FutureNet XR シリーズ

設定例集

Ver 1.2.0



※上記写真は XR-540/C です。

センチュリー・システムズ株式会社



目次

目次	2
はじめに	6
改版履歴	7
1. インタフェース設定	
1-1. ローカルルータ設定	
1-1-1. 構成図	
1-1-2. 設定例	
1-2. DHCP クライアント設定	
1-2-1. 構成図	
1-2-2. 設定例	
1-3. フリッシ設定	
1-3-1. 構成凶	
1-3-2. 設定例	13
2. PPPoE 設定	14
2-1. 端末型接続設定	
2-1-1. 構成図	
2-1-2. 設定例	
2-2. LAN 型接続設定	
2-2-1. 構成図	
2-2-2. 設定例	
2-3. マルチセッション接続設定	
2-3-1. 構成図	
2-3-2. 設定例	
2-4. マルチホーミング設定	
2-4-1. 構成図	
2-4-2. 設定例	
3. NAT 設定	
	20
3-1. IP マスカレート設定	
3-1-1. 傅成图	
<i>3-1-2. </i>	
5-2. 还旧元 NAI 政化	
5-2-1. (押以凶)	
<i>3⁻2⁻2. </i>	
3-3. ハーナヤルサーハ設正	
3-3-1. 蒨灰凶	34

目次

3-3-2. 設定例	35
4. フィルタ設定	37
4-1. 入力フィルタ設定	37
4-1-1. 構成図	37
4-1-2. 設定例	38
4-2. 転送フィルタ設定	40
4-2-1. 構成図	40
<i>4-2-2. 設定例</i>	41
4-3. ステートフルパケットインスペクション	43
4-3-1. 構成図	43
4-3-2. 設定例	44
5. NAT/フィルタ応用設定	45
5-1. NAT でのサーバ公開1(ポートマッピング)	45
5-1-1. 構成図	45
5-1-2. 設定例	46
5-2. NAT でのサーバ公開 2 (複数 IP+PPPoE)	
5-2-1. 構成図	49
5-2-2. 設定例	50
5-3. NAT でのサーバ公開 3 (複数 IP+Ether)	53
5-3-1. 構成図	53
5-3-2. 設定例	54
5-4. DMZ 構築例(PPPoE)	56
5-4-1. 構成図	56
5-4-2. 設定例	57
5-4-3. 設定例補足	60
6. ブリッジフィルタ設定	61
6-1. 同一 LAN 内でのアクセス制御	61
6-1-1. 構成図	61
6-1-2. 設定例	62
7. DHCP 設定	66
7-1.DHCP サーバ設定	
7-1-1. 構成図	
7-1-2. 設定例	
7-2.DHCP リレー設定	
7-2-1. 構成図	69
7-2-2. 設定例	70

目次

8.	攻撃検出設定	72
	8-1. アクティブファイアウォールの利用	72
	8-1-1. 構成図	72
	8-1-2. 設定例	73
	8-1-3. 設定例補足(メール送信設定)	77
9.	Web 認証設定(ゲートウェイ認証設定)	79
	9-1. ユーザ認証	79
	9-1-1. 構成図	79
	9-1-2. 設定例	80
	9-1-3. 設定例補足(ユーザ認証方法)	84
	9-2. URL 転送	85
	9-2-1. 構成図	85
	9-2-2. 設定例	86
	9-3. ユーザ強制認証+URL 転送+RADIUS 連携	89
	9-3-1. 構成図	89
	9-3-2. 設定例	90
	9-4. Web 認証機能ソリューション例(NS-430 との併用)	97
	9-4-1. 構成図	97
	9-4-2. 設定例	98
10). QoS 設定	.113
	10-1. 带域制限	.113
	10-1-1. 構成図	.113
	10-1-2. 設定例	.114
	10-2. 帯域制御(簡易 QoS 設定と詳細 QoS 設定の利用)	.116
	10-2-1. 構成図	.116
	10-2-2. 設定例	.117
	10-2-3. 設定例補足(クラス階層図)	125
	10-3. PPPoE での帯域制御+優先制御	126
	10-3-1. 構成図	126
	10-3-2. 設定例	127
	10-3-3. 設定例補足(クラス階層図)	143
11	. ソースルート設定	144
	11-1. PPPoE でのソースルートの利用	144
	11-1-1. 構成図	144
	11-1-2. 設定例	145
	11-2. Ether でのソースルートの利用	148

11-2-1. 構成図	148
11-2-2. 設定例	149
12. BGP4 設定1	.51
12-1. ネットワークイベント機能 BGP4 切断監視の利用1	51
12-1-1. 構成図	151
12-1-2. 設定例	152
13. URL フィルタ設定1	.61
13-1. URL フィルタの利用1	.61
13-1-1. 構成図	161
13-1-2. 設定例	162
13-1-3. 設定例補足1 (ルールセット設定における IP アドレス範囲指定)	166
13-1-4. 設定例補足2(ライセンス認証とフィルタによる遮断)	170
13-1-5. 設定例補足3(URL フィルタのログ)1	!71
14. サポートデスクへのお問い合わせ1	.72
14-1. サポートデスクへのお問い合わせに関して1	72
14-2. サポートデスクのご利用に関して1	.72

はじめに

- FutureNet はセンチュリー・システムズ株式会社の登録商標です。
- 本書に記載されている会社名,製品名は、各社の商標および登録商標です。
- 本ガイドは、以下のFutureNet XR 製品に対応しております。
 - XR-510/C
 - XR-540/C
 - XR-730/C
 - ・ XR-1100 シリーズ

※一部設定内容によっては上記機種以外での設定も可能です。詳しくは各製品のユーザーズ ガイドをご参照下さい。

- 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 FutureNet XR シリーズ XR-540/C Ver3.5.2(URL フィルタおよび BGP4 のみ Ver3.6.0)をベースに作成しております。各種機能において、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
1.0.0	初版
1.1.0	ブリッジフィルタ,DHCP,攻撃検出,Web 認証,QoS 設定例追加
1.2.0	ソースルート, URL フィルタ, BGP4(切断監視)設定例追加

1. インタフェース設定

1-1. ローカルルータ設定

LAN A「192.168.10.0/24」とLAN B「192.168.20.0/24」のネットワークを接続し、通信するための設定 をします。

1-1-1. 構成図



LAN A: 192.168.10.0/24

LAN B : 192.168.20.0/24

1-1-2. 設定例

インタフェース設定でそれぞれのネットワークに属する IP アドレスをルータに設定します。 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。

<<インタフェース設定>>

[Ethernet0の設定]

IPアドレスに「192.168.10.1」を設定します。

◎固定アド	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
	ーバから取得
ホ가名	
мартрия	2
IPマス (この)?	カレード(ip masq) ボートで使用するIPアドレスに変換して通信を行います)
27-	トフルパケットインスペクション(spi)
s	PI で DROP したパケットのLOGを取得
proxy :	arp
Directe	ed Broadcast

[Ethernet1の設定]

IPアドレスに「192.168.20.1」を設定します。

⊙ 固定アド	レスで使用
IPアドレス	192.168.20.1
ネットマスク	255.255.255.0
мти	1500
ODHOPH	ーバから取得
ホスト名	
маорк ир	2
IPマス (この)	カレード(ip masq) ドートで使用するIPアドレスII変換して通信を行います)
27-	トフルパケットインスペクション(spi)
□ s	PI で DROP したパケットのLOGを取得
proxy :	arp
Directo	ed Broadcast

1-2. DHCP クライアント設定

CATV など IP アドレスを DHCP にて払い出される場合には、DHCP クライアントの設定を行います。

1-2-1. 構成図



1-2-2. 設定例

本設定例ではEther1インタフェースをDHCPクライアントとして利用するための設定を行っています。

<<インタフェース設定>>

[Ethernet0の設定]

IPアドレスに「192.168.10.1」を設定します。

⊙固定アド	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
	ーバから取得
ホ가名	
MACTELS	2
IPマス (この)?	カレード(ip masq) ボートで使用するIPアドレスに変換して通信を行います)
27-	トフルパケットインスペクション(spi)
□ s	PI で DROP したパケットのLOGを取得
proxy :	qrp
Directe	ed Broadcast

[Ethernet1の設定]

「DHCP サーバから取得」を選択します。

※ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設 定しています。

〇固定アト	レスで使用
IPアドレス	0
ネットマスク	255.255.255.0
MTU	1500
	ーバから取得
ホ가名	
MACTELS	2
■ IPマス (この)	カレード(ip masq) ドートで使用するIPアドレスに変換して通信を行います)
27-	トフルパケットインスペウション(spi)
□s	PI で DROP したパケットのLOGを取得
proxy	arp
Directo	ed Broadcast

1-3. ブリッジ設定

2 つ以上の Ethernet インタフェース,また VLAN インタフェースをブリッジ設定することが可能です。ブ リッジフィルタ設定と組み合わせることで、同一 LAN の特定エリアを分離し、フィルタリングによる制 御を行うことも可能です。

1-3-1. 構成図



LAN : 192.168.10.0/24

1-3-2. 設定例

本設定例では二つの同一ネットワークを接続するための設定を行っています。

<<インタフェース設定>>

[Bridge の設定]

ブリッジインタフェースのインタフェース番号を設定します。

本設定例では、Ehernet0とEthernet1でブリッジを設定します。

基本設定		
インターフェース名	br <mark>0 [0-4095]</mark>	☑ _{有効}
Interface 設定		
 ✓ Ethernet0 ● 使用する ● VLAVを使用する VLAND 	Ethernet1	Ethernet2

IPアドレスに「192.168.10.1」,ネットマスクに「255.255.255.0」を設定します。

Network 設定		
・ 固定アドレスで	で使用	
IPアドレス	192.168.10.1	
ネットマスク	255.255.255.0	
мти	1500	
	から取得	
ホスト名		
 IPマスカレード(このボートで使用す) 	ĵp masq) するIPアドレスに変換して通信を	行います)
コステートフルバ	ケットインスペクション(spi)	
	DP したパケットのLOGを取得	
proxy arp		
	Mask Requestに応答	

2. PPPoE 設定

2-1. 端末型接続設定

フレッツ ADSL やBフレッツなど PPPoE 接続を必要とする環境で、IP アドレスを1 つ利用できるサービ スで利用可能な設定です。

2-1-1. 構成図



2-1-2. 設定例

PPPoE 接続に必要な設定を行います。

<<インタフェース設定>>

[Ethernet0の設定]

IPアドレスに「192.168.10.1」を設定します。

⊙固定アト	レスで使用
IPアドレス	192.168.10.1
ネットマスク	255.255.255.0
мти	1500
	ーバから取得
ホ가名	
марти	2
	カレード(ip masq) ボートで使用するIPアドレスに変換してim信を行います) トフル・ボルト クロマクロション (col)
	FT で DROP したパケットのLOGを取得
proxy	arp
Directo	ed Broadcast

[Ethernet1の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※PPPoE で接続する場合には "ppp" という論理インタフェースを自動的に生成し、この論理インタフェースを使って PPPoE 接続を行います。

● 固定アト	レスで使用
IPアドレス	0
ネットマスク	255.255.255.0
мти	1500
ODHOPH	ーバから取得
ホ가名	
мартия	2
□ IPマス (この)	カレード(ip masq) ドートで使用するIPアドレスに変換して通信を行います)
27-	トフルパケットインスペウション(spi)
□s	PI で DROP したパケットのLOGを取得
proxy	arp
Direct:	ed Broadcast

<<PPP/PPPoE 設定>>

[接続先設定]

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

ユーザロ	test1@centurysys
パスワード	test1pass

[接続設定]

本設定例では、ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」 にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有 効」に設定します。

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	OEther0 OEther1 OEther2 OBRI(64K) OBRI MP(128K) OLeased Line(64K) OLeased Line(128K) ORS232C
接統形態	○ 手動接続 ● 常時接続 ○ スケジューラ接続
RS2320/BRI接続タイプ	 ● 通常 ○ On-Demand接続
IPマスカレード	○無効 ⊙有効
ステートフルパケット インスペクション	○ 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の再接続性を高めるために、PPPoE 特殊オプションを設定します。

PPPoE特殊オプション (全回線共通)	 ✓ 回線接続時に前回のPPPcE セッションのPADTを強制送出 ✓ 非接続SessionのIPv4Packet受信時[JPADTを強制送出
	些 非接続SessionのLOP-EchoRequest受信時↓□PADTを強制送出

接続が完了した場合、回線状態が以下のように表示されます。

鼻で接続しています

2-2. LAN 型接続設定

フレッツ ADSL やBフレッツなど PPPoE 接続を必要とする環境で、IP アドレスを複数利用可能な場合、 ルータの LAN 側にもグローバル IP アドレスを割り当てることができます。

またこの接続は Unnumbered 接続とも呼ばれています。

2-2-1. 構成図



2-2-2. 設定例

PPPoE 接続に必要な設定を行い、LAN 側にもグローバル IP アドレス"10.10.10.0/29"を利用可能にする ための設定を行います。

<<インタフェース設定>>

[Ethernet0の設定]

IPアドレスに「10.10.10.1」,ネットマスクに「255.255.255.248」を設定します。

◎固定アド	レスで使用
IPアドレス	10.10.10.1
ネットマスク	255.255.255.248
MTU	1500
	ーバから取得
ホオ名	
MACTELS	2
IPマス (この)	カレード(ip masq) ボートで使用するIPアドレスに変換して通信を行います)
77-	トフルパケットインスペウション(spi)
□ si	PI で DROP したパケットのLOGを取得
proxy	arp
Directo	ed Broadcast

[Ethernet1の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※PPPoE で接続する場合には "ppp" という論理インタフェースを自動的に生成し、この論理インタフェ ースを使って PPPoE 接続を行います。

● 固定アト	ドレスで使用	
IPアドレス	0	
ネットマスク	255.255.255.0	
MTU	1500	
	ナーバから取得	
ホスト名		
мартрия	z	
□ IPマス (この)?	カレード(ip masq) 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)
77-	トフルパケットインスペクション(spi)	
□ s	PI で DROP したパケットのLOGを取得	9
proxy	arp	
Direct:	ed Broadcast	

<<PPP/PPPoE 設定>>

[接続先設定]

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

ユーザロ	test1@centurysys
パスワード	test1pass

ppp インタフェースに割り当てる IP アドレス「10.10.10.1」を設定します。

	UnNumbered-PPP回绕使用時に	設定できます
IP761.7	10.10.10.1	
Prux	回線接続時に割り付けるグロ・	- バルPアドレスです

[接続設定]

本設定例では、IPマスカレードを「無効」にし、WANからのパケットをフィルタリングしないためにス テートフルパケットインスペクションを「無効」に設定します。

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 EFR(64K) O EFRI MP(128K) O Leased Line(64K) O Leased Line(128K) O R52320
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	 ● 通常 ○ On-Demand接続
₽マスカレード	⊙ 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
デフォルトルートの設定	○無効 ⊙有効

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ます。

PPPoE特殊オプション (全回線共通)	 ✓ 回線接続時に前回のPPPcE セッションのPADTを強制送出 ✓ 非接続SessionのJPv4Packet受信時しアADTを強制送出 ✓ 非接続SessionのLCP-EchoRequest受信時しアADTを強制送出 	
-------------------------	---	--

接続が完了した場合、回線状態が以下のように表示されます。



2-3. マルチセッション接続設定

Bフレッツなどでは同時に複数の PPPoE 接続を行うことが可能です。これにより複数のプロバイダに接続して利用することも可能です。

2-3-1. 構成図



2-3-2. 設定例

PPPoE 接続(主回線,マルチ回線)に必要な設定を行います。 また宛先 IP アドレスが「10.100.0.0/24」の時には、マルチ回線を利用し、それ以外の宛先 IP アドレス に対しては主回線を利用するように設定しています。

<<インタフェース設定>>

[Ethernet0 の設定]

IPアドレスに「192.168.10.1」を設定します。

⊙固定アト	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
	ーバから取得
ホスト名	
MACTELS	2
IPマス (この)	カレード(ip masq) ボートで使用するIPアドレスに変換して通信を行います)
77-	トフルパケットインスペクション(spi)
□s	PI で DROP したパケットのLOGを取得
proxy	anp
Directi	ed Broadcast

[Ethernet1 の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※PPPoE で接続する場合には "ppp" という論理インタフェースを自動的に生成し、この論理インタフェ ースを使って PPPoE 接続を行います。

⑧ 固定アト	レスで使用
IPアドレス	0
ネットマスク	255.255.255.0
MTU	1500
	ーパから取得
ホスト名	
мартир	2
(20)	カレード(ip masq) ボートで使用するIPアドレスII変換して通信を行います) トコリッチャート
	トフルハケザイフスペシション(Spl) PI で DROP したパケットのLOGを取得
proxy	arp
Direct:	ed Broadcast

<<PPP/PPPoE 設定>>

[接続先設定1]

PPPoE 接続(主回線)で使用するユーザ ID とパスワードを設定します。

ユーザロ	test1@centurysys
パスワード	test1pass

[接続先設定2]

