は て行われます。	、当事者のみが知る共有シークレットに基づい
既知共有鍵情報 -	
名前:	新しい既知共有鍵
鍵 ID:	vpnclient
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	
e3c4 c285	
警告     一般的な語句は辞     一般のな語句は辞     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 月しないでください。
	OK キャンセル

「鍵管理」画面で、登録した既知共有鍵を選択して「プロパティ」をクリックします。「既知共有鍵」画面が開きますので、「ID」タブをクリックします(この画面では既知共有鍵を変更できます)。

既知共有鏈 · · · · · · · · · · · · · · · · · · ·
プロパティ ID
通常は、ID を指定する必要はありません。ただし、IKE アグレッシブ モードでは、両方の ID を指定する必要があります。
ブライマリ ID: 10: 10: 10: 10: 10: 10: 10: 10: 10: 10
ホストドメイン名: vpnclient
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。
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 サーバ「IKE/ISAKMP の設定」における「インタフェー ス ID」と同じ ID を設定します。

※ただしこの時、ホストドメイン名には"@"をつけないで設定して下さい。

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
[週加位)     前除(B) ブロパティ(D)     表示(M)     ま示(M)     しーカル ホストの認証に使用される鍵です。
OK 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下さい。「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。

### <<セキュリティポリシーの設定>>

■ NET-G Secure VPN Client ポリシー エディタ	<u>?</u> ×
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 ●
<u>追加(A)</u> 肖耶余(B) フロパティ(P) 説明 ローカル ホストがセキュリティ ゲートウェイ経由でリモート ブ ークへの IPSec 接続を確立するときに、仮想プライベート されます。	診断(D)… ライベート ネットワ ネットワークが作成
OK キャンセル	道用

ポリシーエディタの「セキュリティポリシー」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	<u>? ×</u>
	ゲートウェイ IP アドレス:	10.10.10.1
- <b>1</b>	リモート ネットワーク:	any 💌
	認証鍵:	🖙 新しい既知共有鍵
		□ レガシ候補を使用する(山)
13断	( <u>D)</u> 7 <u>0777(P)</u>	OK ++>>セル

「VPN 接続を追加」画面が開きます。「ゲートウェイ IP アドレス」で右端の"IP"をクリックし、XR\_A(センター)の WAN 側 IP アドレスを設定します。

「認証鍵」は、既知共有鍵の設定で登録した既知共有鍵の設定名を選択します。

「リモートネットワーク」については右端にある"・・・"をクリックして下さい。

ネットワーク エディタ			? ×
ネットワーク イレー語 名前を後で 「定義されたネットワーク	およびサブネットワ・ 『使用して規則を作 フ	ークに独自の名前を 乍成できます。	付けます。この
名前	IP アドレス	サブネット マスク	
any any6 LAN_A	0.0.0 0:0 192.168.10.0	0.0.0.0 0::0 255.255.255.0	
		新規(N)	肖·耶余( <u>R</u> )
ネットワーク名:	LAN_A		
IP アドレス:	192.168.10.0		<b>%</b>
サブネット マスク:	255.255.255.0		
	[	OK	キャンセル

「ネットワークエディタ」画面が開きます。

「ネットワーク名」は任意の名前を設定することができます。

「IP アドレス」「サブネットマスク」は XR に接続している LAN について設定し (ここでは LAN\_A[センタ 一側のネットワーク]の値を設定しています)、「OK」をクリックします。

VPN 接続	を追加		? ×
	ゲートウェイ IP アドレス:	10.10.10.1	IP
•P 📋	リモート ネットワーク:	LAN_A	<b>•</b>
	認証鍵	🐖 新しい既知共有鍵	•
		□ レガシ候補を倒	使用する( <u>U</u> )
診断	i( <u>D</u> ) プロパティ( <u>P</u> )	. <u>OK</u>	キャンセル

リモートネットワーク設定後、「VPN 接続を追加」画面が開きますので、続いてプロパティをクリックします。

規則のプロバ	<b>ティ</b>		? ×
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	IP
Simula	リモート ネットワーク:	LAN_A	<b>•</b>
IPSec /	IKE 候補		
P 😵	認証鍵:	🚧 新しい既知共有	ī键  _
v	候補テンプレート:	normal	•
			設定
□ 仮想	見IP アドレスを取得する		
-₩₫	です。	ドットワークのアトレス	
□ 拡張			
	VPN ケートワェイ Cは、IKE または CHAP 認証が必要 す。	XAuth、RADIUS、 となる場合がありま	
- 言兌8月 -			
			<u></u>
	<u></u>	OK	 

「規則のプロパティ」画面が開きます。ここで 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		? ×
🥸 IKE 候補と IPSec	候補の各パラメータ値を設定します。	
∛ ┌IKE 候補		
暗号化アルゴリズム:	AES-128	•
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:	AES-128	-
整合性関数	HMAC-SHA-1	•
IPSec モード	tunnel	~
PFS グループ:	MODP 1024 (group 2)	•
▶ 選択した値のみを候補にた	023	
	OK ++	ンセル

「パラメータ候補画面」が開きます。ここで暗号化方式などを設定します。IKE モードは「aggressive mode」を設定します。また「選択した値のみを候補に加える」にチェックをいれます。

規則のプロパ	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:	10.10.10.1	IP
inner	リモート ネットワーク:	LAN_A	<b>_</b>
IPSec /	IKE 候補		
	認証鍵:	🦗 新しい既知共有	键 ▼
v	候補テンプレート	normal	•
			設定
☑ 仮想	見IP アドレスを取得する		
4	仮想 IP アドレスは、内部ネ です。	ミットワークのアドレス	設定
□ 拡張			
<b>S</b>	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	
			変更( <u>C</u> )
		C OK	キャンセル

「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、「設定」ボタンをクリックします。

仮想 IP アドレス	? :	×
● 仮想 IP アドレス ● 行います。	れに割り当てるプロトコルを選択するか、手動で設定を	
プロトコル		
○ IPSec 栓田切 DHCH	Oynamic Host Configuration Protocol)	
C L2TP (Layer Two T	unneling Protocol)	
○ IKE 設定モード		
┌● 手動で指定:		
IP アドレス:	192.168.30.1	
サブネット マスク:	255.255.255.0	
ーロ DNS サーバと WINS	サーバを指定する:	
DNS サーバ		
WINS サーバ		
	OK キャンセル	

「仮想 IP アドレス」画面が開きます。

ここでは XR に接続する際に使用するこの PC の仮想的な IP アドレスを設定します。

この例では「192.168.30.1」としています。

「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\_A(センター)の IPsec サーバにおける「IPsec ポリシーの設定 2」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。この例では、サブネットマスクは 24 ビット マスクとしています。(32 ビットマスクは設定することができません。) 仮想 IP アドレス設定後、「規則のプロパティ」画面を開き、「詳細タブ」をクリックします。ここで詳細 オプションにある「NAT 装置を経由する」のチェックボックスを有効にし、「NAT-T(Network Address Translation Traversal)」を選択します。



これで設定は完了です。

続いて IPsec 接続を行います。



タスクトレーの中にある FutureNet Net-G VPNclient のアイコンを右クリックします。そして「VPN を 選択」の指定し、作成した IPsec ポリシーを選択します。



選択後、IKE のネゴシエーションを行う画面が表示されます。



IPsec が正常に確立した場合、「VPN 接続は正常に確立しました」という画面が表示されます。

これで IPsec 接続は完了です。

## NAT ルータ

### ポイント

この設定例では、NAT ルータの設定例は記載していません。

NAT ルータの主な必要な要件は以下のとおりです。

- ・インターネット接続ができていること
- ・IP マスカレードが有効になっていること
- ・フィルタ設定で IPsec NAT-Traversal で使用する UDP ポートが許可されていること

# 7. IPsec NAT-Traversal 設定例 2

この例は、IPsec NAT-Traversal を利用した IPsec 接続の設定例です。拠点側にインターネットアクセ ス用のNATルータがあり、その配下に IPsec 接続をする XR やVPN クライアントが複数存在する構成です。

# 7-1. 構成例



## 7-2. 要件

- ▶ インタフェースおよび PPP/PPPoE
  - インターネットに PPPoE で接続します。
  - PPPoE 接続は、自動再接続するように設定しています。
  - WAN 側インタフェースの IP マスカレード、ステートフルパケットインスペクションは「有効」にしています。
  - XR\_B(拠点)はローカルルータの設定をします。

主なインタフェースおよび PPP/PPPoE のパラメータ(1)

	XR_A(センター)	XR_B2(拠点)
LAN 側インタフェース	Ether0	Ether0
LAN 側 IP アドレス	192.168.10.1	192. 168. 120. 254
WAN 側インタフェース	Ether1[ppp0]	Ether1[ppp0]
WAN 側 IP アドレス	10. 10. 10. 1	動的 IP
PPPoE ユーザ名	test1@centurysys	test2@centurysys
PPPoE パスワード	test1pass	test2pass
WAN 側接続回線	PPPoE 接続	PPPoE 接続

主なインタフェースおよび PPP/PPPoE のパラメータ(2)

	XR_B(拠点)	PC(拠点)
LAN 側インタフェース	Ether0	_
LAN 側 IP アドレス	192.168.20.1	-
WAN 側インタフェース	Ether1	_
WAN 側 IP アドレス	192. 168. 120. 1	192. 168. 120. 10
デフォルトゲートウェイ	192. 168. 120. 254	192. 168. 120. 254

#### ▶ IPsec

- 鍵交換モードはアグレッシブモードを使用しています。
- XR\_A(センター)は 192.168.10.0/24 <-> 192.168.20.0/24, 192.168.10.0/24 <-> 192.168.120.10/32の時に IPsec を適用します。
- XR\_B(拠点)は192.168.20.0/24 <-> 192.168.10.0/24 の時に IPsec を適用します。
- PC(拠点)は192.168.120.10/32 <-> 192.168.10.0/24の時に IPsec を適用します。
- XR\_A(センター)は、IPsec NAT-TraversalのResponder 側になるため、NAT-TraversalのVirtual Private 設定を行っています。
- XR\_B(拠点)は、IPsec NAT-Traversal の Initiator 側になるため、NAT-Traversal を 「使用する」を選択し、Virtual Private 設定を行っていません。
- IPsec KeepAlive は XR\_B(拠点)が動作オプション2で使用しています。

本装置側のパラン	ベータ
----------	-----

	XR_A(センター)	XR_B(拠点)
NAT Traversal	使用する	使用する
Virtual Private 設定	192.168.20.0/24	
Virtual Private 設定 2	192. 168. 120. 10/32	
インタフェースの IP アドレス	10. 10. 10. 1	192. 168. 120. 1
上位ルータの IP アドレス	%ppp0	192. 168. 120. 254
インタフェースの ID		@ipsec1

	XR_A(セ	XR_B(拠点)	
対向拠点	XR_B(拠点)	PC(拠点)	XR_A(センター)
IKE/ISAKMP ポリシー名	XR_B	PC	XR_A
リモート IP アドレス	0. 0. 0. 0	0. 0. 0. 0	10. 10. 10. 1
インタフェースの ID	@ipsec1	@vpnclient	
モード	Aggressive	Aggressive	Aggressive
暗号化アルゴリズム	ゴリズム AES-128 AES-128		AES-128
認証アルゴリズム	認証アルゴリズム SHA1 SHA1		SHA1
DHグループ	Group2	Group2	Group2
ライフタイム	3600(秒)	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey2	ipseckey1

IKE/ISAKMP ポリシーのパラメータ「XR\_A(センター), XR\_B(拠点)」

IPsec ポリシーのパラメータ「XR\_A(センター), XR\_B(拠点)」

	XR_A(セ	XR_B(拠点)		
対向拠点	XR_B(拠点)	PC(拠点)	XR_A(センター)	
使用する IKE ポリシー名	XR_B(IKE1)	PC(IKE2)	XR_A(IKE1)	
本装置の LAN 側のネットワークアドレス	192. 168. 10. 0/24	192.168.10.0/24	192. 168. 20. 0/24	
相手側の LAN 側のネットワークアドレス	vnet:%priv vhost:%priv		192.168.10.0/24	
暗号化アルゴリズム	AES-128	AES-128	AES-128	
認証アルゴリズム	SHA1	SHA1	SHA1	
PFS (DH グループ)	使用する(Group2)	使用する(Group2)	使用する(Group2)	
ライフタイム	28800(秒)	28800(秒)	28800(秒)	
DISTANCE	1	1	1	