PPPoE 接続(マルチ回線#2)で使用するユーザ ID とパスワードを設定します。

ユーザロ	test@example.com
パスワード	testpass

[接続設定]

PPPoE(主回線)に関する設定をします。

本設定例では、ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」 にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有 効」に設定します。

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 Leased Line(64K) O Leased Line(128K) O RS2320
接統形態	○ 手動接続 ○ 常時接続 ○ スケジューラ接続
RS2320/BRI接続タイプ	 ● 通常 ○ On-Demand接続
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 (マルチ接続#2) に関する設定をします。

本設定例では、ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」 にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有 効」に設定します。

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	OEther0 OEther1 OEther2 OBRI(64K) OBRI MP(128K) OLeased Line(64K) OLeased Line(128K) OR5232C
RS232C/BRI接続タイプ	 ● 通常 ○ On-Demand接続
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

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ます。

PPP∞E特殊オプション (全回線共通) ▼	回線接続時に前回のPPPcEセッションのPADTを強制送出 非接続SessionのIPv4Packet受信時 IPADTを強制送出 非接続SessionのLOP-EchoRequest受信時 IPADTを強制送出
---------------------------	--

接続が完了した場合、回線状態が以下のように表示されます。

回線状態 主回線で接続しています マルチ接続 #2で接続しています

<<スタティックルート設定>>

宛先 IP アドレスが「10.100.0.0/24」の時には、マルチ回線を利用するための設定をします。

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>
10.100.0.0	255.255.255.0	ppp2		1

2-4. マルチホーミング設定

PPP/PPPoE 接続の主回線とマルチ回線によるロードバランシング(マルチホーミング)を行うことが可能です。通信のストリーム毎に使用する回線を振り分けます。(ストリームは送信元 IP アドレスと宛先 IP アドレスにより識別します)

※マルチホーミング機能は XR-510/C Ver3.5.0, XR-540/C Ver3.5.0 以降でのみ対応しております。

2-4-1. 構成図



2-4-2. 設定例

マルチホーミング機能を有効にし、PPPoE 接続(主回線,マルチ回線)に必要な設定を行います。 またスタティックルート設定でデフォルトルートを主回線(ppp0)とマルチ回線(ppp2)で設定します。

〈〈インタフェース設定〉〉

[Ethernet0の設定]

IPアドレスに「192.168.10.1」を設定します。

③固定アト	ドレスで使用
IPアドレス	192.168.10.1
ネットマスク	255.255.255.0
мти	1500
	トーバから取得
ホスト名	
MACTELS	2
IPマス (この)?	カレード(ip masq) ボートで使用するIPアドレスII変換して通信を行います)
27-	トフルパケットインスペクション(spi)
□ s	PI で DROP したパケットのLOGを取得
proxy	arp
Direct	ed Broedcast

[Ethernet1の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※PPPoE で接続する場合には "ppp" という論理インタフェースを自動的に生成し、この論理インタフェ ースを使って PPPoE 接続を行います。

◎固定アト	シスで使用
IPアドレス	0
ネットマスク	255.255.255.0
MTU	1500
OHOPH	ナーバから取得
ホ가名	
мартия	2
IPマス (この)	カレードûp mesq) ボートで使用するIPアドレスに変換して通信を行います)
77-	トフルパケットインスペクション(spi)
□ s	PI で DROP したパケットのLOGを取得
proxy	arp
Direct:	ed Broadcast

<<システム設定>>

[マルチホーミング設定]

マルチホーミングを機能させるために「有効」を選択します。

マルチホーミング	⊙有効	○無効

<<スタティックルート設定>>

主回線 (ppp0) とマルチ回線 (ppp2) をデフォルトルートとして設定します。

アドレス	ネットマスク	インターフェー ス/ゲートウェー	イ ディスタンス <1-255>
0.0.0.0	0.0.0.0	рррО	1
0.0.0.0	0.0.0	ppp2	1

<<PPP/PPPoE 設定>>

[接続先設定1]

PPPoE 接続(主回線)で使用するユーザ ID とパスワードを設定します。

ユーザロ	test1@centurysys
パスワード	test1pass

[接続先設定2]

PPPoE 接続(マルチ回線#2)で使用するユーザ ID とパスワードを設定します。

ユーザロ	test@example.com
パスワード	testpass

[接続設定]

PPPoE(主回線)に関する設定をします。

デフォルトルートは「無効」を選択します。

本設定例では、ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」 にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有 効」に設定します。

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 Ether O Ether O Ether O BRI(54K) O BRI MP(128K) O Leased Line(54K) O Leased Line(128K) O 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	 ● 通常 ○ On-Demand接続
IPマスカレード	○無効 ◎ 有効
ステートフルパケット インスペクション	○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 (マルチ接続#2) に関する設定をします。

本設定例では、ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」 にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有 効」に設定します。

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
接続ポート	O Ether O Ether O Effi(64K) O BRI MP(128K) O Leased Line(64K) O Leased Line(128K) O RS232D
RS232C/BRI接続タイプ	 ● 通常 ○ On-Demand接続
IPマスカレード	○無効 ◎ 有効
ステートフルバケット インスペクション	○無効 ○ 有効 □ DROP したパケットのLOGを取得

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。

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

接続が完了した場合、回線状態が以下のように表示されます。

 回換状金
 主回線で接続しています マルチ接続 #2で接続しています

3. NAT 設定

3-1. IP マスカレード設定

プライベート IP アドレスのネットワーク内にある端末がインターネットへアクセスする際など、送信元 IP アドレスを IP マスカレードの設定を有効にしたインタフェースの IP アドレスに変換して通信するこ とができます。

3-1-1. 構成図



3-1-2. 設定例

送信元 IP アドレスを変換するインタフェースで IP マスカレードの設定を有効にしています。

<<インタフェース設定>>

[Ethernet0の設定]

IPアドレスに「192.168.10.1」を設定します。

固定アド	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
	ーバから取得
ホ가名	
мартир	2
IPマス (この)	カレード(ip masq) ドートで使用するIPアドレスに変換して通信を行います)
27-	トフルパケットインスペウション(spi)
S	PI で DROP したパケットのLOGを取得
proxy :	qrp
Directe	ed Broadcast

[Ethernet1の設定]

IPアドレスに「10.10.10.1」,ネットマスクに「255.255.255.252」を設定します。

ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にします。 ※WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」 に設定します。

⑧ 固定ア	レスで使用
IP アドレス	10.10.10.1
ネットマスク	255.255.255.252
мти	1500
ODHOPH	ーバから取得
ホスト名	
мартир	2
■ IPマス (この)	カレード(ip masq) ドートで使用する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)
□s	PI で DROP したパケットのLOGを取得
proxy	arp
Directo	ed Broadcast

[その他の設定]

デフォルトゲートウェイの設定	
10.10.10.2	

3-2. 送信元 NAT 設定

ある特定のネットワークやホストを指定し、送信元 IP アドレスの変換を行うことができます。例えばプ ライベート IP アドレスのある特定の端末のみ送信元 IP アドレスを変換するといった場合に利用します。

3-2-1. 構成図



3-2-2. 設定例

ある特定の端末のみ送信元 IP アドレスを変換するための設定をします。

<<インタフェース設定>>

[Ethernet0の設定]

IPアドレスに「192.168.10.1」を設定します。

⊙ 固定アド	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
	一パから取得
ホスト名	
MACTELS	2
IPマス (この)?	カレード(p masq) ボートで使用するIPアドレスII変換して通信を行います)
77-	トフルパケットインスペクション(spi)
□ s	PI で DROP したパケットのLOGを取得
proxy :	arp
Directo	ed Broadcast

[Ethernet1の設定]

IPアドレスに「10.10.10.1」,ネットマスクに「255.255.255.252」を設定します。

※WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」 に設定します。

◎固定アド	レスで使用
IPアドレス	10.10.10.1
ネットマスク	255.255.255.252
мти	1500
	ーバから取得
ホオト名	
мартир	2
IPマス (この)	カレード(ip masq) ドートで使用するIPアドレスに変換して通信を行います)
27-	トフルパケットインスペクション(spi)
□ s	PI で DROP したパケットのLOGを取得
proxy:	arp
Directo	ed Broadcast

[その他の設定]

デフォルトゲートウェイの設定	
10.10.10.2	

<<NAT 設定>>

[送信元 NAT]

LAN上にある「192.168.10.10」の端末の送信元 IP アドレスを eth1 からのパケット送信時に「10.10.1」に変換する設定をします。

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
192.168.10.10	10.10.10.1	eth1

3-3. バーチャルサーバ設定

プライベート IP アドレスのネットワーク内にあるサーバをインターネット経由でアクセスさせる場合、 バーチャルサーバ機能によりルータ経由でのアクセスが可能になります。

3-3-1. 構成図



3-3-2. 設定例

プライベート IP アドレスのネットワーク内にあるサーバをインターネットからアクセス可能にするた めの設定をします。

<<インタフェース設定>>

[Ethernet0の設定] IPアドレスに「192.168.10.1」を設定します。

⊙ 固定アド	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
	ーバから取得
ホ가名	
мартк из	2
	カレード(pinasa) ドートで使用するIPアドレスII変換して通信を行います) トフリージャルト グロスペパション (con)
	PIでDROPしたパケットのLOGを取得
proxy :	arp
Directo	ed Broadcast

[Ethernet1の設定]

IPアドレスに「10.10.10.1」,ネットマスクに「255.255.255.252」を設定します。

⊙ 固定アド	レスで使用
IPアドレス	10.10.1
ネットマスク	255.255.255.252
MTU	1500
	ーバから取得
ホ가名	
мартгия	2
IPマス (このえ)	カレード(ip masq) ドートで使用するIPアドレスに変換して通信を行います)
27-	トフルパケットインスペクション(spi)
🗆 si	PI で DROP したパケットのLOGを取得
proxy :	qte
Directe	ed Broadcast

[その他の設定]

デフォルトゲートウェイの設定	
10.10.10.2	

<<NAT 設定>>

[バーチャルサーバ]

LAN 上にある WEB サーバ, TELNET サーバをインターネットからアクセス可能にするための設定をします。 インターネットから「10.10.10.1」で TCP ポート 80 番宛てのパケットを受信した場合は、192.168.10.100 に転送します。

インターネットから「10.10.10.1」で TCP ポート 23 番宛てのパケットを受信した場合は、192.168.10.101 に転送します。

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	ポート	インターフェース
192.168.10.100	10.10.10.1	top 💌	80	eth1
192.168.10.101	10.10.10.1	tcp 💌	23	eth1
4. フィルタ設定

4-1. 入力フィルタ設定

入力フィルタでは外部からルータ宛に送信されたパケットのうち、ルータ自身で受信し処理するものを 対象とします。本設定例ではインターネットからの ICMP パケットは許可するが、Web 設定画面へのアク セス (TCP ポート 880 番) は破棄する設定です。

4-1-1. 構成図



4-1-2. 設定例

外部からの XR へのアクセスを制限します。

<<インタフェース設定>>

[Ethernet0の設定]

IPアドレスに「192.168.10.1」を設定します。

 固定アド 	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
	ーバから取得
ホスト名	
мартрия	2
	カレード(ip mesq) ドートで使用するIPアドレスに変換して通信を行います) トフルバイヤトインスペワション(coi)
	PIでDROPしたパケットのLOGを取得
proxy :	arp
Directe	ed Broadcast

[Ethernet1の設定]

IPアドレスに「10.10.10.1」,ネットマスクに「255.255.255.252」を設定します。

◎ 固定アド	レスで使用
IP アドレス	10.10.10.1
ネットマスク	255.255.255.252
MTU	1500
	ーバから取得
ホスト名	
маоряил	ξ
 IPマス) (このか) 	カレード(p masq) ドートで使用するIPアドレスII変換して通信を行います)
75-	トフルパケットインスペクション(spi)
🗆 si	PI で DROP したパケットのLOGを取得
proxy :	arp
Directe	ed Broadcast

[その他の設定]

デフォルトゲートウェイの設定	
10.10.10.2	

<<フィルタ設定>>

[入力フィルタ]

インターネット側から本装置宛の ICMP パケットを許可しています。

インターネット側から本装置宛の TCP ポート 880 番宛のパケットを破棄しています。

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	ICMP type/code	送信元MACアドレス	LOG
eth1	パケット受信時	許可 🚩	icmp 💌							
eth1	パケット受信時	破棄 💌	tcp 💌				880			

4-2. 転送フィルタ設定

転送フィルタでは本装置で内部転送(本装置がルーティング)するパケットを制御するときに利用しま す。本設定例ではバーチャルサーバでインターネットに公開している WEB サーバ, TELNET サーバに対し て WEB サーバへのアクセスは許可, TELNET サーバへは指定した IP アドレスからのアクセスのみ許可し、 その他からの TELNET アクセスは破棄する設定です。

4-2-1. 構成図



4-2-2. 設定例

ルータを経由するパケットに対してアクセス制限を行います。

〈〈インタフェース設定〉〉

[Ethernet0の設定]

IPアドレスに「192.168.10.1」を設定します。

●固定アド	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
	ーバから取得
ホスト名	
мартрия	2
IPマズ (この)	カレード(ip masq) ドートで使用するIPアドレスに変換して通信を行います)
27-	トフルパケットインスペクション(spi)
🗆 si	PI で DROP したパケットのLOGを取得
proxy :	arp
Directe	ed Broadcast

[Ethernet1の設定]

IPアドレスに「10.10.10.1」,ネットマスクに「255.255.255.252」を設定します。

● 固定アド	レスで使用
IPアドレス	10.10.10.1
ネットマスク	255.255.255.252
мти	1500
	ーバから取得
ホスト名	
маоряии	ξ
 IPマス) (このか) 	カレード(ip masq) ドートで使用するIPアドレスに変換して通信を行います)
27-	トフルパケットインスペクション(spi)
🗆 si	PI で DROP したパケットのLOGを取得
proxy :	que
Directe	ed Broadcast

[その他の設定]

デフォルトゲートウェイの設定	
10 10 10 2	

<<NAT 設定>>

[バーチャルサーバ]

LAN 上にある WEB サーバ, TELNET サーバをインターネットからアクセス可能にするための設定をします。 インターネットから「10.10.10.1」で TCP ポート 80 番宛てのパケットを受信した場合は、 「192.168.10.100」に転送します。

インターネットから「10.10.10.1」で TCP ポート 23 番宛てのパケットを受信した場合は、 「192.168.10.101」に転送します。

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
192.168.10.100	10.10.10.1	tcp 💌	80	eth1
192.168.10.101	10.10.10.1	top 💌	23	eth1

<<フィルタ設定>>

[転送フィルタ]

LAN 上にある WEB サーバ, TELNET サーバをインターネットからアクセス可能にするための設定をします。 インターネットからの WEB サーバ (TCP ポート 80 番) 宛のパケットを許可しています。

インターネットから送信元 IP アドレス「10.20.10.1」で TELNET サーバ (TCP ポート 23 番) 宛のパケットを許可しています。

インターネットから送信元 IP アドレス「10.20.10.1」以外の TELNET サーバ(TCP ポート 23 番) 宛のパ ケットを破棄しています。

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	ICMP type/code	送信元MACアドレス
eth1	パケット受信時 ⊻	許可 💌	tcp 💌				80		
eth1	パケット受信時 💌	許可 💌	tcp 💌	10.20.10.1			23		
eth1	パケット受信時 💌	破棄 💌	tcp 💌				23		

4-3. ステートフルパケットインスペクション

ステートフルパケットインスペクションは、パケットを監視してパケットフィルタリング項目を随時変 更する機能で、動的パケットフィルタリングともいわれる機能です。

4-3-1. 構成図



4-3-2. 設定例

<<インタフェース設定>>

[Ethernet0の設定]

IPアドレスに「192.168.10.1」を設定します。

◎固定アド	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
ODHOPH	ーバから取得
ホスト名	
маорк ир	4
IPマズ (この)	カレード(ip masq) ドートで使用するIPアドレスII変換して通信を行います)
27-	トフルパケットインスペクション(spi)
🗆 si	PI で DROP したパケットのLOGを取得
proxy :	qte
Directe	ed Broadcast

[Ethernet1の設定]

IP アドレスに「10.10.10.1」, ネットマスクに「255.255.255.252」を設定します。

WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に 設定します。

※ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にしています。

固定7	ドレスで使用
IPアドレス	, 10.10.10.1
ネットマス	255.255.255.252
MTU	1500
ODHOP	サーバから取得
ホオ名	
маорғ и	z
	スカレード(ip masq))ボートで使用するIPアドレスに変換して通信を行います)
✓ 75	ートフルパケットインスペクション(spi)
	SPI で DROP したパケットのLOGを取得
prox	/ arp
Direc	ted Broadcast

[その他の設定]

デフォルトゲートウェイの設定	
10.10.10.2	

5. NAT/フィルタ応用設定

5-1. NAT でのサーバ公開1 (ポートマッピング)

バーチャルサーバ設定例では変換前後のポート番号は同じでしたが、変換前後のポート番号を指定する ことにより、下記例のように複数のWEBサーバに対してのアクセスが可能になります。

5-1-1. 構成図



5-1-2. 設定例

グローバル IP アドレス「10.10.10.1」の TCP ポート 80 番宛てのパケットを受信した場合は、「192.168.10.100」 TCP ポート 80 番に、「10.10.1」で TCP ポート 8080 番宛てのパケットを受信した場合は、「192.168.10.101 」 TCP ポート 80 番に NAT 変換します。

〈〈インタフェース設定〉〉

[Ethernet0の設定]

IPアドレスに「192.168.10.1」を設定します。

⊙固定アト	レスで使用
IPアドレス	192.168.10.1
ネットマスク	255.255.255.0
мти	1500
	ーパから取得
ホスト名	
MACTELS	2
IPマス (この)	カレード(ip masq) ボートで使用するIPアドレスに変換して通信を行います)
27-	トフルパケットインスペウション(spi)
□s	PI で DROP したパケットのLOGを取得
proxy	arp
Direct:	ed Broadcast

[Ethernet1の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※PPPoE で接続する場合には "ppp" という論理インタフェースを自動的に生成し、この論理インタフェ ースを使って PPPoE 接続を行います。

◎固定アト	シスで使用
IPアドレス	0
ネットマスク	255.255.255.0
MTU	1500
OHOPH	ナーバから取得
ホ가名	
мартия	2
IPマス (この)	カレードûp mesq) ボートで使用するIPアドレスに変換して通信を行います)
77-	トフルパケットインスペクション(spi)
□ s	PI で DROP したパケットのLOGを取得
proxy	arp
Direct:	ed Broadcast

<<PPP/PPPoE 設定>>

[接続先設定]

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

ユーザロ	test1@centurysys
パスワード	test1pass

[接続設定]

ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

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 Ether O Ether O Ether O BRI(64K) O BRI MP(128K) O Leased Line(64K) O Leased Line(128K) O RS232C
接続形態	○ 手動接続 ● 常時接続 ○ スケジューラ接続
RS2320/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の再接続性を高めるために、PPPoE 特殊オプションを設定します。

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

接続が完了した場合、回線状態が以下のように表示されます。

回換状 差 主回換で接続しています

<<フィルタ設定>>

[転送フィルタ]

LAN 上にある WEB サーバ1, 2をインターネットからアクセス可能にするための設定をします。

インターネットから宛先 IP アドレス「192.168.10.100」で WEB サーバ1 (TCP ポート 80 番) 宛のパケ ットを許可します。

インターネットから宛先 IP アドレス「192.168.10.101」で WEB サーバ2 (TCP ポート 80 番) 宛のパケ ットを許可します。

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	ICMP type/code	送信元MACアドレス	LOG
рррО	パケット受信時 ⊻	許可 💌	top 💌			192.168.10.100	80			
рррО	パケット受信時 ⊻	許可 💌	tcp 💌			192.168.10.101	80			

<<NAT 設定>>

[バーチャルサーバ]

LAN 上にある WEB サーバ1, 2 をインターネットからアクセス可能にするための設定をします。

インターネットから「10.10.10.1」で TCP ポート 80 番宛てのパケットを受信した場合は、 「192.168.10.100」TCP ポート 80 番に転送します。

インターネットから「10.10.10.1」で TCP ポート 8080 番宛てのパケットを受信した場合は、 「192.168.10.101」TCP ポート 80 番に転送します。

サーバのアドレス	公開するグローバルアドレス	∵ ⊅o N	אוב	ポート	インターフェース
192.168.10.100	10.10.10.1	tcp	*	80	рррО
192.168.10.101:80	10.10.10.1	tcp	~	8080	ррр0

5-2. NAT でのサーバ公開2(複数 IP+PPPoE)

複数のグローバル IP アドレスが割り当てられる場合、それぞれのグローバル IP アドレス毎にプライベ ート IP アドレスを持ったサーバに対してのバーチャルサーバ設定をすることにより、異なるグローバル IP アドレスでそれぞれのサーバに対してアクセスすることができます。

本設定例は WAN 側の回線に PPPoE を利用した例になります。

5-2-1. 構成図



5-2-2. 設定例

グローバル IP アドレス「10.10.1.1」は「192.168.10.100」に、「10.10.10.2」は「192.168.10.101」に NAT 変換します。

<<インタフェース設定>>

[Ethernet0の設定]

IPアドレスに「192.168.10.1」を設定します。

固定アド	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
	一パから取得
ホ가名	
MACTELS	2
IPマス (この)	カレード(ip mesq) ドートで使用するIPアドレスに変換して通信を行います)
27-	トフルパケットインスペウション(spi)
S	PI で DROP したパケットのLOGを取得
proxy :	anp
Directe	ed Broedcast

[Ethernet1の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※PPPoE で接続する場合には "ppp" という論理インタフェースを自動的に生成し、この論理インタフェ ースを使って PPPoE 接続を行います。

③固定ア	レスで使用
IPアドレス	0
ネットマスク	255.255.255.0
MTU	1500
OHOPH	ーバから取得
ホ가名	
мартир	2
IPマス (この)	カレード(ip masq) ボートで使用するIPアドレスに変換して通信を行います)
77-	トフルパケットインスペウション(spi)
□ s	PI で DROP したパケットのLOGを取得
proxy	arp
Directo	ed Broadcast

<<PPP/PPPoE 設定>>

[接続先設定]

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

ユーザロ	test1@centurysys
パスワード	test1pass

[接続設定]

ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

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 Ether O Ether O Ether O BRI(64K) O BRI MP(128K) O Leased Line(64K) O Leased Line(128K) O RS232C
接続形態	○ 手動接続 ● 常時接続 ○ スケジューラ接続
RS2320/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の再接続性を高めるために、PPPoE 特殊オプションを設定します。

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

接続が完了した場合、回線状態が以下のように表示されます。

回換状 差 主回換で接続しています

<<フィルタ設定>>

[転送フィルタ]

LAN 上にある WEB サーバ, FTP サーバへインターネットからアクセス可能にするための設定をします。

インターネットから宛先 IP アドレス「192.168.10.100」で WEB サーバ (TCP ポート 80 番) 宛のパケットを許可します。

インターネットから宛先 IP アドレス「192.168.10.101」で FTP サーバ (TCP ポート 20,21 番) 宛のパケ ットを許可します。

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	ICMP type/code	送信元MADアドレス	LOG
ppp0	パケット受信時 💌	許可 💌	tcp 💌			192.168.10.100	80			
рррО	パケット受信時 💌	許可 💌	tcp 💌			192.168.10.101	20:21			

<<NAT 設定>>

[バーチャルサーバ]

LAN 上にある WEB サーバ, FTP サーバへインターネットからアクセス可能にするための設定をします。 インターネットから「10.10.10.1」で TCP ポート 80 番宛てのパケットを受信した場合は、 「192.168.10.100」TCP ポート 80 番に転送します。

インターネットから「10.10.10.2」で TCP ポート 20,21 番宛てのパケットを受信した場合は、 「192.168.10.101」TCP ポート 20,21 番に転送します。

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	ポート	インターフェース
192.168.10.100	10.10.10.1	tcp 💌	80	ppp0
192.168.10.101	10.10.10.2	tcp 💌	20:21	рррО

5-3. NAT でのサーバ公開3 (複数 IP+Ether)

複数のグローバル IP アドレスが割り当てられる場合、それぞれのグローバル IP アドレス毎にプライベ ート IP アドレスを持ったサーバに対してのバーチャルサーバ設定をすることにより、異なるグローバル IP アドレスでそれぞれのサーバに対してアクセスすることができます。 本設定例は WAN 側の回線に Ethernet を利用した例になります。

5-3-1. 構成図



5-3-2. 設定例

グローバル IP アドレス「10.10.1.1」は「192.168.10.100」に、「10.10.10.2」は「192.168.10.101」に NAT 変換します。

<<インタフェース設定>>

[Ethernet0の設定]

IPアドレスに「192.168.10.1」を設定します。

固定 ア	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
	ーバから取得
ホ가名	
мартир	2
IPマス (この)	カレード(ip masq) ドートで使用するIPアドレスに変換して通信を行います)
27-	トフルパケットインスペウション(spi)
S	PI で DROP したパケットのLOGを取得
proxy :	qrp
Directe	ed Broadcast

[Ethernet1の設定]

IPアドレスに「10.10.10.1」,ネットマスクに「255.255.255.248」を設定します。

ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にしています。 WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に 設定します。

③固定アト	レスで使用
IPアドレス	10.10.10.1
ネットマスク	255.255.255.248
MTU	1500
	ーパから取得
ホスト名	
мартя из	2
IPマス (この)?	カレード(ip masq) ドートで使用する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ウション(spi)
□s	PI で DROP したパケットのLOGを取得
proxy	arp
Directo	ed Broadcast

[その他の設定]

デフォルトゲートウェイの設定	
10.10.10.6	

<<仮想インタフェース設定>>

WAN 側で利用するグローバル IP アドレス「10.10.10.2」を設定します。

インターフェース 仮想I/F番号		IPアドレス	ネットマスク	
eth1	1	10.10.10.2	255.255.255.248	

<<フィルタ設定>>

[転送フィルタ]

LAN 上にある WEB サーバ, FTP サーバへインターネットからアクセス可能にするための設定をします。

インターネットから宛先 IP アドレス「192.168.10.100」で WEB サーバ (TCP ポート 80 番) 宛のパケットを許可します。

インターネットから宛先 IP アドレス「192.168.10.101」で FTP サーバ (TCP ポート 20,21 番) 宛のパケ ットを許可します。

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	ICMP type/code	送信元MACアドレス	LOG
eth1	パケット受信時 💌	許可 💌	tcp 💌			192.168.10.100	80] 🗆
eth1	パケット受信時 💌	許可 💌	tcp 💌			192.168.10.101	20:21			

<<NAT 設定>>

[バーチャルサーバ]

LAN 上にある WEB サーバ, FTP サーバへインターネットからアクセス可能にするための設定をします。 インターネットから「10.10.10.1」で TCP ポート 80 番宛てのパケットを受信した場合は、 「192.168.10.100」 TCP ポート 80 番に転送します。

インターネットから「10.10.10.2」で TCP ポート 20,21 番宛てのパケットを受信した場合は、 「192.168.10.101」TCP ポート 20,21 番に転送します。

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	ポート	インターフェース
192.168.10.100	10.10.10.1	tcp 💌	80	eth1
192.168.10.101	10.10.10.2	tcp 💌	20:21	eth1

5-4. DMZ 構築例 (PPPoE)

XR シリーズで XR-540/C のように3ポート(3セグメント)以上を有する製品では、インターネットに 公開するサーバと社内 LAN を物理的に分けて構成することが可能です。

5-4-1. 構成図



5-4-2. 設定例

<<インタフェース設定>>

[Ethernet0の設定]

IPアドレスに「10.10.10.1」,ネットマスクに「255.255.255.248」を設定します。

DMZ から LAN, WAN へのアクセスを制限するために、ステートフルパケットインスペクションを「有効」 に設定します。

◎固定アド	シレスで使用
IP アドレス	10.10.10.1
ネットマスク	255.255.255.248
MTU	1500
	ーバから取得
ホスト名	
MACTELS	2
IPマス (この)	カレード(ip masq) ボートで使用する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ウション(spi)
□ s	PI で DROP したパケットのLOGを取得
proxy	arp
Directo	ed Broadcast

[Ethernet1の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※PPPoE で接続する場合には "ppp" という論理インタフェースを自動的に生成し、この論理インタフェースを使って PPPoE 接続を行います。

⊙ 固定アト	[、] レスで使用
IPアドレス	0
ネットマスク	255.255.255.0
MTU	1500
OHOPH	ーバから取得
ホ가名	
мартия	2
IPマス (この)	カレード(ip masq) ボートで使用するIPアドレスに変換して通信を行います)
77-	トフルパケットインスペウション(spi)
□ s	PI で DROP したパケットのLOGを取得
proxy	arp
Directo	ed Broadcast

[Ethernet2の設定] IPアドレスに「192.168.10.1」を設定します。



<<PPP/PPPoE 設定>>

[接続先設定]

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

ユーザロ	test1@centurysys
パスワード	test1pass

ppp0 インタフェースに割り当てる IP アドレス「10.10.10.1」を設定します。

	UnNumbered—PPP回線使用時に設定できます	
IP761.7	10.10.10.1	
111123	回線接続時に割り付けるグローバルIPアドレスです	

[接続設定]

IP マスカレードを「無効」にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

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 Ether O Ether O Ether O BRI(64K) O BRI MP(128K) O Leased Line(64K) O Leased Line(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	 ● 通常 ○ On-Demand接続
IPマスカレード	⊙ 無効 ○ 有効
ステートフルパケット インスペクション	○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。



接続が完了した場合、回線状態が以下のように表示されます。



<<フィルタ設定>>

[転送フィルタ]

DMZ 上にある WEB サーバに対してインターネットからアクセス可能にするための設定をします。

インターネット側からの宛先 IP アドレス「10.10.10.2」の WEB サーバ (TCP ポート 80 番) 宛のパケットを許可します。

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	ICMP type/code	送信元MACアドレス	LOG
ррр0	パケット受信時 ⊻	許可 💌	tcp 💌			10.10.10.2	80			

<<NAT 設定>>

[送信元 NAT]

LAN 上にある「192.168.10.0/24」のネットワーク内の端末の送信元 IP アドレスを ppp0 からパケット送 信時に「10.10.10.1」に変換します。

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	
192.168.10.0/24	10.10.10.1	ррр0	

5-4-3. 設定例補足

本設定例ではDMZ内の端末からのWANアクセスを制限しています。設定としては、「インタフェース設定」 →「Ethernet0の設定」のステートフルパケットインスペクションを有効にしているためです。 WANアクセスを許可する場合は、以下の設定を追加する必要があります。

<<フィルタ設定>>

[転送フィルタ]

DMZ 上にある端末からインターネットへアクセス可能にするための設定をします。 ppp0 から送信される送信元 IP アドレス「10.10.0/29」のパケットを許可します。

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	ICMP type/code	送信元MACアドレス	LOG
ppp0	パケット送信時 💌	許可 🔽	全て 💌	10.10.10.0/29						

6. ブリッジフィルタ設定

6-1. 同一 LAN 内でのアクセス制御

XRをブリッジモードで使用することによりブリッジフィルタを使用することができます。 本設定例では同一LAN内の特定のエリアをXRで分離し、ブリッジフィルタで各サーバへのアクセスを制限しています。

6-1-1. 構成図



6-1-2. 設定例

同一 LAN 内にある WEB サーバおよび SSH サーバへのアクセスを制限します。

<<インタフェース設定>>

[Bridge の設定]

ブリッジインタフェースのインタフェース番号を設定します。

本設定例では、Ehernet0 と Ethernet1 でブリッジを設定します。

基本設定		
インターフェース名	br <mark>0 [0-4095]</mark>	☑ _{有効}
Interface 設定		
 ● 使用する ● 使用する ● vLAVを使用する vLAN ID 	Ethernet1	Ethernet2

IP アドレスに「192.168.10.1」,ネットマスクに「255.255.255.0」を設定します。 ※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。

Network設定	
・ 固定アドレス	で使用
IPアドレス	192.168.10.1
ネットマスク	255.255.255.0
мти	1500
	から取得
ホスト名	
 IPマスカレード (このボートで使用) 	(ip masq) するIPアドレスに変換して通信を行います)
コテートフルノ	「ケットインスペクション(spi)
	OP したパケットのLOGを取得
proxy arp	
	Mask Request门応答

<<ブリッジフィルタ設定>>

ブリッジフィルタは全て詳細設定で設定を行っています。

〈転送フィルタ〉

[No.1]

eth0→eth1 への送信元 MAC アドレス「00:80:6D:70:FF:00」の端末からの ARP フレームを許可する設定 をします。

No.	1
入力インタフェース	Not eth0
出力インタフェース	□ _{Not} eth1
送信元MACアドレス	Not
宛先MACアドレス	Not
Policy	許可 💌
待機	□ 有効

OPCODE	Not 💌 [0-65535]
送信元MACアドレス	Not 00:80:6D:70:FF:00
宛先MACアドレス	Not
送信元IPアドレス	Not
宛先IPアドレス	Not

[No.2]

eth0→eth1 への送信元 MAC アドレス「00:80:6D:70:FF:00」の端末からのプロトコルタイプが IPv4 で送 信元 IP アドレス「192.168.10.10」,宛先 IP アドレス「192.168.10.100」TCP ポート 80 番宛のフレーム を許可する設定をします。

	Not eth0
出カインタフェース	Not eth1
	Not 00:80:6D:70:FF:00
宛先MACアドレス	Not
Policy 許	न 💌
待機] _{有効}