IPsec Keepalive のパラメータ

	XR_B(拠点)
対向拠点	XR_A(センター)
Policy No.	1
source address	192. 168. 20. 1
destination address	192.168.10.1
interval(sec)	30
watch count	3
timeout/delay(sec)	60
動作option	2
interface	ipsec6

## ▶ その他

● 本設定例では、NAT ルータとして XR を使用しています。

## 7-3. 設定例

### センタールータ(XR\_A)

ポイント

XR\_B(拠点), PC(拠点)と IPsec NAT-Traversal で接続するための設定を行います。

IPsec の鍵交換モードはアグレッシブモードを使用します。

XR\_A(センター)は、IPsec NAT-Traversal の Responder 側になるため、NAT-Traversal の Virtual Private 設定を行っています。

IPsec NAT-Traversal で使用する UDP のポート番号宛先 500 番, 4500 番をフィルタで許可しています。

## 〈〈インタフェース設定〉〉

[Ethernet0の設定]

<ol> <li>固定アド</li> </ol>	レスで使用	
₽₽Fレス	192.168.10.1	
ネットマスク	255.255.255.0	
мτυ	1500	

Ethernet0 に関する設定をします。

※IPアドレスの設定を変更した場合、その設定した IPアドレスが即反映されます。

[Ethernet1の設定]

⊙ 固定アド	レスで使用	
ℙアドレス	0	
ネットマスク	255.255.255.0	
мти	1500	

Ethernet1に関する設定をします。 PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

## <<PPP/PPPoE 設定>>

[接続先設定1]

ユーザロ	test1@centurysys	
パスワード	test1pass	

PPPoE 接続で使用するユーザ ID, パスワードを登録します。

[接続設定]

接続先の選択	●接統先1 ●接統先2 ●接統先3 ●接統先4 ●接統先5
接続ポート	O Ether0 • Ether1 • Ether2 • BRI(64K) • BRI MP(128K) • RS232C
接続形態	○ 手動接続 ○ 常時接続 ○ スケジューラ接続
RS232C/BRI接続タイプ	<ul> <li>● 通常</li> <li>● On-Demand接続</li> </ul>
ドマスカレード	○無効 ● 有効
ステートフルバケット インスペウション	○無効 ○有効 □DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ● 有効

PPPoE 接続するインタフェース、および接続形態を選択します。 ※この例では、ルータ経由でのインターネットアクセスも可能になっています。



PPPoEの再接続性を高めるために、PPPoE 特殊オプションを設定しています。

## <<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ррр0	パケ水受信時	許可 🔽	udp 💌				500	
ррр0	パケ水受信時	許可 🔽	udp 💌				4500	

IKE パケット, NAT-Traversal 使用時にカプセル化する UDP ポート「4500」のパケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

この時拠点からの IKE パケットや NAT-Traversal でカプセル化されたパケットは、NAT ルータでポート 変換されることを考慮し、送信元ポートを「空欄」に設定しています。

### <<各種サービスの設定>>

### <IPsec サーバ>

[本装置の設定]

NAT Traversal	⊙ 使用する ○ 使用しない
Virtual Private設定	%v4:192.168.20.0/24
Virtual Private設定2	%v4:192.168.120.10/32

NAT Traversal を利用するため、「使用する」を選択します。

Virtual Private 設定では、NAT-Traversal を使用しているルータ配下の LAN または NAT-Traversal を使 用している機器のアドレスを設定します。

この例では、XR\_B2(拠点)の配下のルータ XR\_B の LAN 側「192.168.20.0/24」および VPN Client の IP アドレスを設定しています。

[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	%ррр0
インターフェー スのロ	(例:@xr.centurysys)

XR\_A(センター)のWAN 側インタフェースの IP アドレス,および上位ルータの IP アドレスを設定します。 PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。 [IKE/ISAKMPの設定1]

IKE/ISAKMPポリシー名	XR_B
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	@ipsec1 (例:@xr.centurysys)
モードの設定	aggressive モード 💌
モードの設定	aggressive モード 💌 1番目 group2-aes128-sha1 💌
モードの設定	aggressive モード 💌 1番目 group2-aes128-sha1 💌 2番目 使用しない
モードの設定 transformの設定	aggressive モード マ 1番目 group2-aes128-sha1 マ 2番目 使用しない マ 3番目 使用しない マ
モードの設定 transformの設定	aggressive モード 💌 1番目 group2-aes128-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 🔍

XR\_B(拠点)に対する IKE/ISAKMP ポリシーを設定します。

鍵の設定	
<ul> <li>PSKを使用する</li> <li>RSAを使用する</li> <li>V509を使用する場合は</li> <li>RSAに設定してください)</li> </ul>	ipseckey1

事前共有鍵(PSK)として「ipseckey1」を設定しています。

[IPsec ポリシーの設定 1]

○ 使用する ○ 使用しない ③ Responderとして使用する ○ On-Demandで使用する

XR\_B(拠点)の IP アドレスが不定のため、「Responder として使用する」を選択します。

使用するIKEポリシー名の選択	XR_B (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	vnet:%priv (例:192.168.0.0/24)
FH2のTransFormの選択	aes128-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)
DISTANCE	1 (1~255まで)

XR\_B(拠点)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。

NAT-Traversal を使用しているルータ配下のネットワークを指定する場合は「vnet:%priv」を指定します。

[IKE/ISAKMPの設定2]

IKE/ISAKMPポリシー名	PC
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Ю	@vpnclient (例:@xr.centurysys)
モードの設定	aggressive モード 🔽
	1番目 group2-aes128-sha1 💌
h	1番目 group2-aes128-sha1 マ 2番目 使用しない
transformの設定	1番目 group2-aes128-sha1 マ 2番目 使用しない マ 3番目 使用しない マ
transformの設定	1番目 group2-aes128-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 ♥

PC(拠点)に対する IKE/ISAKMP ポリシーを設定します。

鍵の設定	
<ul> <li>PSKを使用する</li> <li>RSAを使用する</li> <li>0x500を使用する場合は</li> <li>RSAに設定してください)</li> </ul>	ipseckey2

事前共有鍵(PSK)として「ipseckey2」を設定しています。

[IPsec ポリシーの設定 2]

🔿 使用する 🔿 使用しない 💿 Responderとして使用する 🔿 On-Dermandで使用する

PC(拠点)の IP アドレスが不定のため、「Responder として使用する」を選択します。

使用するIKEポリシー名の選択	PC (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	aes128-sha1 💌
PFS	<ul> <li>● 使用する</li> <li>● 使用しない</li> </ul>
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)
DISTANCE	1 ()~255まで)

PC(拠点)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。 NAT-Traversal を使用している機器を指定する場合は「vhost:%priv」を指定します。

【IPsec サーバ】

<u>IPsecサーバ</u>

○停止 ⊙起動

IPsec サーバ機能を起動します。

```
拠点ルータ(XR_B)
```

ポイント

XR\_A(センター)と IPsec NAT-Traversal で接続するための設定を行います。

IPsec の鍵交換モードはアグレッシブモードを使用します。

XR\_B(拠点)は、IPsec NAT-Traversal の Initiator 側になるため、NAT-Traversal を「使用する」を選択 し、Virtual Private 設定を行っていません。

## 〈〈インタフェース設定〉〉

[Ethernet0の設定]

<ul> <li>固定アド</li> </ul>	レスで使用
₽₽Fレス	192.168.20.1
ネットマスク	255.255.255.0
мти	1500

Ethernet0 に関する設定をします。

※IPアドレスの設定を変更した場合、その設定した IPアドレスが即反映されます。

[Ethernet1の設定]

<ol> <li>固定アド</li> </ol>	シンプロション
ℙアドレス	192.168.120.1
ネットマスク	255.255.255.0
мти	1500

Ethernet1の IP アドレスの設定をします。



この例では、NAT Traversal を使用するルータの WAN 側では IP マスカレードおよびステートフルパケットインスペクション(spi)は使用していません。

[その他の設定]



XR\_Bの上位ルータである XR\_B2 をデフォルトゲートウェイとして指定しています。

## <<各種サービスの設定>>

<IPsec サーバ>

[本装置の設定]

NAT Traversal

💿 使用する 🔘 使用しない

NAT Traversal を利用するため、「使用する」を選択します。

[本装置側の設定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	192.168.120.254	
インターフェー スのID	@ipsec1	(例:@xr.centurysys)

WAN 側インタフェースの IP アドレス,および上位ルータの IP アドレスを設定します。 XR\_B は NAT ルータ配下にあるため、「インタフェースの ID」を設定しています。

[IKE/ISAKMPの設定1]

IKE/ISAKMPポリシー名	XR_A
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Ю	(例:@xr.centurysys)
モードの設定	aggressive モード 💌
	1╋目 group2-aes128-sha1 🔽
transformの設定	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)

XR\_A(センター)に対する ISAKMP ポリシーの設定を行います。

鍵の設定	
<ul> <li>PSKを使用する</li> <li>RSAを使用する</li> <li>(509を使用する場合は RSAに設定してください)</li> </ul>	ipseckey1

事前共有鍵(PSK)として「ipseckey1」を設定します。

[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
-----------------------------------	------------------

XR\_A(センター)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

使用するIKEポリシー名の選択	XR_A ((KE1) 💌
本装置側のL4N側のネットワークアドレス	192.168.20.0/24 (期:192.168.00/24)
相手側のLAN側のネットワークアドレス	192.168.10.0/24 (期:192.168.00/24)
PH2のTransFormの選択	aes128-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)
DISTANCE	1 (1~255まで)

XR\_A(センター)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

#### [IPsec Keep-Alive 設定]

enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1 <u>米</u>	動作option 2 <u>米</u>	interface	backup SA
	192.168.20.1	192.168.10.1	30	3	60		<ul><li>✓</li></ul>	ipsecő 💌	

XR\_A(センター)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

IPsecサーバ	○停止	⊙起動	
----------	-----	-----	--

IPsec サーバ機能を起動します。

## PC(拠点)

### ポイント

PC(拠点)は「FutureNet VPN Client/NET-G」をインストールした PC からの IPsec NAT-Traversal 接続に なります。

### <<既知共有鍵(Pre shared Key)の設定>>

INET-G Secure VPN Client ポリシー エディタ
セキュリティ ポリシー   鏈管理
<u> 遠加の(D)</u> 前時(E) プロパティ(D) 表示(D) 表示(D) 新しい認証鍵を追加します。
OK キャンセル 適用

「鍵管理」タブをクリックし、「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ので、「既知共有鍵を作成する」を選択し、「次へ」ボタンをク リックして下さい。
既知共有鍵		X
<b>既知共有鍵の作成</b> 共有シークレットを入力してくださ	(v.	
既知共有鍵に自分だけが参照 回入力します。フィンガープリン! 確認します。 ┌既知共有鍵	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 を使用して、実際にシークレットを表示せずに通信相手とシークレットを	
名前:	新しい既知共有鏈	
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):	e3c4 c285	
	(戻る(日) 完了 キャンセル	

「既知共有鍵の作成」画面が開きます。ここで既知共有鍵を作成します。「名前」には任意の設定名を入 カします。「共有シークレット」「共有シークレットの確認」項目には既知共有鍵を入力し、「完了」ボタ ンをクリックします。

この例では共有シークレットとして「ipseckey2」を設定しています。



「鍵管理」画面に戻ります。既知共有鍵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 リックして下さい。「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。

#### <<ID の設定>>

既知共有鍵	<u>?</u> ×
プロパティ ID	
びたいます。 既知共有鍵認証は て行われます。	、当事者のみが知る共有シークレットに基づい
既知共有鍵情報 -	
名前:	新しい既知共有鍵
鍵 ID:	vpnclient
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	
e3c4 c285	
警告     一般的な語句は辞     一般のな語句は辞     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 月しないでください。
	OK キャンセル

「鍵管理」画面で、登録した既知共有鍵を選択して「プロパティ」をクリックします。「既知共有鍵」画面が開きますので、「ID」タブをクリックします(この画面では既知共有鍵を変更できます)。