Not TCP

[1-65535]*

[1-65535]*

Not

Not 80

IP Protocol

送信元ポート

宛先ボート

[No.3]

eth0→eth1 への送信元 MAC アドレス「00:80:6D:70:FF:01」の端末からの ARP フレームを許可する設定 をします。

Να	3
入力インタフェース	Not eth0
出力インタフェース	□ _{Not} eth1
送信元MACアドレス	Not
宛先MACアドレス	
Policy	許可 💌
待機	口有效
OPCOL 送信元 和PP 宛先州 送信元 宛先P	DE Inot Information (D-65535) MACOTFLZ Inot U0:80:6D:70:FF:01 ACOTFLZ Inot Information MPTFLZ Inot Information FFCLZ Inot Information

[No. 4]

eth0→eth1 への送信元 MAC アドレス「00:80:6D:70:FF:01」の端末からのプロトコルタイプが IPv4 で送 信元 IP アドレス「192.168.10.11」,宛先 IP アドレス「192.168.10.101」TCP ポート 22 番宛のフレーム を許可する設定をします。

INC	4	
入力インタフュ		t eth0
出力インタフュ		t eth1
送信元MACア	FLA DNO	t 00:80:6D:70:FF:01
宛先MACアド	LA DNot	
Policy	許可	
待機		効
	送信元IPアドレス	R
	送信元IPアドレス 宛先IPアドレス	R 192.168.10.11
0	送信元IPアドレス 宛先IPアドレス TOS	R Not 192.168.10.11
⊙ IPv4	送信元IPアドレス 宛先IPアドレス TOS IP Protocol	R Not 192.168.10.11
⊙ IPv4	送信元IPアドレス 宛先IPアドレス TOS IP Protocol 送信元ポート	R Not 192.168.10.11

[No.5]

eth0→eth1 へのその他の通信は破棄する設定をします。

Na	5
入力インタフェース	Not eth0
出力インタフェース	Not eth1
送信元MACアドレス	Not
宛先MACアドレス	Not
Policy	破棄 💌
待機	口有効

7. DHCP 設定

7-1. DHCP サーバ設定

DHCP サーバとして利用することにより、LAN 側の端末に自動的に IP アドレス等の設定をすることが可能です。

また IP アドレスの固定割り付けの設定を行うことにより、DHCP クライアントの MAC アドレス毎に常に 同じ IP アドレスを割り当てることができます。

7-1-1. 構成図



7-1-2. 設定例

MAC アドレス「00:80:6d:70:ff:ff」の端末には IP アドレス「192.168.10.10」を割り当て、その他の端 末にはリース範囲の IP アドレスを割り当てます。

なお固定割り付けで割り当てる IP アドレスはリース範囲外である必要があります。

〈〈インタフェース設定〉〉

[Ethernet0の設定]

IPアドレスに「192.168.10.1」を設定します。

⊙固定アト	レスで使用
IPアドレス	192.168.10.1
ネットマスク	255.255.255.0
мτυ	1500
	ーバから取得
ホスト名	
мартыра	2
IPマス (この) ステー	カレード(ip masq) ボートで使用するIPアドレスに変換して通信を行います) トフルバケット-インスペジション(spi)
□s	PI で DROP したパケットのLOGを取得
proxy	arp
Directi	ed Broadcast

<<各種サービスの設定>>

<DHCP (Relay)サーバ>
[DHCP 設定]
「DHCP サーバを使用する」を選択します。

サーバの選択
OHCPサーバを使用する
OHCPリレーを使用する

[DHCP サーバ設定]

· · · · · · · · · · · · · · · · · · ·		
DHCP サーバで割り当てる	IPア	ドレスの範囲等を設定します。
	TT /	

使用する

ルータアドレス ドメイン名

プライマリDNS セカンダリDNS

プライマリMINSサーバ セカンダリMINSサーバ スコープル

MACアドレス

00:80:6d:70:ff:ff

※動作中の場合は、一度「停止」→「起動」を行ってください。

[DHCP IP アドレス固定割り付け設定]

【DHCP(Relay)サーバ】

DHCP(Relay)サーバを起動します。

標準リース時間 600 最大リース時間 7200

インタフェース eth0

192.168.10.1

example.co.jp 192.168.10.1

ネットワーク 192.168.10.0 サブネットマスク 255.255.255.0 ブロードキャスト 192.168.10.255 リース開始アドレス 192.168.10.100 リース終了アドレス 192.168.10.200

DHCP(Relay)#75	○停止	⊙起動	

MACアドレス「00:80:6d:70:ff:ff」の端末に IPアドレス「192.168.10.10」を割り付けます。

IPアドレス

192.168.10.10

7-2. DHCP リレー設定

DHCP リレー機能を利用することにより、異なるネットワークにある DHCP サーバで IP アドレスを一括管 理している場合、XR 経由で端末に IP アドレスを払い出すことができます。

7-2-1. 構成図



7-2-2. 設定例

<<インタフェース設定>>

[Ethernet0の設定]

IPアドレスに「192.168.10.1」を設定します。

◎固定アド	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
ODHOPH	ーバから取得
ホスト名	
мартрия	1
IPマズ (この)	カレード(ip masq) ドートで使用するIPアドレスに変換して通信を行います)
27-	トフルパケットインスペクション(spi)
🗆 si	PI で DROP したパケットのLOGを取得
proxy :	qre
Directe	ed Broadcast

[Ethernet1の設定]

IP アドレスに「192.168.20.1」を設定します。

●固定アド	レスで使用
IPアドレス	192.168.20.1
ネットマスク	255.255.255.0
MTU	1500
	ーバから取得
ホ가名	
мартя из	2
IPマス (この)	カレード(ip mesq) ドートで使用するIPアドレスに変換して通信を行います)
27-	トフルパケットインスペクション(spi)
□ s	PI で DROP したパケットのLOGを取得
proxy :	arp
Directo	ed Broadcast

<<各種サービスの設定>>

<DHCP(Relay)サーバ>

[DHCP 設定]

「DHCP リレーを使用する」を選択します。

DHCP サーバの IP アドレスとして「192.168.20.100」を設定します。

サーバの選択	○DHCPサーバを使用する ⊙DHCPリレーを使用する			
рнориј	DHDPリレーサーバ使用時に設定して下さい			
上位DHCPサーバの IPアドレス	192.168.20.100			
DHCP relay over XXX	● 使用しない ● 使用する			

【DHCP(Relay)サーバ】

DHCP(Relay)サーバを起動します。

※動作中の場合は、一度「停止」→「起動」を行ってください。

DHCP(Relay)サーバ	○停止	◎起動	

8. 攻撃検出設定

8-1. アクティブファイアウォールの利用

攻撃検出機能により Alert が発生した場合、その後同一の IP アドレスからの通信を自動でブロックする ことができます。

通信のブロックは一定時間経過後に解除されます。

本設定例では、バーチャルサーバ機能を利用して Web サーバを公開し、フィルタ設定でポート番号 80 のみ許可しています。

8-1-1. 構成図


8-1-2. 設定例

「IP アドレス 10.10.10.1 ポート 80」を「IP アドレス 192.168.10.100 ポート 80」に NAT 変換します。 攻撃検出機能を有効に、アクティブファイアウォールを使用します。ただし対象外 IP アドレスとして 「10.10.30.1」を設定しています。

〈〈インタフェース設定〉〉

[Ethernet0の設定] IPアドレスに「192.168.10.1」を設定します。

	シレスで使用
IPアドレス	192.168.10.1
ネットマスク	255.255.255.0
мти	1500
	ーバから取得
ホスト名	
мартрия	2
P7X	カレード(ip masq) ボートで使用するIPアドレスに変換して(通信を行います)
27-	トフルパケット・インスペクション(spi)
□s	PI で DROP したパケットのLOGを取得
proxy	arp
Directo	ed Broadcast

[Ethernet1の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※PPPoE で接続する場合には "ppp" という論理インタフェースを自動的に生成し、この論理インタフェ ースを使って PPPoE 接続を行います。

◎固定アト	レスで使用
IPアドレス	0
ネットマスク	255.255.255.0
мти	1500
	ーパから取得
ホスト名	
мартрия	2
IPマス (この)	カレード(ip masq) ボートで使用するIPアドレスに変換して通信を行います)
75-	トフルパケットインスペウション(spi)
□ s	PI で DROP したパケットのLOGを取得
proxy	arp
Direct:	ed Broadcast

<<PPP/PPPoE 設定>>

[接続先設定]

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

ユーザロ	test1@centurysys
パスワード	test1pass

[接続設定]

ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

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	OEther0 OEther1 OEther2 OBRI(64K) OBRI MP(128K) OLeased Line(64K) OLeased Line(128K) ORS232C
接統形態	○ 手動接続 ● 常時接続 ● スケジューラ接続
RS2320/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
デフォルトルートの設定	○無効 ● 有効

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ます。

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

接続が完了した場合、回線状態が以下のように表示されます。

自殺状態 王国線で接続しています

<<フィルタ設定>>

[転送フィルタ]

LAN 上にある WEB サーバヘインターネットからアクセス可能にするための設定をします。

インターネットから宛先 IP アドレス「192.168.10.100」で WEB サーバ (TCP ポート 80 番) 宛のパケットを許可します。

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	ICMP type/code	送信元MADアドレス	LOG
ppp0	パケット受信時 ⊻	許可 💌	tcp 💌			192.168.10.100	80]

<<NAT 設定>>

[バーチャルサーバ]

LAN 上にある WEB サーバヘインターネットからアクセス可能にするための設定をします。

インターネットから「10.10.10.1」で TCP ポート 80 番宛てのパケットを受信した場合は、 「192.168.10.100」TCP ポート 80 番に転送します。

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
192.168.10.100	10.10.10.1	top 💌	80	ppp0

<<各種サービスの設定>>

〈攻撃検出サービス〉

[インタフェース設定]

攻撃検出を行うインタフェースとして「ppp0」, IPアドレスとして「10.10.10.1」を設定します。 攻撃検出後のブロック時間を「5」分とし、False Positive Unblockを「無効」に設定しています。 ※False Positive Unblock とは本来攻撃ではないが、攻撃と間違えて遮断する可能性のあるものをブ

ロック"しない"(「有効」)か"する"(「無効」)かを設定します。

本設定例では、本来攻撃ではない通信もブロックの対象としています。

インタフェース	ppp0
IPアドレス	10.10.10.1
ブロック時間	5 分
False Positive Unblock	○ 有効 ④ 無効

[対象外 IP アドレス設定]

通信をブロックしない送信元 IP アドレスとして「10.10.30.1」を設定しています。 ※仮に対象外 IP アドレスからの攻撃を検出しても通信のブロック対象とはなりません。

対象外IPアドレス	
10.10.30.1	

【攻撃検出サービス】 攻撃検出サービスを起動します。 ※動作中の場合は、一度「停止」→「起動」を行ってください。

攻撃検出サービス ○停止 ◎起動

8-1-3. 設定例補足(メール送信設定)

本設定例では攻撃検出サービスにより不正アクセスを検知し、ブロックします。

この設定に加えてメール送信設定をおこなうことにより、ブロックした送信元 IP アドレスをメールで通知するといったことも可能です。

<<システム設定>>

<メール送信機能の設定>

[基本設定]

メール送信のための基本設定を行います。

本設定例では、メール認証の方式として SMTP-Auth (plain)を使用しています。

基本設定		
メール認証	〇記証しない 〇 POP before SMTP 〇 SMTP-Auth(login) ④ SMTP-Auth(plain)	
SMTPサーバアドレス	smtp.example.co.jp	
SMTPサーバポート	25	
POP3サーバアドレス		
ユーザロ	xr	
パスワード	systemmail	

シスログメールを送信するための設定を行います。

検出文字列の指定では、「Blocking host」を指定しています。これによりシスログで「Blocking host」の文字列と一致したログが出力された場合にメールを送信することができます。

以下は送信時のメール内容例です。

Jun 30 14:35:29 localhost snortsam[6122]: Blocking host 10.10.50.1 completely for 300 seconds (Sig_ID: 100000121).

シスログのメール送信			
ログのメール送信	○送信しない ○送信する		
送信先メールアドレス	admin@example.co.jp		
送信元メールアドレス	xr@example.co.jp		
件名	Log keyword detection		
検出文字列の指定	文字列は1行1255文字まで、最大32 Blocking host	圏(行)までです。	

【DNS キャッシュ】

メール送信時の名前解決を可能にするため、DNS キャッシュ機能を起動します。

DNS+e ^{-yy} 2_	動
-------------------------	---

9. Web 認証設定 (ゲートウェイ認証設定)

9-1. ユーザ認証

XR を経由する通信を行う場合に、XR でユーザ ID, パスワードによる認証を必要とするように設定する ことが可能です。これにより外部へアクセスできるユーザを制限するといった利用方法も可能になりま す。

9-1-1. 構成図



---- 未認証ユーザからの通信

9-1-2. 設定例

Web 認証機能の MAC フィルタで許可されている端末「00:80:6D:70:FF:FF」のみ認証を必要とせず、その 他の端末は認証を必要とするように設定します。

<<インタフェース設定>>

[Ethernet0の設定]

IPアドレスに「192.168.10.1」を設定します。

⊙ 固定アド	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
	ーバから取得
ホ가名	
MACTELS	2
IPマス (この)	カレード(ip masq) ドートで使用するIPアドレスに変換して通信を行います)
1 75-	トフルパケットインスペクション(spi)
s s	PI で DROP したパケットのLOGを取得
proxy :	arp
Directe	ed Broadcast

[Ethernet1の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※PPPoE で接続する場合には "ppp" という論理インタフェースを自動的に生成し、この論理インタフェ ースを使って PPPoE 接続を行います。

◎固定アド	レスで使用
IP アドレス	D
ネットマスク	255.255.255.0
мти	1500
	ーバから取得
ホ가名	
мартия	
□ IPマスた (このポ)レード(ip masq) ートで使用するIPアドレスII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)
	1 で DROP したパケットのLOGを取得
proxy a	rp.
Directed	d Broadcast

<<PPP/PPPoE 設定>>

[接続先設定]

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

ユーザロ	test1@centurysys
パスワード	test1pass

[接続設定]

ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

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	OEther0 OEther1 OEther2 OBRI(64K) OBRI MP(128K) OLeased Line(64K) OLeased Line(128K) ORS2320
接続形態	○ 手動接続 ○ 常時接続 ○ スケジューラ接続
RS2320/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の再接続性を高めるために、PPPoE 特殊オプションを設定します。

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

接続が完了した場合、回線状態が以下のように表示されます。

回線状況 主回線で接続しています

<<Web 認証設定>>

[基本設定]

インターネット側へ通信する際に XR でのユーザ認証を必要とするように設定します。 また MAC アドレスフィルタを利用するため、「使用する」を選択しています。

基本設定		
本機能	○ 使用しない	⊙ 使用する
認証	○ しない (URL転送のみ)	 する
80/tcp 監視	◎ 行わない	O 175
MACアドレスフィルタ	○ 使用しない	 使用する

URL 転送は行わないため、設定していません。

URL転送		
URL		
通常認証後	⊙ 行わない (デフォルト)	O 175
強制認証後	 行わない(エンドユーザ要求URL) 	0 175

XR でアカウントの管理を行うため、「ローカル」を選択します。

認証方法		
⊙ ດ−カル	O RADIUSサーバ→ローカル	

認証で許可された通信が無通信状態となってから 30 分経過した場合は、切断するよう設定しています。

接統許可時間	
アイドルタイムアウト 30	分 (1~43200)
○ セッションタイムアウト	分 (1~43200)
○ 認証を受けたWebブラウザのウ	インドウを閉じるまで

[ユーザ設定]

認証で使用するユーザ ID,パスワードを設定します。

ユーザロ	パスワード	
user	pass	

[MAC アドレスフィルタ]

認証を必要とせず通信が可能な端末を登録します。インタフェースはフィルタリングを行うインタフェ ースを設定します。

MACアドレスフィルタの 追加			
MAOPFLス	00:80:6d:70:ff:ff		
インタフェース	eth0		
動作	動作 許可 💌		

MAC アドレスフィルタ登録後は、以下のように表示されます。

MACTELZ	インタフェース	動作	設定変更
00.80.6d:70 .ff.ff	eth0	許可	编集 削除

[ログ設定]

Web 認証時のアクセスログおよびエラーログを取得するように設定しています。 ※ログを取得する場合は、SYSLOG サービスは必ず「起動」してください。

エラーログ	○使用しない	⊙ syslog IRZ	
アクセスログ	○使用しない	⊙ syslce ⊐RZ	

9-1-3. 設定例補足(ユーザ認証方法)

本設定例では端末から一度 XR にアクセスし、そこで認証を行う必要があります。

端末から XR の認証画面にアクセスします。

アクセスする際は本設定例の場合、以下の形式でアドレスを指定してアクセスします。

http://192.168.10.1/login.cgi

アクセス後、認証画面がポップアップしますので、ユーザ ID,パスワードを入力します。

ユーザネ	6とパスワードが必要です	×
?		い
	user	
	パスワード	

	 パスワードマネージャを使ってこのパスワードを記憶する。 OK キャンセル 	

認証に成功すると、以下のメッセージが表示され、インターネット側へのアクセスが可能になります。

You can connect to the External Network (user@192.168.10.100).

Date: Tue Jul 1 14:07:00 2008

9-2. URL 転送

Web認証機能では単にユーザ認証という用途だけではなく、XR配下の端末がWebアクセスを行った際に、 XRで指定したURLへ転送させるといったことも可能です。

9-2-1. 構成図



9-2-2. 設定例

ユーザ認証を行わず URL 転送を行う場合、あらかじめ許可しておく通信を設定しておく必要があります。 本設定例では Web 認証フィルタで UDP ポート 53 番をあらかじめ許可しています。それ以外の通信に関し ては、あらかじめ許可されていないため、Web 認証による URL 転送後に通信可能になります。

<<インタフェース設定>>

[Ethernet0の設定] IPアドレスに「192.168.10.1」を設定します。

	シレスで使用
IPアドレス	192.168.10.1
ネットマスク	255.255.255.0
MTU	1500
	ーバから取得
ホスト名	
мартил	2
	カレード(ip masq) ボートで使用するIPアドレスに変換して通信を行います)
75-	トフルパケットインスペクション(spi)
□s	PI で DROP したパケットのLOGを取得
proxy :	arp
Directi	ed Broadcast

[Ethernet1の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※PPPoE で接続する場合には "ppp" という論理インタフェースを自動的に生成し、この論理インタフェ ースを使って PPPoE 接続を行います。

◎固定アト	レスで使用
IPアドレス	0
ネットマスク	255.255.255.0
мти	1500
	ーバから取得
ホスト名	
мартир	2
ロ IPマス (この)	カレード(ip masq) ボートで使用するIPアドレスに変換して通信を行います)
27-	トフルパケットインスペウション(spi)
□ s	PI で DROP したパケットのLOGを取得
proxy	arp
Directo	ed Broadcast

<<PPP/PPPoE 設定>>

[接続先設定]

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

ユーザロ	test1@centurysys
パスワード	test1pass

[接続設定]

ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

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	OEther0 OEther1 OEther2 OBRI(64K) OBRI MP(128K) OLeased Line(64K) OLeased Line(128K) ORS2320
接続形態	○ 手動接続 ○ 常時接続 ○ スケジューラ接続
RS2320/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の再接続性を高めるために、PPPoE 特殊オプションを設定します。

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

接続が完了した場合、回線状態が以下のように表示されます。

国袋状態 主国線で接続しています

<<Web 認証設定>>

[基本設定]

インターネット側へ通信する際にユーザ認証を必要とせず、URL 転送のみ行うように設定しています。 80/tcp 監視を「行う」を選択し、TCP ポート 80 番のコネクションがあったときに、強制的に Web 認証を 行うように設定します。

基本設定		
本機能	○ 使用しない	使用する
認証	しない(URL転送のみ)	0 1 3
80/tcp 監視	○ 行わない	 行う
MACアドレスフィルタ	⊙ 使用しない	 使用する

転送する URL を設定します。

強制認証後に URL 転送が行われるように設定します。

URL転送		
URL	http://www.centurysys.co.jp	
通常認証後	⊙ 行わない (デフォルト)	O (T)
強制認証後	○ 行わない (エンドユーザ要求URL)	 行う

Web 認証で許可された通信が無通信状態となってから 30 分経過した場合は、切断するよう設定しています。

接続許可時間				
 アイドルタイムアウト 30 	分 (1~43200)			
○ セッションタイムアウト	分 (1~43200)			
○ 認証を受けたWebブラウザのウ	インドウを閉じるまで			

[フィルタ設定]

あらかじめ許可しておく通信として UDP ポート 53 番を許可しています。

これにより Web アクセス時に行う名前解決は、Web 認証の対象とはならないようにしています。

※このフィルタ設定は「フィルタ設定」→「Web 認証フィルタ」と同じものです。

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	ICMP type/code	送信元MACアドレス	LOG
eth0	パケット受信時 ⊻	許可 💌	udp 💌				53]

9-3. ユーザ強制認証+URL 転送+RADIUS 連携

Web 認証機能で TCP ポート 80 番のコネクションを監視し、このコネクションがあった際に認証画面がポ ップアップするように設定することが可能です。

そしてユーザ認証成功後、指定した URL へ転送することも可能です。

またアカウントの管理を XR ではなく、RADIUS サーバで管理することも可能です。本設定例では RA-630 でアカウントの管理を行っています。

9-3-1. 構成図



9-3-2. 設定例

《XR の設定》

Web 認証機能で TCP ポート 80 番のコネクションを監視し、このコネクションがあった際に認証画面がポ ップアップするように設定します。

その際あらかじめ許可しておく通信を設定しておく必要があります。

本設定例ではWeb認証フィルタでUDPポート53番をあらかじめ許可しています。それ以外の通信に関しては、あらかじめ許可されていないため、Web認証によるユーザ認証後、通信可能になります。

<<インタフェース設定>>

[Ethernet0の設定]

IPアドレスに「192.168.10.1」を設定します。

固定 ア	*レスで使用
₽₽Fレス	192.168.10.1
ネットマスク	255.255.255.0
MTU	1500
	ーバから取得
ホスト名	
MAOPHUS	2
IPマス (この)	カレード(ip masq) ボートで使用するIPアドレスに変換して通信を行います)
27-	トフルパケットインスペクション(spi)
□s	PI で DROP したパケットのLOGを取得
proxy	arp
Directo	ed Broadcast

[Ethernet1の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※PPPoE で接続する場合には "ppp" という論理インタフェースを自動的に生成し、この論理インタフェ ースを使って PPPoE 接続を行います。

◎ 固定アト	レスで使用
IPアドレス	0
ネットマスク	255.255.255.0
мти	1500
	ーバから取得
ホスト名	
мартир	2
IPマス (この)	カレード(ip masq) ボートで使用するIPアドレスに変換して通信を行います)
77-	トフルパケットインスペクション(spi)
□s	PI で DROP したパケットのLOGを取得
proxy	arp
Direct:	ed Broadcast

<<PPP/PPPoE 設定>>

[接続先設定]

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

ユーザロ	test1@centurysys
パスワード	test1pass

[接続設定]

ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

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 Ether O Ether O Ether O BRI(64K) O BRI MP(128K) O Leased Line(64K) O Leased Line(128K) O RS232C
接続形態	○ 手動接続 ● 常時接続 ○ スケジューラ接続
RS2320/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の再接続性を高めるために、PPPoE 特殊オプションを設定します。

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

接続が完了した場合、回線状態が以下のように表示されます。

回換状 差 主回換で接続しています

<<Web 認証設定>>

[RADIUS 設定]

RADIUS サーバに関する設定を行います。

本設定例ではアトリビュートとして「Idle-Timeout」を設定しています。これにより RADIUS サーバより 送信される Idle-Timeout を利用することが可能です。

プライマリサー	パ設定				
IP7FLス	192.168.10.254				
ポート番号	○ 1645 ④ 1812 ○ 手動設定				
secret			secret		
ナーバ共通設: NAS	定 3HP-Address			192.168.10.1	
NAS-Identifier				XR	
使纳拉可味的		(5-5)(2)送7号	ナヤスフレル	ュートの地学)	
度和GT 可時間 アイドルタイ	(ムアウト	arater Id	die-Timeo	ut_28	~
セッションター	ብራ ፖታት	指定しない			~

[基本設定]

TCP ポート 80 番のコネクションを監視し、このコネクションがあった際に認証画面がポップアップする ように、80/tcp 監視を「行う」を選択します。

基本設定		
本機能	○ 使用しない	 使用する
認証	○ しない (URL転送のみ)	 する
80/tcp 監視	○ 行わない	 ① 行う
MACアドレスフィルタ	⊙ 使用しない	 使用する

転送する URL を設定します。

強制認証後に URL 転送が行われるように設定します。

URL転送		
URL	http://www.centurysys.co.jp	_
通常認証後	⊙ 行わない (デフォルト)	O 175
強制認証後	○ 行わない (エンドユーザ要求URL)	 行う

RADIUS サーバでのみアカウントの管理を行うため、「RADIUS サーバ」を選択します。

認証方法		
🔘 ຊ-ສາມ	O RADIUSサーバ→ローカル	RADIUSサーバ

接続許可時間は「アイドルタイムアウト」を選択します。

※RADIUS サーバからの該当アトリビュートがなければ、ここで設定した値を使用します。

接統許可時間	
アイドルタイムアウト 30	分 (1~43200)
○ セッションタイムアウト	分 (1~43200)
○ 認証を受けたWebブラウザのウ	インドウを閉じるまで

[フィルタ設定]

あらかじめ許可しておく通信として UDP ポート 53 番を許可しています。

これにより Web アクセス時に行う名前解決は、Web 認証の対象とはならないようにしています。

※このフィルタ設定は「フィルタ設定」→「Web 認証フィルタ」と同じものです。

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	ICMP type/code	送信元MACアドレス	LOG
eth0	パケット受信時 ⊻	許可 💌	udp 💌				53]

《RA-630の設定》

<<管理機能>>

〈ネットワーク〉

[基本情報]

Ether0 で IP アドレスに「192.168.10.254/24」を設定します。

※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。

■基本情報	
Ether0	
IPアドレス	192.168.10.254/24
MTU	1500
通信モード	💿 Auto 🌑 10M Half 💿 10M Full 🌑 100M Half 🌑 100M Full

設定後は以下のように表示されます。

Ether0	IPアドレス	192.168.10.254/24	
	MTU	1500	編集
	通信モード	Auto	

<<RADIUS>>

〈サーバ〉

[基本情報]

XR で設定しているポート番号と同じポート番号「1812/1813」,認証方式として「PAP/CHAP」を選択します。

☆ポート番号	■ RADIUSサーバ証明書
 ● 1645/1646 ● 1812/1813 ● 1645/1646≿1812/1813 	 ● 使用しない ● 本装置の証明書を使用する
 ● 手動設定 認証用 アカウンティング用 	シリアルナンバ
■認証方式	
🗹 PAP/CHAP 🔲 EAP-MD5	
EAP-TLS EAP-PEAP EAP-TTLS	

[クライアント]

RADIUS クライアントである XR の情報を登録します。

クライアント新規追加	
クライアント名	XR
IPアドレス	192.168.10.1
シークレット	secret
アドレスプール	指定しない 🕑

〈プロファイル〉

[ユーザ基本情報]

ユーザを作成するためにはユーザ基本情報プロファイルの作成が必要です。

認証方式として「PAP/CHAP」を選択します。

📰 ユーザ基本情報プロファイル 新	所規追加
プロファイル名	xrbasic
認証方式	PAP/CHAP
同時接続数	
IPアドレス割り当て	💿 未使用 🌑 RADIUSクライアント 🌑 アドレスプール 🌑 固定
アドレスプール	指定しない 💌

[応答アトリビュート]

応答アトリビュートプロファイルを作成します。

■応答アトリビュートプロファ	イル 新規追加
プロファイル名	xrreply

応答アトリビュート一覧の「xrreply」の新規追加からアトリビュートとして「Idle-Timeout」を選択し、 値として「1800」を設定しています。

■応答アトリビュート 新規追加		
プロファイル名	xrreply	
アトリビュート	Idle-Timeout	V
値	1800	

[ユーザプロファイル]

作成したユーザ基本情報を選択してユーザプロファイルを作成します。

__ユーザプロファイル 新規i	助
プロファイル名	xruser
基本	xrbasic 💌
izie	指定しない。
証明書	指定しない 🐱
応答	xrreply
グループ	指定しない 🔽

〈ユーザ〉

[ユーザ]

ユーザ ID/パスワードを設定します。本設定例ではユーザ ID「user」,パスワード「pass」と設定しています。

プロファイルはユーザプロファイルで作成した「xruser」を選択します。

user
pass
xruser 💌
● ロックしない ● ロックする

<<RADIUS>>

〈サーバ〉

[起動・停止]

RADIUS サーバを起動し設定を反映させます。

■起動·停止	
	現在の状態
	停止中
	起動

9-4. Web 認証機能ソリューション例 (NS-430 との併用)

Web 認証機能ではルータ経由での通信の可否を制御することが可能ですが、ルータ配下の社内セグメントへの接続の可否を制御することはできません。そこで社内セグメントへの不正接続を防止する機能に特化した「NS-430」をルータ配下のスイッチに接続し、不正接続を防止します。

なお Web 認証および NS-430 で使用するユーザ ID, パスワードは RADIUS サーバで一括管理することが可 能です。本設定例では RA-630 でアカウントの管理を行っています。

9-4-1. 構成図



※一部の通信は除く

9-4-2. 設定例

《XR の設定》

Web 認証機能で TCP ポート 80 番のコネクションを監視し、このコネクションがあった際に認証画面がポ ップアップするように設定します。

その際あらかじめ許可しておく通信を設定しておく必要があります。

本設定例ではWeb認証フィルタでUDPポート53番をあらかじめ許可しています。それ以外の通信に関しては、あらかじめ許可されていないため、Web認証によるユーザ認証後、通信可能になります。

<<インタフェース設定>>

[Ethernet0の設定]

IPアドレスに「192.168.10.1」を設定します。

⊙固定アト	ジレスで使用
IPアドレス	192.168.10.1
ネットマスク	255.255.255.0
MTU	1500
	ーパから取得
ホ가名	
MACTELS	2
IPマス (この)	カレード(ip masq) ボートで使用するIPアドレスに変換して通信を行います)
27-	トフルパケットインスペクション(spi)
□s	PI で DROP したパケットのLOGを取得
proxy	arp
Directo	ed Broadcast

[Ethernet1の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※PPPoE で接続する場合には "ppp" という論理インタフェースを自動的に生成し、この論理インタフェ ースを使って PPPoE 接続を行います。

◎ 固定アト	レスで使用
IPアドレス	0
ネットマスク	255.255.255.0
мти	1500
	ーバから取得
ホスト名	
мартир	2
IPマス (この)	カレード(ip masq) ボートで使用するIPアドレスに変換して通信を行います)
77-	トフルパケットインスペクション(spi)
□s	PI で DROP したパケットのLOGを取得
proxy	arp
Direct:	ed Broadcast

[Ethernet2の設定] IPアドレスに「192.168.20.1」を設定します。

IP アドレ	ج 192.168.20.1
ネットマス	255.255.255.0
мто	1500
	7スカレード(ip masq) のボートで使用するIPアドレスに変換して通信を行います) テートフルバケットインスペクション(spi)
] SPI で DROP したパケットのLOGを取得
pro	xxy arp
	acted Decidencet

<<PPP/PPPoE 設定>>

[接続先設定]

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

ユーザロ	test1@centurysys
パスワード	test1pass

[接続設定]

ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

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	OEther0 OEther1 OEther2 OERI(64K) OERI MP(128K) OLeased Line(64K) OLeased Line(128K) ORS232C
接続形態	○ 手動接続 ● 常時接続 ● スケジューラ接続
RS2320/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の再接続性を高めるために、PPPoE 特殊オプションを設定します。

PPPoE特殊オプション (全回線共通)	 ✓ 回線接続時に前回のFFPcE セッションのFADTを強制送出 ✓ 非接続SessionのIFv4Packet受信時ITPADTを強制送出 ✓ 非接続SessionのIFv4Packet受信時ITPADTを強制送出
	「「非接続SessionのLCP-EchoRequest受信時にPADTを強制送出」

接続が完了した場合、回線状態が以下のように表示されます。

|--|

<<Web 認証設定>>

[RADIUS 設定]

RADIUS サーバに関する設定を行います。

本設定例ではアトリビュートとして「Idle-Timeout」を設定しています。これにより RADIUS サーバより 送信される Idle-Timeout を利用することが可能です。

プライマリサーバ	设定				
IP7Fレス	192.168.20.254				
ポート番号	○ 1645 ④ 1812 ○ 手動設定				
secret	secret				
サーバ共通設定 NASHF	D-Address			192.168.20.1	
	ou other		++ 7	· 1.04600	
姜\$克計可時間(PCA	uus y – r	いから送信る	きれるアトリ	ビュートの相定)	
ፖ-ሹብ/タイムን	1ムアウト Idle-Timeout_28 💌			*	
セッションタイム	アウト	ケト 指定しない 🗸			

[基本設定]

TCP ポート 80 番のコネクションを監視し、このコネクションがあった際に認証画面がポップアップする ように、80/tcp 監視を「行う」を選択します。

基本設定		(2)
本機能	○ 使用しない	使用する
認証	○ しない (URL転送のみ)	 する
80/tcp 監視	○ 行わない	 ① 行う
MACアドレスフィルタ	⊙ 使用しない	 使用する

転送する URL を設定します。

強制認証後に URL 転送が行われるように設定します。

URL転送		
URL	http://www.centurysys.co.jp	_
通常認証後	⊙ 行わない (デフォルト)	O 175
強制認証後	○ 行わない (エンドユーザ要求URL)	 行う

RADIUS サーバでのみアカウントの管理を行うため、「RADIUS サーバ」を選択します。

認証方法		
◯ ローカル	O RADIUSサーバ→ローカル	In RADIUS # − /

接続許可時間は「アイドルタイムアウト」を選択します。

※RADIUS サーバからの該当アトリビュートがなければ、ここで設定した値を使用します。

接統許可時間				
アイドルタイムアウト 30	分 (1~43200)			
○ セッションタイムアウト	分 (1~43200)			
○ 認証を受けたWebブラウザのウ	インドウを閉じるまで			

[フィルタ設定]

あらかじめ許可しておく通信として UDP ポート 53 番を許可しています。

これにより Web アクセス時に行う名前解決は、Web 認証の対象とはならないようにしています。

※このフィルタ設定は「フィルタ設定」→「Web 認証フィルタ」と同じものです。

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	ICMP type/code	送信元MACアドレス	LOG
eth0	パケット受信時 ⊻	許可 💌	udp 💌				53]

《NS-430 の設定》

機器情報をホワイトリストに登録し、その情報を元にアドレス解決制限を行っています。 ホワイトリストに登録されていない機器に関しては、MAC アドレスをユーザ ID/パスワードとして、 Radius サーバへ認証/アカウンティングを行います。

<<管理機能>>

〈インタフェース〉

[イーサネット]

Ether0 で IP アドレスに「192.168.20.10/24」を設定します。 ※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。

IPアドレス	192.168.20.10/24
デフォルトルート	
メトリック	[0-255]
フィルタ名	
MTU	1500 byte [68-1500] (デフォルト:1500)
通信モード	☑ 自動 100M 全二重

Ether1でIPアドレスに「192.168.10.10/24」を設定します。

※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。

IPアドレス	192.168.10.10/24
デフォルトルート	
メトリック	[0-255]
フィルタ名	
MTU	1500 byte [68-1500] (デフォルト:1500)
通信モード	☑ 自動 100M 全二重

設定後は以下のように表示されます。

インタフェース	IPアドレス	フィルタ名	MTU	通信モード	編集	削除
Ether0	192.168.20.10/24		1500	auto	編集	
Ether1	192.168.10.10/24		1500	auto	編集	削除

<<ネットワーク監視機能>>

<RADIUS 連携>

[RADIUS]

RADIUS サーバの設定を行います。

ガライマリ					
IPアドレス	192.168.20.	254			
ポート番号	1812/1813	3 💌			
認証ポート	1812	[1024-60000]			
アカウンティングポート	1813	[1024-60000]			
クライアントIPアドレス	192.168.20.	10			
シークレット	ns430secre	it .			