既知共有鍵
(לפולד) ID
通常は、ID を指定する必要はありません。ただし、IKE アグレッシブ モードでは、両方の ID を指定する必要があります。
<b>ローカル</b>
プライマリ ID: 📃 ホスト ドメイン名 💌
ホストドメイン名: vpnclient
_ IJ£~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。
<u> </u>

「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 サーバ「IKE/ISAKMP の設定」における「インタフェー ス ID」と同じ ID を設定します。

※ただしこの時、ホストドメイン名には"@"をつけないで設定して下さい。

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
[週加位)     前除(B) ブロパティ(D)     表示(M)     ま示(M)     しーカル ホストの認証に使用される鍵です。
OK 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下さい。「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。

### <<セキュリティポリシーの設定>>

■ NET-G Secure VPN Client ポリシー エディタ	<u>?</u> ×
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 ●
<u>追加(A)</u> 肖耶余(B) フロパティ(P) 説明 ローカル ホストがセキュリティ ゲートウェイ経由でリモート ブ ークへの IPSec 接続を確立するときに、仮想プライベート されます。	診断(D)… ライベート ネットワ ネットワークが作成
OK キャンセル	道用

ポリシーエディタの「セキュリティポリシー」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	<u>? ×</u>
	ゲートウェイ IP アドレス:	10.10.10.1
- <b>1</b>	リモート ネットワーク:	any 💌
	認証鍵:	🖙 新しい既知共有鍵
		□ レガシ候補を使用する(山)
13断	( <u>D)</u> 7 <u>0777(P)</u>	OK ++>>セル

「VPN 接続を追加」画面が開きます。「ゲートウェイ IP アドレス」で右端の"IP"をクリックし、XR\_A(センター)の WAN 側 IP アドレスを設定します。

「認証鍵」は、既知共有鍵の設定で登録した既知共有鍵の設定名を選択します。

「リモートネットワーク」については右端にある"・・・"をクリックして下さい。

ネットワーク エディタ			? ×
ネットワーク イレー語 名前を後で 「定義されたネットワーク	およびサブネットワ・ 『使用して規則を作 フ	ークに独自の名前を 乍成できます。	付けます。この
名前	IP アドレス	サブネット マスク	
any any6 LAN_A	0.0.0 0:0 192.168.10.0	0.0.0.0 0::0 255.255.255.0	
		新規(N)	肖·耶余( <u>R</u> )
ネットワーク名:	LAN_A		
IP アドレス:	192.168.10.0		<b>%</b>
サブネット マスク:	255.255.255.0		
	[	OK	キャンセル

「ネットワークエディタ」画面が開きます。

「ネットワーク名」は任意の名前を設定することができます。

「IP アドレス」「サブネットマスク」は XR に接続している LAN について設定し (ここでは LAN\_A[センタ 一側のネットワーク]の値を設定しています)、「OK」をクリックします。

VPN 接続	を追加		<u>?</u> ×
	ゲートウェイ IP アドレス:	10.10.10.1	IP
~~ <u>_</u>	リモート ネットワーク:	LAN_A	<b>•</b>
	認証鍵:	🐖 新しい既知共有鍵	•
		🔲 レガシ候補を使用	する(U)
诊断	( <u>D</u> ) プロパティ( <u>P</u> ).	. OK *	キャンセル

リモートネットワーク設定後、「VPN 接続を追加」画面が開きますので、続いてプロパティをクリックします。

規則のプロバ	<b>ティ</b>		<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:	10.10.10.1	IP
Sumal	リモート ネットワーク:	LAN_A	▼
IPSec /	IKE 候補		
· 🍄	認証鍵:	🐖 新しい既知共有	■鍵 💽
~	候補テンプレート:	normal	<b>•</b>
			設定
□ 仮想	見IP アドレスを取得する		
- <b>1</b> ∕- <mark>8</mark>	仮想 IP アドレスは、内部> です。	ネットワークのアドレス	
匚 拡張	121E		
	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
- #兄□月 -			
			<u></u>
		ОК	*+>\tr

「規則のプロパティ」画面が開きます。ここで 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		? ×
🥸 IKE 候補と IPSec	候補の各パラメータ値を設定します。	
∛ ┌IKE 候補		
暗号化アルゴリズム:	AES-128	•
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:	AES-128	-
整合性関数	HMAC-SHA-1	•
IPSec モード	tunnel	~
PFS グループ:	MODP 1024 (group 2)	•
▶ 選択した値のみを候補にた	023	
	OK ++	ンセル

「パラメータ候補画面」が開きます。ここで暗号化方式などを設定します。IKE モードは「aggressive mode」を設定します。また「選択した値のみを候補に加える」にチェックをいれます。

規則のプロパ	<del>7</del> 7		? ×
全般	É糸田		
リモート:	Eンドポイント		
	ゲートウェイ IP アドレス:	10.10.10.1	IP
<b>.</b>	リモート ネットワーク:	LAN_A	<b>•</b>
IPSec /	IKE 候補		
<b>*</b>	認証鍵	🐖 新しい既知共有	键 🔽
<b>v</b>	候補テンプレート	normal	<b>_</b>
□ 仮想	IP アドレスを取得する		
-1× <mark>=</mark>	仮想 IP アドレスは、内部ネ です。	シャトワークのアドレス	
□ 拡張			
	VPN ケートリエイ Cld、IKE または CHAP 認証が必要。 す。	XAuth、RADIUS、 となる場合がありま	
一記四月一			
			& C 🗠
		OK	キャンセル

「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。

「詳細タブ」をクリックします。ここで詳細オプションにある「NAT 装置を経由する」のチェックボッ クスを有効にし、「NAT-T(Network Address Translation Traversal)」を選択します。

規則のプロパう	<del>7</del> 4	? ×
全般 詳		
セキュリテ	ィの関連付けの有効期間	-
<b>\$</b>	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。	
監査オプ	ション	-
61	▼ この規則を監査する(A)	
詳細オプ	ション	-
NAT-T	<ul> <li>□P. 圧縮を適用する①</li> <li>○ PMTU (Path Maximum Transfer Unit) を発見する(M)</li> <li>○ NAT 天置を経由する</li> <li>○ NAT-T (Network Address Translation Traversal)</li> <li>○ ポート(ご適用する UDP カプセル化: 2746</li> <li>記動時で(閉(⑤)</li> <li>□ 記動時で(閉(⑤)</li> <li>□ お削し入りングを拒否する</li> <li>* D 圧縮情報</li> <li>NAT-T と IP 圧縮を同時(ご選択することはできません (前者は後者をサポートしません)。</li> </ul>	

これで設定は完了です。

続いて IPsec 接続を行います。



タスクトレーの中にある FutureNet Net-G VPNclient のアイコンを右クリックします。そして「VPN を 選択」の指定し、作成した IPsec ポリシーを選択します。

VPN 接続の状態	×
次の場所への VPN 接続を開いています 10.10.10.1 (LAN_A)	
	(キャンセル)

選択後、IKE のネゴシエーションを行う画面が表示されます。

VPN 接続	の状態	×
8	VPN 接続は正常に確立されました。	
-		

IPsec が正常に確立した場合、「VPN 接続は正常に確立しました」という画面が表示されます。

これで IPsec 接続は完了です。

# NAT ルータ

## ポイント

この設定例では、NAT ルータの設定例は記載していません。

NAT ルータの主な必要な要件は以下のとおりです。

- ・インターネット接続ができていること
- ・IP マスカレードが有効になっていること
- ・フィルタ設定で IPsec NAT-Traversal で使用する UDP ポートが許可されていること

# 8. IPsec backupSA 機能(IPsec 冗長化)利用例

センター側回線やセンター側の障害に備えて、IPsec backupSA 機能を搭載しています。IPsec のメイン の VPN 回線に障害が発生した場合、バックアップ側のセキュリティゲートウェイに対して即時に VPN を 張ることができます。

この例では、センターメインルータの WAN 回線に障害が発生した場合に、拠点ルータの IPsec backupSA 機能によりバックアップ経路を確立するための設定例です。



# 8-1. 構成例

# 8-2. 要件

- ▶ インタフェースおよび PPPoE
  - インターネットには PPPoE で接続します。
  - PPPoE 接続は、自動再接続するように設定しています。
  - WAN 側インタフェースの IP マスカレード、ステートフルパケットインスペクションは「有効」にしています。

主なインタフェースおよび PPPoE のパラメータ

	XR_A(センター1)	XR_A2(センター2)	XR_B(拠点)
LAN 側インタフェース	Ether0	Ether0	Ether0
LAN 側 IP アドレス	192. 168. 10. 1	192. 168. 10. 2	192. 168. 20. 1
WAN 側インタフェース	Ether1[ppp0]	Ether1[ppp0]	Ether1[ppp0]
WAN 側 IP アドレス	10. 10. 10. 1	10. 10. 20. 1	動的 IP
PPPoE ユーザ名	test1@centurysys	test2@centurysys	test3@centurysys
PPPoE パスワード	test1pass	test2pass	test3pass
接続回線	PPPoE 接続	PPPoE 接続	PPPoE 接続

#### ≻ IPsec

- 鍵交換モードはアグレッシブモードを使用します。
- XR\_A(センター1)は 192. 168. 10. 0/24 <-> 192. 168. 20. 0/24 の時に IPsec を適用しま す。
- XR\_A2(センター2)は192.168.10.0/24 <-> 192.168.20.0/24 の時に IPsec を適用しま す。
- XR\_B(拠点)は192.168.20.0/24 <-> 192.168.10.0/24の時に IPsec を適用します。
- IPsec KeepAlive は XR\_A(センター1), XR\_A2(センター2)が動作オプション 1 で、 XR\_B(拠点)が動作オプション 2 で使用します。
- XR\_B(拠点)は IPsec KeepAlive backup SA 機能を使用します。
   この時 XR\_A(センター1)に対する IPsec トンネルのディスタンス値を「1」, XR\_A2(センター2)に対する IPsec トンネルのディスタンス値を「2」に設定しています。

本装置側のパラメータ

	XR_A(センター1)	XR_A2(センター2)	XR_B(拠点)
インタフェースの IP アドレス	10. 10. 10. 1	10. 10. 20. 1	%ppp0
上位ルータの IP アドレス	%ppp0	%ppp0	
インタフェースの ID			@ipsec1

	(L\$), <u>AR_A2</u> (L	~ / Z/]
	XR_A(センター1)	XR_A2(センター2)
対向拠点	XR_B(拠点)	XR_B(拠点)
IKE/ISAKMP ポリシー名	XR_B	XR_B
リモート IP アドレス	0. 0. 0. 0	0. 0. 0. 0
モード	Aggressive	Aggressive
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
DH グループ	Group2	Group2
ライフタイム	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey2

IKE/ISAKMP ポリシーのパラメータ(1) 「XR\_A(センター), XR\_A2(センター2)」

IPsec ポリシーのパラメータ(1) 「 $XR_A(センター), XR_A2(センター2)$ 」

	XR_A(センター1)	XR_A2(センター2)
対向拠点	XR_B(拠点)	XR_B(拠点)
使用する IKE ポリシー名	XR_B(IKE1)	XR_B(IKE1)
本装置の LAN 側のネットワークアドレス	192.168.10.0/24	192. 168. 10. 0/24
相手側の LAN 側のネットワークアドレス	192.168.20.0/24	192. 168. 20. 0/24
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
PFS (DH グループ)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)
DISTANCE	1	1

IKE/ISAKMP ポリシーのパラメータ(2) 「XR\_B(拠点)」

	XR_B (	拠点)
対向拠点	XR_A(センター1)	XR_A2(センター2)
IKE/ISAKMP ポリシー名	XR_A	XR_A2
リモート IP アドレス	10. 10. 10. 1	10. 10. 20. 1
モード	Aggressive	Aggressive
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
DH グループ	Group2	Group2
ライフタイム	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey2

IPsec ポリシーのパラメータ(2) 「XR\_B(拠点)」

	XR_B (	拠点)
対向拠点	XR_A(センター1)	XR_A2(センター2)
使用する IKE ポリシー名	XR_A(IKE1)	XR_A2(IKE2)
本装置の LAN 側のネットワークアドレス	192.168.20.0/24	192. 168. 20. 0/24
相手側の LAN 側のネットワークアドレス	192.168.10.0/24	192.168.10.0/24
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
PFS (DH グループ)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)
DISTANCE	1	2