認証およびアカウンティングを使用するように設定しています。

動作設定				
121E	使用す	a 💌		
アカウンティング	使用す	a 💌		
タイムアウト	5	秒 [3-30] (デフォルト:5)		
最大試行回数	3	[1-10] (デフォルト:3)		
アクセプトキャッシュ保持時間	300	秒 [30-86400] (デフォルト:300)		
リジェクトキャッシュ保持時間	300	秒 [30-86400] (デフォルト:300)		

[アトリビュート]

キャッシュ保持時間でアトリビュートとして「Session-Timeout」を選択します。

登録先キャッシュ/リス	卜名
アトリビュート	取得しない
ベンダID	[1-65535]
タイプ	[1-255]
キャッシュ保持時間	
アトリビュート	Session-Timeout (27) 💌
ベンダID	[1-65535]
タイプ	[1-255]

<ネットワーク監視>

[端末リスト]

端末情報をホワイトリストへの登録します。

本設定例では以下のルールでホワイトリストに登録します。

機器名	MAC アドレス	リスト
監視端末	00-80-6D-85-FF-F0	ホワイトリスト
RA-630 (RADIUS)	00-80-6D-75-FF-F0	ホワイトリスト
XR(ethO 側)	00-80-6D-70-FF-F0	ホワイトリスト
XR(eth2 側)	00-80-6D-70-FF-F2	ホワイトリスト

MAC アドレス「00-80-6D-85-FF-F0」をホワイトリストに登録します。

リスト名	ホワイトリスト 💌
MACアドレス	00-80-6D-85-FF-F0
IPアドレス	192.168.20.100
備考	

MAC アドレス「00-80-6D-75-FF-F0」をホワイトリストに登録します。

リスト名	#ワイトリスト 💌
MACTFUR	00-80-6D-75-FF-F0
IPアドレス	192.168.20.254
備考	

MACアドレス「00-80-6D-70-FF-F0」をホワイトリストに登録します。

リスト名	<u>ホワイトリスト</u>
MACTFUR	00-80-6D-70-FF-F0
IPアドレス	192.168.10.1
備考	

MAC アドレス「00-80-6D-70-FF-F2」をホワイトリストに登録します。

リスト名	ホワイトリスト 💌
MACアドレス	00-80-6D-70-FF-F2
IPアドレス	192.168.20.1
備考	

ホワイトリスト登録後は、以下のように表示されます。

端末リス	:ŀ-					
ホワイ	トリスト				ni: n	
	MAOPFLス	IPアドレス	備考	編集	削除	^
	00-80-6D-85-FF-F0	192.168.20.100		編集	削除	
	00-80-6D-75-FF-F0	192.168.20.254		編集	削除	=
	00-80-6D-70-FF-F0	192,168,10,1		編集	削除	
	00-80-6D-70-FF-F2	192.168.20.1		編集	削除	~

[基本設定]

ネットワーク監視で「使用する」,制限設定でアラート,接続制限で「使用する」を選択します。 優先リスト名で「ホワイトリスト」,デフォルト動作で「拒否」を選択しています。

ネットワーク監視	使用する 💌
ローカルキャッシュ	
定期解放	使用しない 💌
保持時間	5 分 [1-144000] 💌
制限設定	
アラート	使用する 💌
接続制限	使用する 💌
優先リスト名	ホワイトリスト 💌
デフォルト動作	拒否 💌

[アドレス解決制限]

アドレス解決制限で「使用する」を選択します。

アラートを「使用する」にし、端末検出ログとしてホワイトキャッシュ,ローカルキャッシュ,アクセ プトキャッシュおよびリジェクトキャッシュを取得するように設定しています。

アドレス解決制限	使用する 💌
アラート	
アラート	使用する 💌
端末検出ログ	
端末検出ログ	取得する 💌
ホワイトキャッシュ	取得する 💌
ブラックキャッシュ	取得しない 💌
ローカルキャッシュ	取得する 💌
アクセプトキャッシュ	取得する 💌
リジェクトキャッシュ	取得する 💌

《RA-630の設定》

<<管理機能>>

〈ネットワーク〉

[基本情報]

Ether0 で IP アドレスに「192.168.20.254/24」を設定します。

※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。

基本情報	
Ether0	
IPアドレス	192.168.20.254/24
MTU	1500
通信モード	💿 Auto 🌑 10M Half 💿 10M Full 🌑 100M Half 🌑 100M Full

設定後は以下のように表示されます。

Ether0	IPアドレス	192.168.20.254/24	
	MTU	1500	編集
	通信モード	Auto	

<<RADIUS>>

〈サーバ〉

[基本情報]

XR, NS で設定しているポート番号と同じポート番号「1812/1813」,認証方式として「PAP/CHAP」を選択 します。

∰ポート番号	Ⅲ RADIUSサーバ証明書
1645/1646	 使用しない
1812/1813	● 本装置の証明書を使用する
1645/1646と1812/1813	
● 手動設定	シリアルナンバ
認証用	
アカウンティング用	
■認証方式	
EAP-TTLS	

[クライアント]

RADIUS クライアントである XR の情報を登録します。

クライアント新規追加	
クライアント名	XR
IPアドレス	192.168.20.1
シークレット	secret
アドレスプール	指定しない 🔽

RADIUS クライアントである NS-430 の情報を登録します。

■クライアント新規追加	
クライアント名	NS430
IPアドレス	192.168.20.10
シークレット	ns430secret
アドレスプール	指定しない ∨

〈プロファイル〉

[ユーザ基本情報]

Web 認証用のユーザを作成するためにはユーザ基本情報プロファイルの作成が必要です。 認証方式として「PAP/CHAP」を選択します。

■ ユーザ基本情報プロファイル	> 新規追加
プロファイル名	xrbasic
認証方式	PAP/CHAP
同時接続数	
IPアドレス割り当て	💿 未使用 🍈 RADIUSクライアント 🌑 アドレスブール 🌑 固定
アドレスプール	指定しない 💌

[応答アトリビュート]

Web 認証用の応答アトリビュートプロファイルを作成します。

■ 応答アトリビュートプロファ	・イル 新規追加	
プロファイル名	xrreply	

応答アトリビュート一覧の「xrreply」の新規追加からアトリビュートとして「Idle-Timeout」を選択し、 値として「1800」を設定しています。

■応答アトリビュート 新規追	助o	
プロファイル名	xrreply	
アトリビュート	Idle-Timeout	<u>~</u>
値	1800	
[ユーザプロファイル]

作成したユーザ基本情報,応答アトリビュートを選択して Web 認証用のユーザプロファイルを作成しま す。

_ユーザプロファイル 新規i	۵da
プロファイル名	xruser
基本	xrbasic 💌
121E	指定しない。
証明書	指定しない 🐱
応答	xrreply 💌
グループ	<mark>指定しない 🔽</mark>

〈ユーザ〉

[ユーザ]

Web 認証用のユーザ ID/パスワードを設定します。本設定例ではユーザ ID「user」,パスワード「pass」 と設定しています。

プロファイルはユーザプロファイルで作成した「xruser」を選択します。

📖 ユーザ 新規追加	
ユーザID	user
バスワード	pass
プロファイル	xruser 💌
■固定IPアドレス払い出し	
IPアドレス	
ネットマスク	
■アカウントのロック	
ロック	⊙ ロックしない ● ロックする

〈プロファイル〉

[ユーザ基本情報]

NS-430 用のユーザを作成するためにはユーザ基本情報プロファイルの作成が必要です。 認証方式として「PAP/CHAP」を選択します。

_ユーザ基本情報プロファイル 新規追加		
プロファイル名	ns430basic	
認証方式	PAP/CHAP 💌	
同時接続数		
IPアドレス割り当て	◆ 未使用 ● RADIUSクライアント ● アドレスプール ● 固定	
アドレスプール	指定しない。 🔽	

[応答アトリビュート] NS-430 用の応答アトリビュートプロファイルを作成します。

∭応答アトリビュートプロファイル 新規追加			
プロファイル名	ns430reply		

応答アトリビュート一覧の「ns430reply」の新規追加からアトリビュートとして「Session-Timeout」を 選択し、値として「180」を設定しています。

■応答アトリビュート 新規追	1九0		
プロファイル名	ns430reply		
アトリビュート	Session-Timeout	×	
値	180		

[ユーザプロファイル]

作成したユーザ基本情報,応答アトリビュートを選択して NS-430 用のユーザプロファイルを作成します。

■ユーザプロファイル 新き	追加
プロファイル名	ns430user
基本	ns430basic 💌
izie	指定しない 💟
証明書	指定しない 💌
応答	ns430reply 💌
グループ	指定しない 💌

〈ユーザ〉

[ユーザ]

NS-430 用のユーザ ID/パスワードを設定します。ユーザ ID/パスワードは、認証する端末の MAC アドレ スを設定します。

NS-430から RADIUS サーバにユーザ ID/パスワードを送信する際には MAC アドレスの英文字は全て大文字 になります。

プロファイルはユーザプロファイルで作成した「ns430user」を選択します。

Ⅲユーザ 新規追加	
ユーザロ	00-80-6D-71-FF-00
パスワード	00-80-6D-71-FF-00
プロファイル	ns430user 👻
■固定IPアドレス払い出し	
IPアドレス	
ネットマスク	
<u>∭</u> アカウントのロック	
ロック	💿 ロックしない 🍥 ロックする

その他設定が必要なユーザを登録後、以下のように表示されます。

No.	lock	ユーザID	プロファイル	IPアドレス	言羊糸田	証明書
		user	xruser		表示	
		00-80-6D-71-FF-00	ns430user		表示	
		00-80-6D-72-FF-00	ns430user		表示	

<<RADIUS>>

〈サーバ〉

[起動・停止]

RADIUS サーバを起動し設定を反映させます。

記動·停止	
	現在の状態
	停止中
	起動

10. QoS 設定

10-1. 帯域制限

XRではTBFを利用することにより帯域制限を行うことができます。 本設定例では帯域を10000Kbps(10Mbps)に制限しています。

10-1-1. 構成図



10-1-2. 設定例

<<インタフェース設定>>

[Ethernet0の設定]

IPアドレスに「192.168.10.1」を設定します。

◎固定アド	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	
ODHOPH	ーパから取得	
ホスト名		
мартрия	1	
IPマズ (この)	カレード(ip masq) ドートで使用するIPアドレスに変換して通信を行います)	
27-	トフルパケットインスペクション(spi)	
🗆 si	PI で DROP したパケットのLOGを取得	
proxy :	qte	
Directed Broadcast		

[Ethernet1の設定]

IP アドレスに「192.168.20.1」を設定します。

●固定アド	シレスで使用
IPアドレス	192.168.20.1
ネットマスク	255.255.255.0
MTU	1500
	ーバから取得
ホ가名	
мартя из	2
IPマス (この)	カレード(ip mesq) ボートで使用するIPアドレスに変換して通信を行います)
27-	トフルパケットインスペクション(spi)
□ s	PI で DROP したパケットのLOGを取得
proxy :	arp
Directo	ed Broadcast

<<QoS 設定>>

<QoS 詳細設定>

[Interface Queueing 設定]

eth1 で利用するキューイング方式として「tbf」を選択し、制限 Rate「10000 Kbit/s」(10Mbps), Buffer Size「20k byte」を設定しています。

**TBF とは帯域制御方法の一つでトークンバケツにトークンをある一定の速度(トークン速度)で収納 していきます。このトークン1個ずつがパケットを1個ずつつかみ、トークン速度を超えない範囲でパ ケットを送信していきます。(帯域制限を行う場合に利用されます)

Interface名	eth1
Queueing Discipline	tbf 💌
pfifo queue limit (pfifc)選択時有効)	
TBF	Parameter設定
制服用ate	10000 Kbit/s
Buffer Size	20k byte
Limit Byte (takenが利用できるようになるまで Queueing可能なbyte教)	byte

【QoS 機能】

QoS 簡易設定・詳細設定を有効にします。

※動作中の場合は、一度「無効」→「有効」を行ってください。

10-2. 帯域制御(簡易 QoS 設定と詳細 QoS 設定の利用)

XR では簡易 QoS 機能以外により詳細な設定を可能にする詳細 QoS 設定を実装しています。これによりより細かい設定ができるようになっています。

本設定例ではキューイング方式は CBQ, TBF, SFQ を利用しています。

10-2-1. 構成図



10-2-2. 設定例

本設定例の制御条件は以下のようになります。

- a. 10000kbps, 20000kbps, 70000kbpsの3つのクラスを作成します。
- b. 10000kbps, 20000kbpsのクラスでは「TBF」を行います。
- c. 70000kbps のクラスでは「SFQ」を行います。
- d. 送信元 IP アドレスが 192.168.10.10 のパケットを 10000Kbps のクラスに送ります。
- e. 送信元 IP アドレスが 192.168.10.11 で送信元ポートが TCP 80 番のパケットを 20000Kbps のクラス に送ります。
- f. その他の通信(dとeで選別したパケット以外)は70000Kbpsのクラスに送ります。

<<インタフェース設定>>

[Ethernet0の設定]

IPアドレスに「192.168.10.1」を設定します。

 固定ア 	シレスで使用
IPアドレス	192.168.10.1
ネットマスク	255.255.255.0
MTU	1500
	ーバから取得
ホスト名	
мартир	2
IPマス (この)?	カレード(ip masq) ボートで使用するIPアドレスに変換して通信を行います)
27-	トフルパケット インスペクション(spi)
□s	PI で DROP したパケットのLOGを取得
proxy	arp
Direct	ed Broadcast

[Ethernet1の設定]

IPアドレスに「192.168.20.1」を設定します。

固定 ア	レスで使用
IPアドレス	192.168.20.1
ネットマスク	255.255.255.0
MTU	1500
	ーバから取得
ホスト名	
мартир	4
Pマス (この)	カレード(ip masq) ドートで使用するIPアドレスに変換して通信を行います) トフルバケットインスペクション(spi)
	PI で DROP したパケットのLOGを取得
proxy :	arp
Directe	ed Broedcest

<<QoS 設定>>

<QoS 簡易設定>

[回線帯域設定]

eth1 インタフェースの回線帯域を設定します。本設定例では「100000Kbit/s」(100Mbps)を設定しています。



[QoS 簡易設定(登録・編集)]

送信元 IP アドレスが 192.168.10.10 の通信に「10000Kbit/s」(10Mbps)を割り当てる設定を行います。 帯域は借用しません。

設定番号		2				
クラス帯域	10000 Kbit/s [必》					
インターフェー ス名	eth1					
プロトコル番号 (*)		(1-255)				
送信元⊩アドレス(*)	192.168.10.10/32					
送信元ポート番号 (*)	(1-65535)					
饱先IPアドレス(*)						
砲先ポート (*)		(1-65535)				
憂先度	1 (1-8) [必須]				
带域借用	0する	⊙ しない				

[QoS 簡易設定(登録・編集)]

送信元 IP アドレスが 192.168.10.11 で送信元ポートが TCP 80 番の通信に「20000Kbit/s」(20Mbps)を割 り当てる設定を行います。帯域は借用しません。

20000 eth1	Kbit/s [必須				
eth1	(1.055)				
6	(1.055)				
	6 (1-255)				
192.168.10.11/32					
80 (1-65535)					
	(1-65535)				
1 0	-8) [必須]				
Ota	●しない				
	80 80 1 0 可する (項目以上指				

設定後は以下のように表示されます。

				(1)9-	-フェース名 eth1 切替/回線帯域設定] 回線带域 1 【 情報	00000 Kbit/ 表示	5			
	クラ ス	親 クラ ス	帯域	プロトコ ル	送信元 IP <i>T</i> ドレス	送信元 ポート番 号	宛先 IPアド レス	宛先 ポート番 号	優先度	帯域借用	操作
1	1	0	100000						1	しな い	首唱金
2	10	1	10000		192.168.10.10/32				1	しな い	<u>編集</u> , 削 隂
3	11	1	20000	6	192.168.10.11/32	80			1	しな い	<u>編集</u> , 削 除

<QoS 詳細設定>

[パケット分類設定]

[パケット入力時の設定]

[No.1]

QoS 簡易設定ではクラス分けを行う際にプロトコル, IP アドレス, ポート番号を設定する必要がありま したが、条件を特に指定せず eth0 で受信したその他のパケットに対しても別途クラスを設定します。 ここでは eth0 インタフェースで受信したパケットに対しては「mark」「1」とする設定を行います。

設定番号	設定番号 1								
	パケット分類条件								
プロトコル	(Protocol番号)	□ Not条件							
送信元アドレス		□ _{Not条件}							
送信元ポート	(ボート番号/範囲指定:で番号)連結)	□ _{Not条件}							
宛先アドレス		□ _{Not条件}							
宛先ボート	(ポート番号/範囲指定は:で番号連結)	□ Not条件							
インターフェース	eth0	□ _{Not条件}							
TOS/MARK/ DSCP值	 ○ TOS ○ MARK ○ DSCP ○ マッチ条件無効 上記で選択したマッチ条件に対応する設定値 	TOS Bitf値 hex CMormal Service 2:Minimize cost 4:Maximize Reliability 8:Maximize Throughput 10:Minimize Delay MARK(値 (1-999) DGOP Bit値 hex(0-3f)							

	TOS/MARK/DSCP値の設定 設定対象 OTOS/Precedence OMARK ODSCP							
設定対象								
設定値	・MARK設定(1-999) 1 ・TOS/Precedence設定 選択して下さい ▼ TOS Bit 選択して下さい ▼ Precedence Bit ・DSOP設定 選択して下さい ▼ DSOP Bit							

設定後は以下のように表示されます。

				パケット [<u>切琴:ロー</u>	- 入力時の設う - カルパケット出力	定 時]			
				パケット分類条件				設定値	
	プロトコル	送信元アドレ ス	送信元ポート	宛先アドレ ス	宛先ポート	インター フェース	TOS/MARK/ DSCP値	TOS/MARK/ DSCP値	Configure
1						eth0		MARK 1	Edit.Remove

[CLASS 分けフィルタ設定]

PriorityはすでにQoS簡易設定で設定済みの設定を優先させるため、それよりも大きい値を設定します。 (本設定例では「3」を設定しています)

またパケット分類設定で作成した情報を利用するため、Marking 情報によるフィルタを選択し、先ほど 設定した Mark 値「1」を設定します。

設定番号	3
Description	
Priority	3 (1-999)
□パケットへッダ	情報によるフィルタ
プロトコル	(Protocol番号)
送信元アドレス	
送信元ポート	(水-ト番号)
宛先アドレス	
宛先ボート	(水-ト番号)
TOS值	(hex0-fe)
DSCP值	(hex0-3f)
☑ Marking 情報に	よるフィルタ
Mark值	1 (1-999)

設定後は以下のように表示されます。(QoS 簡易設定で設定した項目も含まれます)

100	FilterType	Description	Priority	プロ トコ ル	送信元アドレス	送信元 ポート	宛先 アドレ ス	宛先 ボート	TOS 値	DSCP 値	MARK 値	Configure
1	Packet Head		1		192.168.10.10/32							Edit.Remove
2	Packet Head		2	6	192.168.10.11/32	80						Edit.Remove
3	Mark		3								1	Edit.Remove

[CLASS 設定]

親クラスの下に置くクラスの中で、QoS 簡易設定で指定した通信以外のその他の通信に関するクラスを 設定します。

CLASS 分けフィルタ設定で設定したフィルタ No.3 (パケット分類設定で設定したその他の通信)の通信 に「70000Kbit/s」(70Mbps)を割り当てる設定を行います。帯域は借用しません。

Description	
Interface名	eth1
Class ID	12
親dass ID	1
Priority	1
Rate設定	70000 Kbit/s
Class内Average Packet Size設定	1000 byte
Maximum Burst設定	100
Bounded設定	● 有効 ● 無効
Filter設定	1.3 2. 3. 4. 5.
(Filter番号を入力してください)	6. 7. 8. 9. 10.

設定後は以下のように表示されます。(QoS 簡易設定で設定した項目も含まれます)

	Description	Interface名	ID	親 CLASS ID	Priority	Rate	平均 Packet Size	Maximum Burst	Configure
1		eth1	1	0	1	100000Kbit/s	1000	100	Edit.Remove
2		eth1	10	1	1	10000Kbit/s	1000	100	Edit.Remove
3		eth1	11	1	1	20000Kbit/s	1000	100	Edit.Remove
4		eth1	12	1	1	70000Kbit/s	1000	100	Edit.Remove

[CLASS Queueing 設定]

CLASS 設定で設定したクラス内で更にキューイングを行うため、CLASS Queueing 設定を行います。 [No. 1]

ID「10」のクラスで QDISC 番号を「20」とし、キューイング方式として「tbf」を選択し、制限 Rate「10000 Kbit/s」(10Mbps), Buffer Size「20k byte」を設定しています。

**TBF とは帯域制御方法の一つでトークンバケツにトークンをある一定の速度(トークン速度)で収納 していきます。このトークン1個ずつがパケットを1個ずつつかみ、トークン速度を超えない範囲でパ ケットを送信していきます。(帯域制限を行う場合に利用されます)

Description	
Interface名	eth1
QDISC番号	20
MAJORID	1
class ID	10
Queueing Discipline	tbf 💌
pfifolimit (PFIFO選択時有効)	
TBF Pa	rameter設定
策II限Rate	10000 Кыт/я
Buffer Size	20k byte
Limit Byte (takenが利用できるようになるまで queuing可能なbyte数)	byte

[No. 2]

ID「11」のクラスで QDISC 番号を「21」とし、キューイング方式として「tbf」を選択し、制限 Rate「20000 Kbit/s」(20Mbps), Buffer Size「40k byte」を設定しています。

Description	
Interface名	eth1
QDISC番号	21
MAJORID	1
class ID	11
Queueing Discipline	tbf 💌
pfifo limit (FFIFO)選択時有効)	
TBF P	arameter設定
制限Rate	20000 Kbit/s
Buffer Size	40k byte
Limit Byte (tokenが利用できるようになるまで queuing可能なbyte数)	byte

[No.3]

ID「12」のクラスで QDISC 番号を「22」とし、キューイング方式として「sfq」を選択しています。 ※SFQ とはラウンドロビンで順番にトラフィックが送信され、ある特定のトラフィックが他のトラフィ ックを圧迫してしまうことがなくなり、どのトラフィックも公平に送信されるようになります。

Description	
Interface名	eth1
QDISC番号	22
MAJORID	1
dass ID	12
Queueing Discipline	sfq 💌

設定後は以下のように表示されます。

Description	Interface名	QDISC 番号	種別	CLASS ID	MAJOR 番号	Configure
1	eth1	20	tbf	10	1	Edit.Remove
2	eth1	21	tbf	11	1	Edit.Remove
3	eth1	22	sfq	12	1	Edit.Remove

【QoS 機能】

QoS 簡易設定・詳細設定を有効にします。

※動作中の場合は、一度「無効」→「有効」を行ってください。

QoS销息設定 QoS詳細設定	⊙有効	○無効
--------------------	-----	-----

10-2-3. 設定例補足(クラス階層図)

本設定例は以下のようなクラス階層になっています。



10-3. PPPoE での帯域制御+優先制御

本設定例では PPPoE 接続で WEB サーバを公開し、帯域制御,優先制御を行います。 本設定例ではキューイング方式は CBQ, TBF, PQ, SFQ を利用しています。

10-3-1. 構成図



10-3-2. 設定例

本設定例の制御条件は以下のようになります。

- a. 20000kbps, 10000kbps, 15000kbpsの3つのクラスを作成します。
- b. 20000kbps のクラスでは「TBF」を行います。
- c. 10000kbps のクラスでは「PQ」を行います。
- d. 15000kbps のクラスでは「SFQ」を行います。
- e. 送信元 IP アドレスが 192.168.10.100 で送信元ポートが TCP 80 番のパケットを 20000Kbps のクラ スに送ります。
- f. 宛先ポートが telnet (TCP 23番), www (TCP 80番) のパケットを 10000Kbps のクラスに送ります。
- g. 10000Kbps のクラスでは PQ による優先制御を行い、優先度は telnet (TCP 23 番) > www (TCP 80 番) とします。
- h. その他の通信(eとfで選別したパケット以外)は15000Kbpsのクラスに送ります。

<<インタフェース設定>>

[Ethernet0の設定]

IPアドレスに「192.168.10.1」を設定します。

固定 ア	シンスで使用
₽₽Ÿ₽₽ス	192.168.10.1
ネットマスク	255.255.255.0
MTU	1500
	ーバから取得
ホスト名	
мартри	2
IPマス (この)	カレード(ip masq) ボートで使用するIPアドレスに変換して通信を行います)
- 7	トフルパケットインスペクション(spi)
□s	PI で DROP したパケットのLOGを取得
proxy	arp
Direct	ed Broadcast

QoS 設定

[Ethernet1の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※PPPoE で接続する場合には "ppp"という論理インタフェースを自動的に生成し、この論理インタフェースを使って PPPoE 接続を行います。

◎ 固定ア	レスで使用
IPアドレス	0
ネットマスク	255.255.255.0
мти	1500
	ーバから取得
ホ가名	
мартир	2
IPマス (この)	カレードûp masq) ボートで使用するIPアドレスに変換して通信を行います)
🗌 72-	トフルパケットインスペウション(spi)
□s	PI で DROP したパケットのLOGを取得
proxy	arp
Direct	ed Broadcast

<<PPP/PPPoE 設定>>

[接続先設定]

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

ユーザロ	test1@centurysys
パスワード	test1pass

[接続設定]

ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

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	OEther0 OEther1 OEther2 OBRI(64K) OBRI MP(128K) OLeased Line(64K) OLeased Line(128K) ORS2320
接続形態	○ 手動接続 ○ 常時接続 ○ スケジューラ接続
RS2320/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の再接続性を高めるために、PPPoE 特殊オプションを設定します。

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

接続が完了した場合、回線状態が以下のように表示されます。

回換状況 主回換で接続しています

<<フィルタ設定>>

[転送フィルタ]

LAN 上にある WEB サーバをインターネットからアクセス可能にするための設定をします。

インターネットから宛先 IP アドレス「192.168.10.100」で WEB サーバ (TCP ポート 80 番) 宛のパケットを許可します。

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	ICMP type/code	送信元MACアドレス	LOG
ppp0	パケット受信時 ⊻	許可 💌	top 💌			192.168.10.100	80] 🗆

<<NAT 設定>>

[バーチャルサーバ]

LAN 上にある WEB サーバをインターネットからアクセス可能にするための設定をします。

インターネットから「10.10.10.1」で TCP ポート 80 番宛てのパケットを受信した場合は、 「192.168.10.100」に転送します。

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
192.168.10.100	10.10.10.1	tcp 💌	80	рррО

<QoS 詳細設定>

[パケット分類設定]

[パケット入力時の設定]

[No.1]

eth0 インタフェースで受信した送信元 IP アドレス「192.168.10.100」プロトコル番号 6 (TCP) 送信元ポ ート 80 番のパケットに対しては「mark」「1」とする設定を行います。

設定番号	1					
	パケット分類条件					
プロトコル	6 (Protocol番号)	□ _{Not} 条件				
送信元アドレス	192.168.10.100	□ _{Not条件}				
送信元ポート	80 (ボート番号/範囲指定:で番号連結)	□ Not条件				
宛先アドレス		□ _{Not} 条件				
宛先ボート	(ボート番号/範囲指定は:で番号連結)	□ Not条件				
インターフェース	eth0	□ _{Not条件}				
TOS/MARK∕ DSCPI₫	 ○ TOS ○ MAFK ○ DSCP ○ マッチ条件無効 上記で選択したマッチ条件に対応する設定値 	TOS Bitf値 hex ONormal Service 2:Minimize cost 4:Maximize Reliability 8:Maximize Reliability 8:Maximize Delay MARK(値 (1-999) DGCP Bitf値 hex(0-3行				

	TOS/MARK/DS	SCP値	の設定				
設定対象							
設定値	-MARK設定(1-999) 1 -TOS/Precedence設定 選択して下さい 選択して下さい -DSCP設定	~	TOS Bit Precedence Bit				

[No.2]

eth0 インタフェースで受信したプロトコル番号 6(TCP)宛先ポート 23 番のパケットに対しては「mark」 「2」とする設定を行います。

設定番号	2	
	パケット分類条件	
プロトコル	6 (Protocol番号)	□ _{Not条件}
送信元アドレス		□ _{Not条件}
送信元ポート	(ボート番号/範囲指定:で番号連結)	□ _{Not条件}
宛先アドレス		□ _{Not采件}
宛先ボート	23 (ボート番号/範囲指定は:で番号連結)	□ _{Not条件}
インターフェース	eth0	□ _{Not条件}
tos/MARK/ DscPli i	 ○ TOS ○ MARK ○ DSCP ○ マッチ条件無効 上記で選択したマッチ条件に対応する設定値 	TOS Btt値 hex ONormal Service 2:Mnimize cost 4:Maximize Reliability 8:Maximize Throughput 10:Mnimize Delay MARK値(1-999) DGCP Btf値 hex(0-3行

	TOS/MARK/DSCP値の設定
設定対象	
設定値	・MARK設定(1-999) 2 ・TOS/Precedence設定 選択して下さい ● TOS Bit 選択して下さい ● Precedence Bit ・DSCP設定 選択して下さい ● DSOP Bit

[No.3]

eth0 インタフェースで受信したプロトコル番号 6(TCP)宛先ポート 80 番のパケットに対しては「mark」 「3」とする設定を行います。

設定番号	3					
	パケット分類条件					
プロトコル	6 (Protocol番号)	□ _{Not条件}				
送信元アドレス		□ Not 条件				
送信元ポート	(ボート番号/範囲指定:で番号連結)	□ Not条件				
宛先アドレス		□ Not 条件				
宛先ボート	80 (ボート番号/範囲指定は:で番号連結)	□ _{Not条件}				
インターフェース	eth0	□ _{Not条件}				
TOS/MARK/ DSCP值	 ○ TOS ○ MAFIK ○ DSCP ○ マッチ条件無効 上記で選択したマッチ条件に対応する設定値 	TOS Bt/値 hex Othermal Service 2:Mnimize cost 4:Maximize Reliability 8:Maximize Throughput 10:Mnimize Delay MARK値(1-999) DGCP Bt/値 hex(0-3f)				

	TOS/MARK/DSCP値の設定						
設定対象	O TOS/Precedence						
設定値	・MAFK設定(1-999) 3 ・TOS/Precedence設定 選択して下さい 選択して下さい ・DSOP設定 選択して下さい ▼ DSO	TOS Bit Precedence Bit					

[No.4]

上記 No. 1, 2, 3 以外の eth0 インタフェースで受信したパケットに対しては「mark」「4」とする設定を 行います。

設定番号	4					
	パケット分類条件					
プロトコル	(Protocol番号)	□ _{Not条件}				
送信元アドレス		□ _{Not条件}				
送信元ポート	(ポート番号/範囲指定:で番号連結)	□ _{Not条件}				
宛先アドレス		□ _{Not条件}				
宛先ボート	(ボート番号/範囲指定は:で番号連結)	□ _{Not条件}				
インターフェース	eth0	□ _{Not条件}				
TOS/MARK/ DSCP值	 ○ TOS ○ MAFix ○ DSCP ○ マッチ条件無効 上記で選択したマッチ条件に対応する設定値 	TOS Bt/値 hex. CtNormal Service 2:Mnimize cost 4:Maximize Reliability 8:Maximize Throughput 1:OMnimize Delay MARK/値 (1-999) DSCP Bt/値 bax(10-31)				