	XR_A(センター1)	XR_A2(センター2)
対向拠点	XR_B(拠点)	XR_B(拠点)
Policy No.	1	1
source address	192. 168. 10. 1	192. 168. 10. 2
destination address	192. 168. 20. 1	192. 168. 20. 1
interval(sec)	30	30
watch count	3	3
timeout/delay(sec)	60	60
動作option	1	1
interface	ipsec0	ipsec0

IPsec Keepalive  $\mathcal{O}$   $\mathcal{O}$   $\mathcal{O}$   $\mathcal{O}$   $\mathcal{O}$  (1)  $\lceil XR_A(\tau \vee \beta - 1), XR_A2(\tau \vee \beta - 2) \rfloor$ 

IPsec Keepalive のパラメータ (2) 「XR\_B(拠点)」

	XR_B (	拠点)
対向拠点	XR_A(センター1)	XR_A2(センター2)
Policy No.	1	2
source address	192. 168. 20. 1	192. 168. 20. 1
destination address	192. 168. 10. 1	192. 168. 10. 2
interval(sec)	45	60
watch count	3	3
timeout/delay(sec)	60	60
動作option	2	2
interface	ipsec0	ipsec0
backup SA	2	

# ▶ その他

XR\_A(センター1), XR\_A2(センター2)では IPsec 接続していないときに、拠点方向へのルートを IPsec 接続中の XR へ切り替えるためのスタティックルートを設定しています。

### 8-3. 設定例

#### センタールータ1(XR\_A)

#### ポイント

拠点とメインで IPsec 接続するルータになります。 拠点が動的 IP のため、アグレッシブモードを使用します。 WAN 側の回線断等で IPsec KeepAlive による障害が検出された場合、XR\_A2(センター2)へのルーティン グを有効にします。

## 〈〈インタフェース設定〉〉

[Ethernet0の設定]

<ol> <li>固定アド</li> </ol>	レスで使用
IPアドレス	192.168.10.1
ネットマスク	255.255.255.0
MTU	1500

Ethernet0 に関する設定をします。

※IPアドレスの設定を変更した場合、その設定した IPアドレスが即反映されます。

[Ethernet1の設定]

<ol> <li>固定アド</li> </ol>	レスで使用
IP アドレス	0
ネットマスク	255.255.255.0
мти	1500

Ethernet1 に関する設定をします。 PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

#### <<PPP/PPPoE 設定>>

[接続先設定1]

ユーザロ	test1@centurysys	
パスワード	test1pass	

PPPoE 接続で使用するユーザ ID, パスワードを登録します。

[接続設定]

接続先の選択	●接號先1 ●接読先2 ●接號先3 ●接號先4 ●接読先5
接続ボート	O Ether0 • Ether1 • Ether2 • BRI(64K) • BRI MP(128K) • RS232C
接統形態	○ 手動接続 ○ 常時接続 ○ スケジューラ接続
RS232C/BRI接続タイプ	<ul> <li>● 通常</li> <li>● On-Demand接続</li> </ul>
ドマスカレード	○無効 ● 有効
ステートフルパケット インスペウション	○無効 ○有効 □DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ● 有効

PPPoE 接続するインタフェース、および接続形態を選択します。 ※この例では、ルータ経由でのインターネットアクセスも可能になっています。



PPPoEの再接続性を高めるために、PPPoE 特殊オプションを設定しています。

## <<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ррр0	パケ水受信時	許可 🔽	udp 💌		500		500	
ррр0	パケ水受信時	許可 🔽	esp 💌					

IKE パケット, ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

[転送フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ipsec0	パケット受信時 💌	破棄 💌	icmp 💌	192.168.20.1		192.168.10.2		

メインの IPsec SA で接続中に、バックアップの IPsec SA に対する IPsec KeepAlive 要求がセンターメ インルータ(XR\_A)からセンター側 LAN を経由してセンターバックアップルータ(XR\_A2)へ届いてしまい ます。

このフィルタによりそれを防止します。

#### <<各種サービスの設定>>

<IPsec サーバ>

[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	%ррр0
インターフェー スのID	(例:@xr.centurysys)

XR\_A(センター1)のWAN側インタフェースのIPアドレス,および上位ルータのIPアドレスを設定します。 PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。 [IKE/ISAKMPの設定1]

IKE/ISAKMPポリシー名	XR_B
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	@ipsec1 (例:@xncenturysys)
モードの設定	aggressive モード 💌
	1╋目 group2-aes128-sha1 💌
からなっていていた。	2番目 使用しない 🛛 👻
transformの設定	2番目 使用しない <ul> <li>マ</li> <li>3番目 使用しない <ul> <li>マ</li> </ul> </li></ul>
transformの設定	2番目 使用しない ♥ 3番目 使用しない ♥ 4番目 使用しない ♥

XR\_B(拠点)に対する IKE/ISAKMP ポリシーを設定します。

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 RSAL設定してください)</li> </ul>	ipseckey1

事前共有鍵(PSK)として「ipseckey1」を設定しています。

[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
----------------	------------------	------------------

XR\_B(拠点)の IP アドレスが不定のため、「Responder として使用する」を選択します。

使用するIKEポリシー名の選択	XR_B ((KE1) 💌
本装置側のL4N側のネオワークアドレス	192.168.10.0/24 (例:192.168.00/24)
相手側のLAN側のネットワークアドレス	192.168.20.0/24 (例:192.168.00/24)
PH2のTransFormの選択	aes128-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)
DISTANCE	1 (1~255まで)

XR\_B(拠点)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。

[IPsec Keep-Alive 設定]

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1 <u>米</u>	動作option 2 <u>米</u>	interface	backup SA
1		192.168.10.1	192.168.20.1	30	3	60			ipsec0 💌	

XR\_B(拠点)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

## 【IPsec サーバ】



IPsec サーバ機能を起動します。

<<スタティックルート設定>>

No.	アドレス	ネットマスク	インターフェー ス/ゲートウェイ	ディスタンス (1-255>
1	192.168.20.0	255.255.255.0	192.168.10.2	10

IPsec 接続していないときに、拠点方向へのルートを IPsec 接続中の XR ヘフローティングさせるために、 スタティックルートの設定を行います。

この例では、IPsec 接続しているときは、IPsec ルートのディスタンス値(=1)の方がスタティックルート のディスタンス値(=10)より小さいため、IPsec ルートが有効になっているときは、このスタティックル ートは無効の状態になっています。

# センタールータ 2(XR\_A2)

### ポイント

拠点とバックアップで IPsec 接続するルータになります。 拠点が動的 IP のため、アグレッシブモードを使用します。

## 〈〈インタフェース設定〉〉

[Ethernet0の設定]

<ul> <li>         ・         ・         ・</li></ul>	レスで使用
IP アドレス	192.168.10.2
ネットマスク	255.255.255.0
MTU	1500

Ethernet0 に関する設定をします。

※IPアドレスの設定を変更した場合、その設定した IPアドレスが即反映されます。

[Ethernet1の設定]

◎固定アド	レスで使用	
IPアドレス	0	
ネットマスク	255.255.255.0	
MTU	1500	

Ethernet1 に関する設定をします。

PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

## <<PPP/PPPoE 設定>>

[接続先設定1]

ユーザID	test2@centurysys
パスワード	test2pass

PPPoE 接続で使用するユーザ ID,パスワードを登録します。

[接続設定]

接続先の選択	●接號先1 ●接號先2 ●接號先3 ●接號先4 ●接読先5
接続ボート	O Ether0 • Ether1 • Ether2 • BRI(64K) • BRI MP(128K) • RS232C
接統形態	○ 手動接続 ○ 常時接続 ○ スケジューラ接続
RS232C/BRI接続タイプ	<ul> <li>● 通常</li> <li>○ On-Demand接続</li> </ul>
ドマスカレード	○無効 ● 有効
ステートフルパケット インスペウション	○ 無効 ● 有効 □ DROP したパケットのLOGを取得
デフォルトルートの設定	○ 無効 ● 有効

PPPoE 接続するインタフェース、および接続形態を選択します。 ※この例では、ルータ経由でのインターネットアクセスも可能になっています。



PPPoEの再接続性を高めるために、PPPoE 特殊オプションを設定しています。

## <<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ррр0	パケオ受信時	許可 💌	udp 💌		500		500	
рррО	パケオ受信時	許可 💌	esp 💌					

IKE パケット, ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

[転送フィルタ]

インターフェー ス	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ipsec0	パケット受信時 ⊻	破棄 🔽	icmp 💌	192.168.20.1		192.168.10.1		

バックアップの IPsec SA で接続中に、メインの IPsec SA に対する IPsec KeepAlive 要求がセンターバ ックアップルータ(XR\_A2)からセンター側 LAN を経由してセンターメインルータ(XR\_A)へ届いてしまい ます。

これによりメインの IPsec SA が復旧したと誤認してしまうため、IPsec 接続が不安定な状態になります。 このフィルタにより IPsec 接続が不安定になるのを防止します。

#### <<各種サービスの設定>>

<IPsec サーバ>

[本装置側の設定1]

インターフェー スのIPアドレス	10.10.20.1
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)

XR\_A2(センター2)の WAN 側インタフェースの IP アドレス,および上位ルータの IP アドレスを設定します。

PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。

[IKE/ISAKMP の設定 1]

IKE/ISAKMP ポリシーのパラメータは以下のとおりです。

IKE/ISAKMPポリシー名	XR_B				
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	@ipsec1 (例:@vr.centurysys)				
モードの設定	aggressive モード 💌				
	1∰目 group2-aes128-sha1 💌				
	2番目 使用しない 🔽				
transform0/asta	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)				

XR\_B(拠点)に対する IKE/ISAKMP ポリシーを設定します。

鍵の設定	
<ul> <li>PSKを使用する</li> <li>RSAを使用する</li> <li>0509を使用する場合は</li> <li>RSAに設定してください)</li> </ul>	ipseckey2

事前共有鍵(PSK)として「ipseckey2」を設定しています。

[IPsec ポリシーの設定 1]



XR\_B(拠点)の IP アドレスが不定のため、「Responder として使用する」を選択します。

使用するIKEポリシー名の選択	XR_B (IKE1) 💌
本装置側のLAN側のネオワークアドレス	192.168.10.0/24 (9):192.168.00/24)
相手側のLAN側のネットワークアドレス	192.168.20.0/24 (約:192.168.00/24)
PH2のTransFormの選択	aes128-sha1 💌
PFS	<ul> <li>● 使用する</li> <li>● 使用しない</li> </ul>
DH Groupの選択(PFS使用時に有効)	eroup2
SAØF17914	28800 秒 (1081~86400秒まで)
DISTANCE	1 (1~255まで)

XR\_B(拠点)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。

[IPsec Keep-Alive 設定]

enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1 <u>米</u>	動作option 2 <u>米</u>	interface	backup SA
<b>&gt;</b>	192.168.10.2	192.168.20.1	30	3	60			ipsec0 💌	

XR\_B(拠点)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

## 【IPsec サーバ】

Psecty-バ ○停止 ⊙起動
------------------

IPsec サーバ機能を起動します。

<<スタティックルート設定>>

アドレス	ネットマスク	トマスク インターフェース/ゲートウェイ	
192.168.20.0	255.255.255.0	192.168.10.1	10

IPsec 接続していないときに、拠点方向へのルートを IPsec 接続中の XR ヘフローティングさせるために、 スタティックルートの設定を行います。

この例では、IPsec 接続しているときは、IPsec ルートのディスタンス値(=1)の方がスタティックルート のディスタンス値(=10)より小さいため、IPsec ルートが有効になっているときは、このスタティックル ートは無効の状態になっています。

## 拠点ルータ(XR\_B)

#### ポイント

正常時は XR\_A (センター1) と IPsec 接続を行い、XR\_A (センター1)の WAN 側の回線断等で IPsec KeepAlive による障害が検出された場合、XR\_A2 (センター2) と IPsec 接続を行います。 WAN 側 IP アドレスが動的 IP のため、アグレッシブモードを使用します。

#### <<インタフェース設定>>

[Ethernet0の設定]

● 固定アドレスで使用		
ℙアドレス	192.168.20.1	1
ネットマスク	255.255.255	5.0
MTU	1500	

Ethernet0 に関する設定をします。

※IPアドレスの設定を変更した場合、その設定した IPアドレスが即反映されます。

[Ethernet1の設定]

● 固定アドレスで使用		
IP アドレス	0	
ネットマスク	255.255.25	5.0
MTU	1500	

Ethernet1 に関する設定をします。

PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

## <<PPP/PPPoE 設定>>

[接続先設定1]

ユーザロ	test3@centurysys	]
パスワード	test3pass	]

PPPoE 接続で使用するユーザ ID,パスワードを登録します。

[接続設定]

接続先の選択	●接統先1 ●接統先2 ●接統先3 ●接統先4 ●接統先5
接続ボート	O Ether0 O Ether1 O Ether2 O BRI(64K) O BRI MP(128K) O RS2320
接統形態	○ 手動接続 ● 常時接続 ○ スケジューラ接続
RS232C/BRI接続タイプ	<ul> <li>● 通常</li> <li>○ On-Demand接続</li> </ul>
ドマスカレード	○無効 ⊙ 有効
ステートフルパケット インスペウション	○無効 ○ 有効 □ DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ⊙ 有効

PPPoE 接続するインタフェース、および接続形態を選択します。 ※この例では、ルータ経由でのインターネットアクセスも可能になっています。



PPPoEの再接続性を高めるために、PPPoE 特殊オプションを設定しています。

## <<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ррр0	パケ水受信時	許可 🔽	udp 💌		500		500	
ррр0	パケ水受信時	許可 🔽	esp 💌					

IKE パケット, ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

# <<各種サービスの設定>>

#### <IPsec サーバ>

[本装置側の設定 1]

インターフェースのIPアドレス	%рррО	
上位ルータのIPアドレス		
インターフェー スのID	@ipsec1	(例:@xr.centurysys)

PPPoE 接続で WAN 側(ppp0)インタフェースの IP アドレスが不定のため「%ppp0」, インタフェースの ID として「@ipsec1」を設定します。

[IKE/ISAKMPの設定1]

IKE/ISAKMPポリシー名	XR_A
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:@xi.centurysys)
モードの設定	aggressive モード 💌
	1番目 group2-aes128-sha1 💌
two-frame D34 T	2番目 使用しない 🛛 👻
transion to age 2	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 料 (1081~28800秒まで)

XR\_A(センター1)に対する IKE/ISAKMP ポリシーを設定します。

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 RSAL設定してください)</li> </ul>	ipseckey1

事前共有鍵(PSK)として「ipseckey1」を設定しています。

[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-Dermandで使用する

XR\_A(センター1)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

使用するIKEポリシー名の選択	XR_A (IKE1) 💌
本装置側のL4N側のネットワークアドレス	192.168.20.0/24 (第:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.10.0/24 (第:192.168.0.0/24)
FH2のTransFormの選択	aes128-sha1 💌
PFS	<ul> <li>● 使用する</li> <li>● 使用しない</li> </ul>
DH Groupの選択(PFS使用時に有効)	eroup2
SADライフタイム	28800 秒(1081~86400秒まで)
DISTANCE	1 ()~255まで)

XR\_A(センター1)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

```
[IKE/ISAKMPの設定2]
```

IKE/ISAKMPポリシー名	XR_A2	
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	10.10.20.1	
上位ルータのIPアドレス		
インターフェー スのЮ	(例:@xr.centurysys)	
モードの設定	aggressive モード 💌	
	1╋目 group2-aes128-sha1 💌	
	2番目 使用しない 🔽	
(ransiormo)ague	3番目 使用しない 🔽	
	4番目 使用しない 💌	

XR\_A2(センター2)に対する IKE/ISAKMP ポリシーを設定します。

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 RSAL設定してください)</li> </ul>	ipseckey2

事前共有鍵(PSK)として「ipseckey2」を設定しています。

[IPsec ポリシーの設定 2]

🕐 使用する 🔷 使用しない 📀 Responderとして使用する 🔷 On-Dermandで使用する

XR\_B(拠点)は Initiator として動作しますが、backup SA 用の IPsec ポリシーの場合「Responder として 使用する」を選択します。

使用するIKEポリシー名の選択	XR_A2 (IKE2) 💌
本装置側のLAN側のネオワークアドレス	192.168.20.0/24 (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	aes128-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 彩(1081~86400約まで)
DISTANCE	2 (1~255まで)

XR\_A2(センター2)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。

[IPsec Keep-Alive 設定]

enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1 <u>米</u>	動作option 2 <u>米</u>	interface	backup SA
	192.168.20.1	192.168.10.1	45	3	60			ipsec0 💌	2
	192.168.20.1	192.168.10.2	60	3	60			ipsec0 💌	

XR\_A(センター), XR\_A2(センター2)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

XR\_A(センター), XR\_A2(センター2)に IPsec KeepAlive を設定している理由は、拠点が WAN 側動的 IP アドレスを用いた構成で、センター側からの通信があるようなケースでは SA の不一致が起こりうるため、 メイン側, バックアップ側でそれぞれ IPsec KeepAlive を設定しています。(推奨)

※メイン SA とバックアップ SA、または拠点側とセンター側の interval が同じ値の場合、KeepAlive の 周期が同期してしまい、障害時の IPsec 切り替え直後に、切り替えた先でもすぐに障害を検出して、IPsec 通信が不安定になることがあります。これを防ぐために、拠点側の XR 同士の interval は、それぞれ異 なる値を設定することを推奨します。さらにそれぞれの値はセンター側とも異なる値を設定して下さい。

【IPsec サーバ】

IPsecty→バ ○停止 ⊙起動
-------------------

IPsec サーバ機能を起動します。

# 9. ISDN を利用した回線バックアップ例その1 (メイン回線 IPsec)

この例は、PPPoE で IPsec 接続しているメイン回線で障害が発生したときに、拠点側からの ISDN による バックアップを実現する設定例です。

# 9-1. 構成例



## 9-2. 要件

- ▶ インタフェースおよび PPP/PPPoE
  - インターネットに PPPoE で接続します。
  - PPPoE 接続は、自動再接続するように設定しています。
  - WAN 側インタフェースの IP マスカレード、ステートフルパケットインスペクションは「有効」にしています。
  - XR\_B(拠点)はマルチ回線で ISDN オンデマンド接続をします。
  - XR\_A(センター)ではアクセスサーバ機能を使用し、XR\_B(拠点)からのダイアルアップ 接続を受け付けます。

主なインタフェースおよび PPP/PPPoE のパラメータ

	XR_A(センター)	XR_B(拠点)
LAN 側インタフェース	Ether0	Ether0
LAN 側 IP アドレス	192. 168. 10. 1	192. 168. 20. 1
WAN 側インタフェース	Ether1[ppp0]	Ether1[ppp0]
WAN 側 IP アドレス	10. 10. 10. 1	動的 IP
PPPoE ユーザ名	test1@centurysys	test2@centurysys
PPPoE パスワード	test1pass	test2pass
WAN 側接続回線	PPPoE 接続	PPPoE 接続
ISDN 番号	XR_A-123	XR_B-123
ISDN ユーザ名	_	isdntest
ISDN パスワード	_	isdnpass
ISDN 側 IP アドレス	192. 168. 110. 1	192. 168. 120. 1

≻ IPsec

- 鍵交換モードはアグレッシブモードを使用しています。
- XR\_A(センター)は192.168.10.0/24 <-> 192.168.20.0/24の時にIPsecを適用します。
- XR\_B(拠点)は192.168.20.0/24 <-> 192.168.10.0/24の時に IPsec を適用します。
- IPsec KeepAlive は XR\_A(センター)が動作オプション1で、XR\_B(拠点)が動作オプション2で使用しています。

本装置側のパラメータ

	XR_A(センター)	XR_B(拠点)
インタフェースの IP アドレス	10. 10. 10. 1	%ppp0
上位ルータの IP アドレス	%ppp0	
インタフェースの ID		@ipsec1

	XR_A(センター)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター)
IKE/ISAKMP ポリシー名	XR_B	XR_A
リモート IP アドレス	0. 0. 0. 0	10. 10. 10. 1
インタフェースの ID	@ipsec1	
モード	Aggressive	Aggressive
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
DH グループ	Group2	Group2
ライフタイム	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey1

IKE/ISAKMP ポリシーのパラメータ「XR\_A(センター), XR\_B(拠点)」

IPsec ポリシーのパラメータ 「XR\_A(センター), XR\_B(拠点)」

	XR_A(センター)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター)
使用する IKE ポリシー名	XR_B(IKE1)	XR_A(IKE1)
本装置の LAN 側のネットワークアドレス	192. 168. 10. 0/24	192. 168. 20. 0/24
相手側の LAN 側のネットワークアドレス	192. 168. 20. 0/24	192.168.10.0/24
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
PFS (DH グループ)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)
DISTANCE	1	1

	XR_A(センター)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター)
Policy No.	1	1
source address	192. 168. 10. 1	192. 168. 20. 1
destination address	192. 168. 20. 1	192. 168. 10. 1
interval(sec)	30	45
watch count	3	3
timeout/delay(sec)	60	60
動作option	1	2
interface	ipsec0	ipsec0

IPsec Keepalive のパラメータ 「XR\_A(センター), XR\_B(拠点)」

## ▶ その他

- XR\_A(センター)では IPsec トンネルで障害が発生したときに、拠点方向へのルートを ISDN に切り替えるためのスタティックルートを設定しています。
- XR\_B(拠点)では IPsec トンネルで障害が発生したときにセンター側へのルートを ISDN に切り替えるためのルートを設定しています。

#### 9-3. 設定例

#### センタールータ(XR\_A)

ポイント

拠点と IPsec 接続するための設定を行います。 拠点が動的 IP のため、アグレッシブモードを使用します。

アクセスサーバの設定を行い、WAN 側の回線断等で IPsec KeepAlive による障害が検出された場合、ISDN による着信後、XR\_B(拠点)へのルーティングを有効にします。

## 〈〈インタフェース設定〉〉

[Ethernet0の設定]

<ol> <li>固定アド</li> </ol>	レスで使用
₽₽Fレス	192.168.10.1
ネットマスク	255.255.255.0
мτυ	1500

Ethernet0 に関する設定をします。

※IPアドレスの設定を変更した場合、その設定した IPアドレスが即反映されます。

[Ethernet1の設定]

● 固定アドレスで使用				
IP アドレス	0			
ネットマスク	255.255.255.0			
мти	1500			

Ethernet1に関する設定をします。

PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

#### <<PPP/PPPoE 設定>>

[接続先設定1]

ユーザロ	test1@centurysys	
パスワード	test1pass	

PPPoE 接続で使用するユーザ ID, パスワードを登録します。
[接続設定]

接続先の選択	●接號先1 ●接號先2 ●接號先3 ●接號先4 ●接読先5
接続ボート	O Ether0 • Ether1 • Ether2 • BRI(64K) • BRI MP(128K) • RS232C
接統形態	○ 手動接続 ○ 常時接続 ○ スケジューラ接続
RS232C/BRI接続タイプ	<ul> <li>● 通常</li> <li>○ On-Demand接続</li> </ul>
ドマスカレード	○無効 ● 有効
ステートフルパケット インスペウション	○ 無効 ● 有効 □ DROP したパケットのLOGを取得
デフォルトルートの設定	○ 無効 ● 有効

PPPoE 接続するインタフェース、および接続形態を選択します。 ※この例では、ルータ経由でのインターネットアクセスも可能になっています。



PPPoEの再接続性を高めるために、PPPoE 特殊オプションを設定しています。

## <<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ррр0	パケ水受信時	許可 🔽	udp 💌		500		500	
ррр0	パケ水受信時	許可 🔽	esp 💌					

IKE パケット, ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

# <<各種サービスの設定>>

#### <IPsec サーバ>

[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	%ррр0
インターフェー スのID	(例:@xr.centurysys)

XR\_A(センター)のWAN側インタフェースのIPアドレス,および上位ルータのIPアドレスを設定します。 PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。

[IKE/ISAKMPの設定1]

IKE/ISAKMPポリシー名	XR_B
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	@ipsec1 (例:@xr.centurysys)
モードの設定	aggressive モード 💌
-	1番目 group2-aes128-sha1 V
transformの設定	1番目 group2-aes128-sha1 ▼ 2番目 使用しない ▼
transformの設定	1番目 group2-aes128-sha1 ▼ 2番目 使用しない ▼ 3番目 使用しない ▼
transformの設定	1番目 group2-aes128-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 ♥

XR\_B(拠点)に対する IKE/ISAKMP ポリシーを設定します。

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>	ipseckey1

事前共有鍵(PSK)として「ipseckey1」を設定しています。

[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-Dermandで使用する

XR\_B(拠点)の IP アドレスが不定のため、「Responder として使用する」を選択します。

使用するIKEポリシー名の選択	XR_B (IKE1) 💌
本装置側のL4N側のネットワークアドレス	192.168.10.0/24 (191:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.20.0/24 (M):192.168.00/24)
FH2のTransFormの選択	aes128-sha1 💌
PFS	💿 使用する 🔘 使用しない
DH Groupの選択(PFS使用時に有効)	group2
DH Groupの選択(PFS使用時に有効) SAのライフタイム	group2 💌 28800 秒 (1081~86400秒まで)

XR\_B(拠点)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。

[IPsec Keep-Alive 設定]

enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1 <u>米</u>	動作option 2 <u>米</u>	interface	backup SA
	192.168.10.1	192.168.20.1	30	3	60	<ul><li>✓</li></ul>		ipsec0 💌	

XR\_B(拠点)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

<u>IPsecサーバ</u>

○停止 ⊙起動

IPsec サーバ機能を起動します。

【アクセスサーバ】

	BRI 回線
回線1 著信	○許可しない ○許可する

BRI 回線での着信を許可する設定をします。

No.	ፖカウント	パスワード	アカウント毎に別	IPを割り当てる場 含
			本装置のIP	クライアントのIP
1	isdntest	isdnpass	192.168.110.1	192.168.120.1

BRI 回線で着信したときのアカウント,パスワードを設定します。この時に「アカウント毎に別 IP を割り当てる場合」に IP アドレスを設定することにより、着信時に指定した IP アドレスを割り当てることが可能です。

### <<スタティックルート設定>>

アドレス	ネットマスク	インターフェー	- ス/ゲートウェイ	ディスタンス (1-255>
192.168.20.0	255.255.255.0	рррб	192.168.120.1	10

IPsec 接続していないときに、拠点方向へのルートを ISDN 側へフローティングさせるために、スタティ ックルートの設定を行います。

この例では、IPsec 接続しているときは、IPsec ルートのディスタンス値(=1)の方がスタティックルート のディスタンス値(=10)より小さいため、IPsec のルートが有効になっているときは、このスタティック ルートは無効の状態になっています。

またゲートウェイの IP アドレスはアクセスサーバ設定で対向ルータに対して割り当てた IP アドレスになっています。

拠点ルータ(XR\_B)

ポイント

センターと IPsec 接続するための設定を行います。 WAN 側 IP アドレスが動的 IP のため、アグレッシブモードを使用します。 PPP のマルチセッションの設定を行い、ISDN のオンデマンド接続を行える状態に設定します。 WAN 側の回線断等で IPsec KeepAlive による障害が検出された場合、ISDN 側のルートが有効になり、 XR\_A(センター)に対して ISDN による発信を行います。

## <<インタフェース設定>>

[Ethernet0の設定]

<ol> <li>固定アド</li> </ol>	レスで使用	
ℙアドレス	192.168.20.1	
ネットマスク	255.255.255.0	
мти	1500	

Ethernet0 に関する設定をします。

※IPアドレスの設定を変更した場合、その設定した IPアドレスが即反映されます。

[Ethernet1の設定]

⑧ 固定ア	レスで使用
IP アドレス	0
ネットマスク	255.255.255.0
мτυ	1500

Ethernet1に関する設定をします。 PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

### <<PPP/PPPoE 設定>>

[接続先設定1]

ユーザЮ	test2@centurysys	
パスワード	test2pass	

PPPoE 接続で使用するユーザ ID, パスワードを登録します。

[接続先設定2]

ユーザロ	isdntest	]
パスワード	isdnpass	

PPP(ISDN)接続で使用するユーザ ID, パスワードを登録します。

BRI/PPPシリアル回義使用時に設定して下さい					
電話番号	XR_A-123				

XR\_A(センター)の電話番号を登録します。

BRI/PPPシリアル回義使用時に設定して下さい				
ON-DEMAND接続用 切断タイマー	60 <b>≱</b> y			

※この例では ISDN の ON-DEMAND 接続を利用するため、ON-DEMAND 接続用切断タイマーを設定します。 デフォルト値は「180 秒」になります。ご利用環境によって適宜設定を変更して下さい。

[接続設定]

接続先の選択	●接號先1 ●接號先2 ●接號先3 ●接號先4 ●接號先5
接続ポート	O Ether0 • Ether1 • Ether2 • ERI(64K) • ERI MP(128K) • RS2320
接続形態	○ 手動接続 ● 常時接続 ○ スケジューラ接続
RS232C/BRI接続タイプ	<ul> <li>● 通常</li> <li>○ On-Demand接続</li> </ul>
<b>₽マスカレード</b>	○ 無効 ● 有効
ステートフルパケット インスペウション	○ 無効 ● 有効 □ DROP したパケットのLOGを取得
デフォルトルートの設定	○ 無効 ● 有効

PPPoE 接続するインタフェース、および接続形態を選択します。 ※この例では、ルータ経由でのインターネットアクセスも可能になっています。

マル <del>∫</del> PP	マルチPPP/PPPoEセッション機能を利用する際は以下を設定して下さい					
マルチ接続 #2	○無効 ◎ 有効					
接続先の選択	○接號先1 ●接號先2 ●接號先3 ●接號先4 ●接號先5					
接続ポート	O Ether0 O Ether1 O Ether2 O BRI(64K) O BRI MP(128K) O RS2320					
RS232C/BRI接続タイプ	◯ 通常 <sup>●</sup> On-Demand接统					
<b>₽マスカレード</b>	⊙ 無効 ○ 有効					
ステートフルパケット インスペクション	○ 無効 ○ 有効 □ DROP したパケットのLOGを取得					

マルチ接続側(ISDN側)の接続先,接続ポートおよび接続タイプを設定します。



PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定しています。

### <<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ррр0	パケット受信時	許可 🔽	udp 💌		500		500	
ррр0	パケット受信時	許可 💌	esp 💌					

IKE パケット, ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

<<各種サービスの設定>>

### <IPsec サーバ>

[本装置側の設定 1]

インターフェースのIPアドレス	%рррО	
上位ルータのIPアドレス		
インターフェー スのЮ	@ipsec1	(例:@xr.centurysys)

PPPoE 接続で WAN 側(ppp0)インタフェースの IP アドレスが不定のため「%ppp0」, インタフェースの ID として「@ipsec1」を設定します。

[IKE/ISAKMPの設定1]

IKE/ISAKMPポリシー名	XR_A			
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Ю	(例:@xt.centurysys)			
モードの設定	aggressive モード 💌			
	1╋目 group2-aes128-sha1 💌			
	2番目 使用しない 💌			
transformu) ag ja	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)			

XR\_A(センター)に対する IKE/ISAKMP ポリシーを設定します。

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 RSAL設定してください)</li> </ul>	ipseckey1

事前共有鍵(PSK)として「ipseckey1」を設定しています。

[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-Dermandで使用する

XR\_A(センター)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

使用するIKEポリシー名の選択	XR_A (IKE1) 💌
本装置側のL4N側のネオワークアドレス	192.168.20.0/24 (期:192.168.00/24)
相手側のLAN側のネットワークアドレス	192.168.10.0/24 (期:192.168.00/24)
FH2のTransFormの選択	aes128-sha1 💌
PFS	<ul> <li>使用する</li> <li>使用しない</li> </ul>
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)
DISTANCE	1 (1~255まで)

XR\_A(センター)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

[IPsec Keep-Alive 設定]

enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1 <u>米</u>	動作option 2 <u>米</u>	interface	backup SA
<b>V</b>	192.168.20.1	192.168.10.1	45	3	60			ipsec0 💌	

XR\_A(センター)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

IPsecサーバ	○停止	⊙起動	

IPsec サーバ機能を起動します。

### <<スタティックルート設定>>

アドレス	ネットマスク	インターフェー	- ス/ゲートウェイ	ディスタンス (1-255>
192.168.10.0	255.255.255.0	ppp2		10

IPsec 接続していないときに、センター方向へのルートを ISDN 側へフローティングさせるために、スタ ティックルートの設定を行います。

この例では、IPsec 接続しているときは、IPsec ルートのディスタンス値(=1)の方がスタティックルート のディスタンス値(=10)より小さいため、IPsec ルートが有効になっているときは、このスタティックル ートは無効の状態になっています。

またこの例では ISDN 側は「ppp2」インタフェースとなるため、インタフェースの項目に「ppp2」を設定 しています。

# 10. ISDN を利用した回線バックアップ例その2(メイン回線 IPsec)

この例は、PPPoE で IPsec 接続しているメイン回線で障害が発生したときに、拠点からの ISDN によるバ ックアップを実現する設定例です。

またセンターメインルータの機器障害が発生した場合でも、VRRP との組み合わせによりバックアップ経路を利用できます。

## 10-1. 構成例



## 10-2. 要件

- ▶ インタフェースおよび PPP/PPPoE
  - インターネットに PPPoE で接続します。
  - PPPoE 接続は、自動再接続するように設定しています。
  - WAN 側インタフェースの IP マスカレード、ステートフルパケットインスペクションは「有効」にしています。
  - XR\_B(拠点)はマルチ回線で ISDN オンデマンド接続をします。
  - XR\_A2(センター2)ではアクセスサーバ機能を使用し、XR\_B(拠点)からのダイアルアップ接続を受け付けます。

主なインタフェースおよび PPP/PPPoE のパラメータ

	XR_A(センター1)	XR_A2(センター2)	XR_B(拠点)
LAN 側インタフェース	Ether0	Ether0	Ether0
LAN 側 IP アドレス	192. 168. 10. 1	192. 168. 10. 2	192. 168. 20. 1
WAN 側インタフェース	Ether1[ppp0]	_	Ether1[ppp0]
WAN 側 IP アドレス	10. 10. 10. 1	-	動的 IP
PPPoE ユーザ名	test1@centurysys	-	test2@centurysys
PPPoE パスワード	test1pass	-	test2pass
WAN 側接続回線	PPPoE 接続	-	PPPoE 接続
ISDN 番号	_	XR_A-123	XR_B-123
ISDN ユーザ名	-	-	isdntest
ISDN パスワード	-	-	isdnpass
ISDN 側 IP アドレス	_	192. 168. 110. 1	192. 168. 120. 1

≻ VRRP

- Ether0 側で VRRP を使用しています。
- 優先度は XR\_A(センター1)「100」, XR\_A2(センター2)「50」に設定しています。

主な VRRP のパラメータ

	XR_A(センター1)	XR_A2(センター2)
使用するインターフェース	Ether0	Ether0
ルータ ID	51	51
優先度	100	50
IPアドレス	192. 168. 10. 100	

### ≻ IPsec

- 鍵交換モードはアグレッシブモードを使用しています。
- XR\_A(センター1)は 192.168.10.0/24 <-> 192.168.20.0/24 の時に IPsec を適用しま す。
- XR\_B(拠点)は192.168.20.0/24 <-> 192.168.10.0/24 の時に IPsec を適用します。
- IPsec KeepAlive は XR\_A(センター1)が動作オプション1で、XR\_B(拠点)が動作オプション2で使用しています。

本装置側のパラメータ

	XR_A(センター1)	XR_B(拠点)
インタフェースの IP アドレス	10. 10. 10. 1	%ppp0
上位ルータの IP アドレス	%ppp0	
インタフェースの ID		@ipsec1

	XR_A(センター1)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター1)
IKE/ISAKMP ポリシー名	XR_B	XR_A
リモート IP アドレス	0. 0. 0. 0	10. 10. 10. 1
インタフェースの ID	@ipsec1	
モード	Aggressive	Aggressive
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
DH グループ	Group2	Group2
ライフタイム	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey1

IKE/ISAKMPポリシーのパラメータ「XR\_A(センター), XR\_B(拠点)」

IPsec ポリシーのパラメータ 「XR\_A(センター), XR\_B(拠点)」

	XR_A(センター1)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター1)
使用する IKE ポリシー名	XR_B(IKE1)	XR_A(IKE1)
本装置の LAN 側のネットワークアドレス	192.168.10.0/24	192. 168. 20. 0/24
相手側の LAN 側のネットワークアドレス	192. 168. 20. 0/24	192. 168. 10. 0/24
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
PFS (DH グループ)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)
DISTANCE	1	1

	XR_A(センター1)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター1)
Policy No.	1	1
source address	192. 168. 10. 1	192. 168. 20. 1
destination address	192. 168. 20. 1	192. 168. 10. 1
interval(sec)	30	45
watch count	3	3
timeout/delay(sec)	60	60
動作option	1	2
interface	ipsec0	ipsec0

IPsec Keepalive のパラメータ 「XR\_A(センター1), XR\_B(拠点)」

### ▶ その他

- XR\_A(センター1)では IPsec トンネルで障害が発生したときに、拠点方向へのルート を XR\_A2(センター2)に切り替えるためのスタティックルートを設定しています。
- XR\_A2(センター2)では ISDN 接続していないときに拠点方向へのルートを XR\_A(セン ター1)へ切り替えるためのスタティックルートを設定しています。
- XR\_B(拠点)では IPsec トンネルで障害が発生したときにセンター側へのルートを ISDN に切り替えるためのルートを設定しています。

## 10-3. 設定例

## センタールータ1(XR\_A)

ポイント

拠点と IPsec 接続するための設定を行います。

拠点が動的 IP のため、アグレッシブモードを使用します。

WAN 側の回線断等で IPsec KeepAlive による障害が検出された場合、XR\_A2(センター2)へのルーティン グを有効にします。

XR\_Aの機器障害が発生した場合に備えて、XR\_A2(センター2)とのVRRPで冗長化を行っています。

### <<インタフェース設定>>

[Ethernet0の設定]

<ol> <li>固定アド</li> </ol>	レスで使用	
IP アドレス	192.168.10.1	
ネットマスク	255.255.255.0	
MTU	1500	

Ethernet0 に関する設定をします。

※IPアドレスの設定を変更した場合、その設定した IPアドレスが即反映されます。

[Ethernet1の設定]

<ul> <li>固定アド</li> </ul>	レスで使用
IPアドレス	0
ネットマスク	255.255.255.0
MTU	1500

Ethernet1に関する設定をします。 PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

#### <<PPP/PPPoE 設定>>

### [接続先設定1]

ユーザロ	test1@centurysys	
パスワード	test1pass	

PPPoE 接続で使用するユーザ ID,パスワードを登録します。

[接続設定]

接続先の選択	●接統先1 ●接統先2 ●接統先3 ●接統先4 ●接統先5
接続ボート	O Ether0 • Ether1 • Ether2 • BRI(64K) • BRI MP(128K) • RS2320
接続形態	○ 手動接続 ● 常時接続 ● スケジューラ接続
RS232C/BRI接続タイプ	<ul> <li>● 通常</li> <li>○ On-Demand接続</li> </ul>
ドマスカレード	○無効 ⊙ 有効
ステートフルパケット インスペウション	○ 無効 ● 有効 □ DROP したパケットのLOGを取得
デフォルトルートの設定	○ 無効 ● 有効

PPPoE 接続するインタフェース、および接続形態を選択します。 ※この例では、ルータ経由でのインターネットアクセスも可能になっています。

PPPoE特殊オプション (全回線共通) ✓ 回線接続時に前回のPPPœセッションのPADTを強制送出
 ✓ 非接続SessionのIPv4Packet受信時IごPADTを強制送出
 ✓ 非接続SessionのLCP-EchoRequest受信時IごPADTを強制送出

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定しています。

### <<フィルタ設定>>

[入力フィルタ]

インターフェー ス	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
рррО	パケット受信時	許可 🚩	udp 💌		500		500	
рррО	パケット受信時	許可 🔽	esp 💌					

IKE パケット, ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

### <<各種サービスの設定>>

### <IPsec サーバ>

[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	%ррр0
インターフェー スのID	(例:@xr.centurysys)

XR\_A(センター)のWAN 側インタフェースの IP アドレス,および上位ルータの IP アドレスを設定します。 PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。 [IKE/ISAKMPの設定1]

IKE/ISAKMPポリシー名	XR_B
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	@ipsec1 (例:@xr.centurysys)
モードの設定	aggressive モード 💌
	1番目 group2-aes128-sha1 💌
	2番目 使用しない 💌
transformu/asta	3番目 使用しない 🔽
	4番目 使用しない 🔽

XR\_B(拠点)に対する IKE/ISAKMP ポリシーを設定します。

鍵の設定	
<ul> <li>PSKを使用する</li> <li>RSAを使用する</li> <li>(X500を使用する場合は RSAL設定してください)</li> </ul>	ipseckey1

事前共有鍵(PSK)として「ipseckey1」を設定しています。

[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

XR\_B(拠点)の IP アドレスが不定のため、「Responder として使用する」を選択します。

使用するIKEポリシー名の選択	XR_B (IKE1) 💌
本装置側のL4N側のネオワークアドレス	192.168.10.0/24 (M:192.168.00/24)
相手側のLAN側のネットワークアドレス	192.168.20.0/24 (M:192.168.00/24)
FH2のTransFormの選択	aes128-sha1 💌
PFS	💿 使用する 🔘 使用しない
DH Groupの選択(PFS使用時に有効)	eroup2
SADライフタイム	28800 秒 (1081~85400秒まで)
DISTANCE	1 (1~255まで)

XR\_B(拠点)に対して IPsec 通信を行う IP アドレスの範囲を設定しています。

[IPsec Keep-Alive 設定]

enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1 <u>米</u>	動作option 2 <u>米</u>	interface	backup SA
	192.168.10.1	192.168.20.1	30	3	60			ipsec0 💌	

「LAN\_B」に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

## 【IPsec サーバ】

IPsecty→バ ○停止 ⊙起動	
-------------------	--

IPsec サーバを起動します。

【VRRP サービス】

使用するインターフェース	仮想MACアドレス	ルータロ	優先度	IPアドレス	インターバル	Auth_Type	password
Ether 0 💌	使用しない 🔽	51	100	192.168.10.100	1	指定しない 💌	

LAN 側インタフェース「Ether0」で XR\_A2 (センター2)と VRRP による冗長化を行います。

<u>MRPH-EZ</u>	○停止	◉起動	

VRRP サービスを起動します。

<<スタティックルート設定>>

アドレス	ネットマスク	インターフェー ス/ゲートウェイ	ディスタンス <1-255>
192.168.20.0	255.255.255.0	192.168.10.2	10

IPsec 接続していないときに、拠点方向へのルートを XR\_A2 側へフローティングさせるために、スタティックルートの設定を行います。

この例では、IPsec 接続しているときは、IPsec ルートのディスタンス値(=1)の方がスタティックルート のディスタンス値(=10)より小さいため、IPsec ルートが有効になっているときは、このスタティックル ートは無効の状態になっています。

## センタールータ 2(XR\_A2)

### ポイント

アクセスサーバの設定を行い、ISDN による着信後、XR\_B(拠点)へのルーティングを有効にします。 XR\_A の LAN 側で障害が発生した場合に備えて、VRRP で冗長化を行っています。

### <<インタフェース設定>>

[Ethernet0の設定]

<ul> <li>固定アド</li> </ul>	● 固定アドレスで使用			
IP アドレス	192.168.10.2			
ネットマスク	255.255.255.0			
MTU	1500			

Ethernet0 に関する設定をします。

※IPアドレスの設定を変更した場合、その設定した IPアドレスが即反映されます。

【アクセスサーバ】

BRI 回線				
回線1 著信	○許可しない ⊙許可する			

BRI 回線での着信を許可する設定をします。

No.	アカウント	パスワード	アカウント毎に別IPを割り当てる場合		
			本装置のIP	クライアントのIP	
1	isdntest	isdnpass	192.168.110.1	192.168.120.1	

BRI 回線で着信したときのアカウント,パスワードを設定します。この時に「アカウント毎に別 IP を割り当てる場合」に IP アドレスを設定することにより、着信時に指定した IP アドレスを割り当てることが可能です。

### <<スタティックルート設定>>

アドレス	ネットマスク	ネットマスク インターフェー		ディスタンス <1-255>
192.168.20.0	255.255.255.0	рррб	192.168.120.1	1
192.168.20.0	255.255.255.0		192.168.10.1	10

一行目は XR\_B(拠点)からの ISDN 発信を着信した場合に有効になるルートです。ゲートウェイの IP アド レスはアクセスサーバ設定で対向ルータに対して割り当てた IP アドレスになっています。着信していな い場合は、二行目のルートが有効になっています。

【VRRP サービス】

を設定しています。

使用するインターフェース	仮想MACアドレス	ルータロ	優先度	IPアドレス	インターバル	Auth_Type	password
Ether 0 💌	使用しない 🔽	51	50	192.168.10.100	1	指定しない 💌	

LAN 側インタフェース「Ether0」で XR\_A(センター1)と VRRP による冗長化を行います。 この例では、正常時 XR\_A2(センター2)はバックアップとなるため、XR\_A(センター1)より低い優先度「50」

VRRP サービスを起動します。

## 拠点ルータ(XR\_B)

ポイント

XR\_A(センター1)と IPsec 接続するための設定を行います。 WAN 側 IP アドレスが動的 IP のため、アグレッシブモードを使用します。 PPP のマルチセッションの設定を行い、ISDN のオンデマンド接続を行える状態に設定します。 WAN 側の回線断等で IPsec KeepAlive による障害が検出された場合、ISDN 側のルートが有効になり、 XR\_A2(センター2)に対して ISDN による発信を行います。

## 〈〈インタフェース設定〉〉

[Ethernet0の設定]

固定アド	レスで使用	
IP アチ レ ス	192.168.20.1	
ネットマスク	255.255.255.0	
MTU	1500	

Ethernet0 に関する設定をします。

※IPアドレスの設定を変更した場合、その設定した IPアドレスが即反映されます。

[Ethernet1の設定]

<ul> <li>固定アド</li> </ul>	●固定アドレスで使用			
IPアドレス	0			
ネットマスク	255.255.255.0			
MTU	1500			

Ethernet1に関する設定をします。 PPPoE接続で使用するため、IPアドレスに「0」を設定しています。

#### <<PPP/PPPoE 設定>>

### [接続先設定1]

д- ĦD	test2@centurysys	
パスワード	test2pass	

PPPoE 接続で使用するユーザ ID,パスワードを登録します。

[接続先設定2]

ユーザロ	isdntest	]
パスワード	isdnpass	

PPP(ISDN)接続で使用するユーザ ID, パスワードを登録します。

BRI/PPPシリアル回鉄使用時に設定して下さい					
電話番号	XR_A-123				

センタールータ(XR\_A2)の電話番号を登録します。

BRI/PPPシリアル回線使用時に設定して下さい				
ON-DEMAND接続用 切断タイマー	60 <b>≱</b> y			

※この例では ISDN の ON-DEMAND 接続を利用するため、ON-DEMAND 接続用切断タイマーを設定します。 デフォルト値は「180 秒」になります。ご利用環境によって適宜設定を変更して下さい。 [接続設定]

接続先の選択	●接號先1 ●接読先2 ●接號先3 ●接號先4 ●接読先5
接続ポート	O Ether0 • Ether1 • Ether2 • ERI(64K) • ERI MP(128K) • RS2320
接統形態	○ 手動接続 ○ 常時接続 ○ スケジューラ接続
RS232C/BRI接続タイプ	<ul> <li>● 通常</li> <li>● On-Demand接続</li> </ul>
IPマスカレード	○無効 ● 有効
ステートフルパケット インスペウション	○無効 ○有効 □DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ● 有効

PPPoE 接続するインタフェース、および接続形態を選択します。 ※この例では、ルータ経由でのインターネットアクセスも可能になっています。

⋜ルĴ₽₽	マルチPPP/PPPoEセッション機能を利用する際は以下を設定して下さい					
マルチ接続 #2	○無効 ⊙有効					
接続先の選択	○接統先1 ◎接統先2 ○接統先3 ○接統先4 ○接統先5					
接続ボート	O Ether0 O Ether1 O Ether2 O BRI(54K) O BRI MP(128K) O RS232C					
RS232C/BRI接続タイプ	○ 通常 ● On-Demand接続					
ドマスカレード	⊙ 無効 ○ 有効					
ステートフルバケット インスペウション	● 無効 ○ 有効 □ DROP したパケットのLOGを取得					

マルチ接続側(ISDN側)の接続先,接続ポートおよび接続タイプを設定します。

✓回線接続時に前回のPPPoEセッションのPADTを強制送出 PPPoE特殊オプション (全回線共通) ✓非接続SessionのIPv4Packet受信時IIPADTを強制送出 ✓ 非接続SessionのLCP-EchoRequest受信時Ⅰ\_PADTを強制送出

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定しています。

#### <<フィルタ設定>>

[入力フィルタ]

インターフェー ス	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
рррО	パケット受信時	許可 🚩	udp 💌		500		500	
рррО	パケット受信時	許可 🔽	esp 💌					

IKE パケット, ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

### <<各種サービスの設定>>

<IPsec サーバ>

[本装置側の設定1]

インターフェースのIPアドレス	%рррО	
上位ルータのIPアドレス		
インターフェー スのID	@ipsec1	(例:@xr.centurysys)

PPPoE 接続で WAN 側(ppp0)インタフェースの IP アドレスが不定のため「%ppp0」, インタフェースの ID として「@ipsec1」を設定します。

[IKE/ISAKMPの設定1]

IKE/ISAKMPポリシー名	XRA
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Ю	(柳:@va.centurysys)
モードの設定	aggressive モード 💌
	1番目 group2-aes128-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)

XR\_A(センター1)に対する IKE/ISAKMP ポリシーを設定します。

鍵の設定	
<ul> <li>PSKを使用する</li> <li>RSAを使用する</li> <li>(X500を使用する場合は RSAに設定してください)</li> </ul>	ipseckey1

事前共有鍵(PSK)として「ipseckey1」を設定しています。

[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-Dermandで使用する

XR\_A(センター1)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

使用するIKEポリシー名の選択	XR_A (1KE1) 💌
本装置側のL4N側のネットワークアドレス	192.168.20.0/24 (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 (第1:192.168.0.0/24)
FH2のTransFormの選択	aes128-sha1 💌
PFS	<ul> <li>● 使用する</li> <li>● 使用しない</li> </ul>
DH Groupの選択(PFS使用時に有効)	group2
SADライフタイム	28800 彩 (1081~86400秒まで)
DISTANCE	1 (1~255まで)

XR\_A(センター1)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

[IPsec Keep-Alive 設定]

enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1 <u>米</u>	動作option 2 <u>米</u>	interface	backup SA
	192.168.20.1	192.168.10.1	45	3	60			ipsec0 💌	

XR\_A(センター1)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

IPsecサーバ	○停止	⊙起動	

IPsec サーバ機能を起動します。

### <<スタティックルート設定>>

アドレス	ネットマスク	インターフェー	- ス/ゲートウェイ	ディスタンス (1-255>
192.168.10.0	255.255.255.0	ppp2		10

IPsec 接続していないときに、センター方向へのルートを ISDN 側へフローティングさせるために、スタ ティックルートの設定を行います。

この例では、IPsec 接続しているときは、IPsec ルートのディスタンス値(=1)の方がスタティックルート のディスタンス値(=10)より小さいため、IPsec ルートが有効になっているときは、このスタティックル ートは無効の状態になっています。

また ISDN 側は「ppp2」 インタフェースとなるため、インタフェースの項目に「ppp2」を設定しています。

# 11. ISDN を利用した回線バックアップ例その3(メイン回線 IPsec)

この例は、PPPoE で IPsec 接続しているメイン回線で障害が発生したときに、拠点側からの ISDN による バックアップを実現する設定例です。

またセンターメインルータの機器障害や VRRP の状態変化を検出した場合でも、VRRP, Netevent 機能との組み合わせによりバックアップ経路を利用できる設定になっています。

# 11-1. 構成例



# 11-2. 要件

- ▶ インタフェースおよび PPP/PPPoE
  - インターネットに PPPoE で接続します。
  - PPPoE 接続は、自動再接続するように設定しています。
  - WAN 側インタフェースの IP マスカレード、ステートフルパケットインスペクションは「有効」にしています。
  - XR\_B(拠点)はマルチ回線で ISDN オンデマンド接続をします。
  - XR\_A2(センター2)ではアクセスサーバ機能を使用し、XR\_B(拠点)からのダイアルアッ プ接続を受け付けます。

主なインタフェースおよび PPP/PPPoE のパラメータ

	XR_A(センター1)	XR_A2(センター2)	XR_B(拠点)
LAN 側インタフェース	Ether0	Ether0	Ether0
LAN 側 IP アドレス	192. 168. 10. 1	192. 168. 10. 2	192. 168. 20. 1
WAN 側インタフェース	Ether1[ppp0]	-	Ether1[ppp0]
WAN 側 IP アドレス	10. 10. 10. 1	-	動的 IP
PPPoE ユーザ名	test1@centurysys	_	test2@centurysys
PPPoE パスワード	test1pass	_	test2pass
WAN 側接続回線	PPPoE 接続	-	PPPoE 接続
ISDN 番号	_	XR_A-123	XR_B-123
ISDN ユーザ名	_	_	isdntest
ISDN パスワード	-	-	isdnpass
ISDN 側 IP アドレス	_	192. 168. 110. 1	192. 168. 120. 1

≻ VRRP

- Ether0 側で VRRP を使用しています。
- 優先度は XR\_A(センター1)「100」, XR\_A2(センター2)「50」に設定しています。

主な VRRP のパラメータ

	XR_A(センター1)	XR_A2(センター2)
使用するインターフェース	Ether0	Ether0
ルータ ID	51	51
優先度	100	50
IP アドレス	IP アドレス 192. 168. 10. 100	

### ≻ IPsec

- 鍵交換モードはアグレッシブモードを使用しています。
- XR\_A(センター1)は 192.168.10.0/24 <-> 192.168.20.0/24 の時に IPsec を適用しま す。
- XR\_B(拠点)は192.168.20.0/24 <-> 192.168.10.0/24 の時に IPsec を適用します。
- IPsec KeepAlive は XR\_A(センター1)が動作オプション1で、XR\_B(拠点)が動作オプション2で使用しています。

本装置側のパラメータ

	XR_A(センター1)	XR_B(拠点)
インタフェースの IP アドレス	10. 10. 10. 1	%ppp0
上位ルータの IP アドレス	%ppp0	
インタフェースの ID		@ipsec1

	XR_A(センター1)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター1)
IKE/ISAKMP ポリシー名	XR_B	XR_A
リモート IP アドレス	0. 0. 0. 0	10. 10. 10. 1
インタフェースの ID	@ipsec1	
モード	Aggressive	Aggressive
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
DH グループ	Group2	Group2
ライフタイム	3600(秒)	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey1	ipseckey1

IKE/ISAKMP ポリシーのパラメータ「XR\_A(センター1), XR\_B(拠点)」

IPsec ポリシーのパラメータ(1) 「XR\_A(センター1), XR\_B(拠点)」

	XR_A(センター1)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター1)
使用する IKE ポリシー名	XR_B(IKE1)	XR_A(IKE1)
本装置の LAN 側のネットワークアドレス	192.168.10.0/24	192.168.20.0/24
相手側の LAN 側のネットワークアドレス	192. 168. 20. 0/24	192.168.10.0/24
暗号化アルゴリズム	AES-128	AES-128
認証アルゴリズム	SHA1	SHA1
PFS (DH グループ)	使用する(Group2)	使用する(Group2)
ライフタイム	28800(秒)	28800(秒)
DISTANCE	1	1

	XR_A(センター1)	XR_B(拠点)		
対向拠点	XR_B(拠点)	XR_A(センター1)		
Policy No.	1	1		
source address	192. 168. 10. 1	192. 168. 20. 1		
destination address	192. 168. 20. 1	192. 168. 10. 1		
interval(sec)	30	45		
watch count	3	3		
timeout/delay(sec)	60	60		
動作option	1	2		
interface	ipsec0 ipsec0			

IPsec Keepalive のパラメータ 「XR\_A(センター1), XR\_B(拠点)」

### ▶ その他

- XR\_A(センター1)では IPsec トンネルで障害が発生したときに、拠点方向へのルート を XR\_A2(センター2)に切り替えるためのスタティックルートを設定しています。 また VRRP の状態がマスタから変化したとき、Netevent 機能により IPsec を切断しま す。
- XR\_A2(センター2)では ISDN 接続していないときに拠点方向へのルートを XR\_A(セン ター1)へ切り替えるためのスタティックルートを設定しています。
- XR\_B(拠点)では IPsec トンネルで障害が発生したときにセンター側へのルートを ISDN に切り替えるためのルートを設定しています。

## 11-3. 設定例

## センタールータ1(XR\_A)

### ポイント

拠点と IPsec 接続するための設定を行います。

拠点が動的 IP のため、アグレッシブモードを使用します。

WAN 側の回線断等で IPsec KeepAlive による障害が検出された場合、XR\_A2(センター2)へのルーティン グを有効にします。

XR\_Aの機器障害が発生した場合に備えて、XR\_A2(センター2)とのVRRPで冗長化を行っています。

XR\_AのVRRPをトリガに IPsecを接続切断する Netevent 機能の設定を行っています。

「ISDN を利用した回線バックアップ例その2」の「センタールータ1(XR\_A)」の設定に下記の設定を追加することにより、この例のセンタールータ1(XR\_A)の設定条件を満たします。

## <<ネットワークイベント機能>>

[VRRP 監視の設定]

ND	enable	トリガー番号	インターバル	いって	VRRP ルータID
1		1	10	3	51

監視する VRRP のルータ ID を指定します。 これがトリガとなります。

[IPsec 接続切断設定]

NO	iD IPSECポリシー番号。 又はインターフェース名		使用IKE連動機能		使用interface連動機能	
1	ipsec0		使用しない	~	使用する	*

VRRPの状態変化が発生したときのイベント(この例では IPsec)を設定します。

IPsec のインタフェースを指定することにより、このインタフェースで接続している全ての IPsec は切断されます。トリガ復旧時には再度 IPsec 接続されます。

```
[イベント実行テーブル設定]
```

ND 実行イベナ設定 オブション設定 1 IPSECポリシー V 1

実行されるイベントとして IPsec を選択します。

その時の動作は「IPsec 接続切断設定」で設定した動作になります。

[ネットワークイベント設定]

トリガー番号	実行イベントテーブル番号
1	1

「トリガ番号」は、この例では「VRRP 監視の設定」で指定した番号を、「実行イベントテーブル番号」 は「イベント実行テーブル設定」を設定します。

[ネットワークイベントサービス設定]

<u>ネットワークイベント</u>	○ 停止 ⊙ 起動
<u>ping監視</u>	⊙ 停止 ○ 起動
<u>link監視</u>	④ 停止 🔘 起動
<u>vmp監視</u>	○ 停止 ⊙ 起動

この設定例では、「ネットワークイベント」と「VRRP 監視」を使用しますので、この二つを起動します。
# センタールータ 2(XR\_A2)

### ポイント

「ISDN を利用した回線バックアップ例その2」のセンタールータ2(XR\_A2)と同じ設定です。 (設定省略)

# 拠点ルータ(XR\_B)

## ポイント

「ISDN を利用した回線バックアップ例その2」の拠点ルータ(XR\_B)と同じ設定です。 (設定省略)

FutureNet XR シリーズ インターネット VPN 設定例集

#### IPsec 編

## 2007年3月

発行 センチュリー・システムズ株式会社 2006-2007 CENTURYSYSTEMS INC.ALL rights reserved.