	TOS/MARK/DSCP値の設定
設定対象	
設定値	・MARK設定(1-999) 4 ・TOS/Precedence設定 選択して下さい 選択して下さい ・DSCP設定 選択して下さい ・DSCP設定 選択して下さい ・DSCP Bit

設定後は以下のように表示されます。

				バケットス [切琴:ローカ	、力時の設定 ルパケホ出力®	<u>-</u> 				
			パケ	水分類条件				設定値	8	
200	プロトコ ル	送信元アドレス	送信元ポー ト	宛先アドレ ス	宛先ポート	インター フェース	TOS/MARK/ DSCP値	TOS/MA DSCP(RK/ 直	Configure
1	6	192.168.10.100	80			eth0		MARK	1	Edit.Remove
2	6				23	eth0		MARK	2	Edit.Remove
3	6				80	eth0		MARK	3	Edit.Remove
4						eth0		MARK	4	Edit.Remove

[CLASS 分けフィルタ設定]

[No.1]

パケット分類設定で作成した Mark 値「1」を No.1 に設定します。Priority は「1」を設定しています。

設定番号	1					
Description	src19216810100srcport80					
Priority	1 (1-999)					
□パケットへッタ	『情報によるフィルタ					
プロトコル	(Protocol番号)					
送信元アドレス						
送信元ポート	(ポート番号)					
宛先アドレス						
宛先ポート	(ポート番号)					
TOS值	(hex0-fe)					
DSCP值	0nex0-31)					
☑ Marking 情報	こよるフィルタ					
Mark值	1 (1-999)					

[No. 2]

パケット分類設定で作成した Mark 値「2」を No.2 に設定します。Priority は「2」を設定しています。

設定番号	2							
Description	dstport23							
Priority	2 (1-999)							
□ パケットヘッダ	□パケットヘッダ情報によるフィルタ							
プロトコル	(Protocol番号)							
送信元アドレス								
送信元ポート	(ポート番号)							
宛先アドレス								
宛先ポート	(ボート番号)							
TOS值	(hex0-fe)							
DSCP值	(hex0-3f)							
☑ Marking 情報	✓ Marking情報によるフィルタ							
Mark值	2 (1-999)							

[No.3]

パケット分類設定で作成した Mark 値「3」を No.3 に設定します。Priority は「3」を設定しています。

設定番号	3							
Description	dstport80							
Priority	3 (1-999)							
ロバケットヘッタ	「情報によるフィルタ							
プロトコル	(Protocol番号)							
送信元アドレス								
送信元ポート	(ボート番号)							
宛先アドレス								
宛先ポート	(ポート番号)							
TOS值	(hex0-fe)							
DSCP值	(hex0-3f)							
☑ Marking 情報	✓ Marking情報によるフィルタ							
Mark值	3 (1-999)							

[No. 4]

パケット分類設定で作成した Mark 値「4」を No.4 に設定します。Priority は「4」を設定しています。

設定番号	4					
Description	other					
Priority	4 (1-999)					
□パケットへッ5	『情報によるフィルタ					
プロトコル	(Protocol番号)					
送信元アドレス						
送信元ポート	(ポート番号)					
宛先アドレス						
宛先ポート	(ポート番号)					
TOS值	(he×0-fe)					
DSCP值	(hex0-3f)					
☑ Marking 情報	✓ Marking情報によるフィルタ					
Mark值	4 (1-999)					

設定後は以下のように表示されます。

	FilterType	Description	Priority	プロ トコ ル	送信 元ア ドレス	送信元 ポート	宛先 アドレ ス	宛先 ポート	TOS 値	DSCP 値	MARK 値
1	Mark	src19216810100srcport80	1								1
2	Mark	dstport23	2								2
3	Mark	dstport80	3								3
4	Mark	other	4								4

[Interface Queueing 設定]

ppp0で利用するキューイング方式として「cbq」を選択します。

Interface名	ppp0	
Queueing Discipline	cbq 💌	

回線帯域は接続回線の物理的な帯域幅を設定します。(本設定例では 100000Kbps としています)

OBQ Parameter設定					
回線带域	100000 Kbit/s				
平均パケットサイズ	1000 byte				

設定後は以下のように表示されます。

12	Interface名	種別	制限Rate	Buffer	回線帯域	平均Packet Size
1	pppO	cbq			100000Kbit/s	1000

[CLASS 設定]

[No.1]

親クラスの設定をします。Rateは「45000Kbit/s」(45Mbps)を割り当てています。

Description	parent				
Interface名	ppp0				
Class ID	1				
親dass ID	0				
Priority	1				
Rate設定	45000 Kbit/s				
Class内Average Packet Size設定	1000 byte				
Maximum Burst設定	100				
Bounded設定	◎ 有効 ○ 無効				
Filter設定 (Filter番号を入力してくたさい)	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.				

[No. 2]

CLASS 分けフィルタ設定で設定したフィルタ No.1 (パケット分類設定で設定した送信元 IP アドレス「192.168.10.100」送信元ポート TCP 80 番の通信)の通信に「20000Kbit/s」(20Mbps)を割り当てる設 定を行います。帯域は借用しません。

Description	child10				
Interface名	ppp0				
Class ID	10				
親dass ID	1				
Priority	1				
Rate設定	20000 Kbit/s				
Class内Average Packet Size設定	1000 byte				
Maximum Burst設定	100				
Bounded設定	◎ 有効 ○ 無効				
Filter設定 (Filter番号を入力してください)	1.1 2. 3. 4. 5. 6. 7. 8. 9. 10.				

[No.3]

CLASS 分けフィルタ設定で設定したフィルタ No. 2, 3(パケット分類設定で設定した宛先ポート TCP 23,80 番の通信)の通信に「10000Kbit/s」(10Mbps)を割り当てる設定を行います。帯域は借用しません。

Description	child11					
Interface名	ррр0					
Class ID	11					
親dass ID	1					
Priority	1					
Rate設定	10000 Kbit/s					
Class内Average Packet Size設定	1000 byte					
Maximum Burst設定	100					
Bounded設定	● 有効 ● 無効					
Filter設定 (Filter番号を入力してください)	1.2 2.3 3. 4. 5. 6. 7. 8. 9. 10.					

[No.4]

CLASS 分けフィルタ設定で設定したフィルタ No.4 (パケット分類設定で設定したその他の通信)の通信 に「15000Kbit/s」(15Mbps)を割り当てる設定を行います。帯域は借用しません。

Description	child12				
Interface名	ррр0				
Class ID	12				
親dass ID	1				
Priority	1				
Rate設定	15000 Kbit/s				
Class内Average Packet Size設定	1000 byte				
Maximum Burst設定	100				
Bounded設定	◎ 有効 ○ 無効				
Filter設定 (Filter番号を入力してくたさい)	1.4 2. 3. 4. 5.				

設定後は以下のように表示されます。

	Description	Interface名	ID	親 CLASS ID	Priority	Rate	平均 Packet Size	Maximum Burst
1	parent	pppO	1	0	1	45000Kbit/s	1000	100
2	child10	pppO	10	1	1	20000Kbit/s	1000	100
3	child11	pppO	11	1	1	10000Kbit/s	1000	100
4	child12	pppO	12	1	1	15000Kbit/s	1000	100

[CLASS Queueing 設定]

CLASS 設定で設定したクラス内で更にキューイングを行うため、CLASS Queueing 設定を行います。 [No. 1]

ID「10」のクラスで QDISC 番号を「20」とし、キューイング方式として「tbf」を選択し、制限 Rate「20000 Kbit/s」(20Mbps), Buffer Size「40k byte」を設定しています。

**TBF とは帯域制御方法の一つでトークンバケツにトークンをある一定の速度(トークン速度)で収納 していきます。このトークン1個ずつがパケットを1個ずつつかみ、トークン速度を超えない範囲でパ ケットを送信していきます。(帯域制限を行う場合に利用されます)

Description	qdisc20			
Interface名	ррр0			
QDISC番号	20			
MAJORID	1			
dass ID	10			
Queueing Discipline	tbf 💌			
ptifolimit (PFIFO選択時有効)				
TBF	Parameter設定			
集IIB民Rate	20000 Kbit/s			
Buffer Size	40k byte			
Limit Byte (tokenが利用できるようになるまで queuing可能なbyte数)	byte			

[No. 2]

ID「11」のクラスで QDISC 番号を「21」とし、キューイング方式として「pq」を選択し、Band 数は初期 値の 3 バンド(3 クラス)を利用しています。

CLASS 分けフィルタの設定番号とパケットを送るクラス番号(優先度)を関連づけます。

クラス1:送信元ポート TCP 23番

クラス3:送信元ポートTCP 80番

Description	qdisc21		
Interface名	ppp0		
QDISC番号	21		
MAJOR ID	1		
dass ID	11		
Queueing Discipline	pq 💌		

PQ Parameter設定			
最大Band数設定	3 default 3 (2-5)		
priority-map設定	1 2 2 2 1 2 0		
Marking Filterの選択 (PacketヘッダによるFilter設定は選択できません)	FilterNo. Class No. 1. 2 1. 2 1. 2 1. 2 1. 2 1. 2 1. 2 1. 2 1. 2 1. 2 1. 2 1. 2 1. 2 1. 2 10. 10		

[No.3]

ID「12」のクラスで QDISC 番号を「22」とし、キューイング方式として「sfq」を選択しています。 ※SFQ とはラウンドロビンで順番にトラフィックが送信され、ある特定のトラフィックが他のトラフィ ックを圧迫してしまうことがなくなり、どのトラフィックも公平に送信されるようになります。

Description	qdisc22	
Interface咨	рррО	
	22	
MAJOR ID	1	
class ID	12	
Queueine Discipline	sfq 💌	

設定後は以下のように表示されます。

010	Description	Interface名	QDISC 番号	種別	CLASS ID	MAJOR 番号
1	qdisc20	pppO	20	tbf	10	1
2	qdisc21	pppO	21	pq	11	1
3	qdisc22	pppO	22	sfq	12	1

【QoS 機能】

QoS 簡易設定・詳細設定を有効にします。

※動作中の場合は、一度「無効」→「有効」を行ってください。

QoS 筋息設定 QoS詳細設定	⊙有効	○無効
----------------------------	-----	-----

10-3-3. 設定例補足(クラス階層図)

本設定例は以下のようなクラス階層になっています。



11. ソースルート設定

11-1. PPPoE でのソースルートの利用

ソースルート機能を使うことで、外部へアクセスするホスト/ネットワークごとにアクセス回線を選択す ることができます。これにより複数のインターネット接続をおこなって負荷分散が可能となります。

11-1-1. 構成図


11-1-2. 設定例

送信元 IP アドレス「192.168.10.100/24」はプロバイダ A を、「192.168.10.200/24」はプロバイダ B を利用するように設定します。(ソースルートは「192.168.10.200/24」に対してのみ設定しています)

〈〈インタフェース設定〉〉

[Ethernet0の設定] IPアドレスに「192.168.10.1」を設定します。

◎固定ア	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
	ーバから取得
ホ가名	
мартрия	2
IPマス (この)?	カレード(ip masq) ボートで使用するIPアドレスに変換して通信を行います)
27-	トフルパケットインスペウション(spi)
□ s	PI で DROP したパケットのLOGを取得
proxy	arp
Direct:	ed Broadcast

[Ethernet1の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※PPPoE で接続する場合には "ppp" という論理インタフェースを自動的に生成し、この論理インタフェ ースを使って PPPoE 接続を行います。

● 固定アト	レスで使用
IPアドレス	0
ネットマスク	255.255.255.0
мти	1500
ODHOPH	ーバから取得
ホ가名	
мартия	2
□ IPマス (この)	カレード(ip masq) ドートで使用するIPアドレスに変換して通信を行います)
27-	トフルパケットインスペウション(spi)
□s	PI で DROP したパケットのLOGを取得
proxy	arp
Direct:	ed Broadcast

<<PPP/PPPoE 設定>>

[接続先設定1]

PPPoE 接続(主回線)で使用するユーザ ID とパスワードを設定します。

ユーザロ	test1@centurysys
パスワード	test1pass

[接続先設定2]

PPPoE 接続(マルチ回線#2)で使用するユーザ ID とパスワードを設定します。

ユーザロ	test@example.com	
パスワード	testpass	

[接続設定]

PPPoE(主回線)に関する設定をします。

本設定例では、ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」 にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有 効」に設定します。

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	OEther0 OEther1 OEther2 OBRI(64K) OBRI MP(128K) OLeased Line(64K) OLeased Line(128K) ORS232C
接続形態	○ 手動接続 ● 常時接続 ● スケジューラ接続
RS2320/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 (マルチ接続#2) に関する設定をします。

本設定例では、ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」 にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有 効」に設定します。

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
接続ポート	OEther0 OEther1 OEther2 OER1(64K) OBRI MP(128K) OLeased Line(64K) OLeased Line(128K) ORS232C
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

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。

PPPoE特殊オプション (今回道共通)	✓ 回線接続時に前回のPPPcE セッションのPADTを強制送出 ✓ 非接続Session のIPv4Packet受信時にPADTを強制送出
	✓ 非接続SessionのLCP-EchoRequest受信時ICPADTを強制送出

接続が完了した場合、回線状態が以下のように表示されます。

回線状態 主回線で整装しています マルチ接数 ₦2で接続しています

<<ソースルート設定>>

[ソースルートのテーブル設定]

ソースルートで利用する際の上位ルータの IP アドレスおよび DEVICE を設定します。 本設定では ppp2 インタフェースのみ設定しています。

テーブルND	IP	DEMCE
1		ppp2

[ソースルートのルール設定]

送信元 IP アドレス,送信先 IP アドレス(限定しない場合は空欄)およびソースルートのテーブル設定で 設定したテーブル No(本設定例では1)を設定します。

11-11NO	送信元ネットワークアドレス	送信先ネットワークアドレス	ツースルートのテーブル№
1	192.168.10.200		1

11-2. Ether でのソースルートの利用

ソースルート機能を使うことで、外部へアクセスするホスト/ネットワークごとにアクセス回線を選択す ることができます。

本設定例ではインターネット接続しているルータ配下の XR でソールルート機能を利用して負荷分散を 行っています。

11-2-1. 構成図



11-2-2. 設定例

送信元 IP アドレス「192.168.10.100/24」はプロバイダ A を、「192.168.10.200/24」はプロバイダ B を利用するように設定します。(ソースルートは「192.168.10.200/24」に対してのみ設定しています) ※本設定例ではソースルートを設定するルータのみ設定を記載しています。

〈〈インタフェース設定〉〉

[Ethernet0の設定] IPアドレスに「192.168.10.1」を設定します。

③固定アド	レスで使用
IPアドレス	192.168.10.1
ネットマスク	255.255.255.0
мти	1500
	ーバから取得
ホスト名	
маоркия	2
□ IPマス (この)	カレード(ip masq) ドートで使用するIPアドレスに変換して)通信を行います) トフルパケットインスペクション(spi)
s	PIでDROPしたパケナのLOGを取得
proxy :	arp
Directe	ad Broadcast

[Ethernet1の設定]

IP アドレスに「192.168.20.1」を設定します。

固定 ア ド	レスで使用
IPアドレス	192.168.20.1
ネットマスク	255.255.255.0
MTU	1500
	ーバから取得
ホスト名	
мартрия	2
IPマス (この)	カレード(ip masq) ドートで使用するIPアドレスに変換して通信を行います)
27-	トフルパケットインスペクション(spi)
□ s	PI で DROP したパケットのLOGを取得
proxy :	anp
Directo	ed Broadcast

[その他の設定]

デフォルトゲートウェイを設定します。

デフォルトゲートウェイの設定	
192.168.20.11	

〈〈ソースルート設定〉〉

[ソースルートのテーブル設定]

ソースルートで利用する際の上位ルータの IP アドレスおよび DEVICE を設定します。

本設定では IP アドレス「192.168.20.12」, DEVICE「eth1」を設定します。

テーブルNO	IP	DEMCE	
1	192.168.20.12	eth1	

[ソースルートのルール設定]

送信元 IP アドレス,送信先 IP アドレス(限定しない場合は空欄)およびソースルートのテーブル設定で 設定したテーブル No(本設定例では1)を設定します。

11-11NO	送信元ネットワークアドレス	送信先ネットワークアドレス	ソースルートのテーブルNO
1	192.168.10.200		1

12. BGP4 設定

12-1. ネットワークイベント機能 BGP4 切断監視の利用

BGP4 とネットワークイベント機能 BGP4 切断監視を組み合わせて利用することにより、BGP4 の neighbor state 状態を監視し、Neighbor state に変化があった場合にイベントを発生させることができます。本 設定例では BGP4 で Neighbor state が Established へ変化した時に、VRRP の優先度を変更させています。

12-1-1. 構成図



12-1-2. 設定例

XR で AS65001 の BGP スピーカに対して BGP4 による接続ができるよう設定を行います。 またネットイベント機能の BGP4 切断監視を使用し、Neighbor state を監視します。状態変化が発生し た際に VRRP の優先度を変更します。

《XR_A の設定》

〈〈インタフェース設定〉〉

[Ethernet0の設定]

IPアドレスに「10.10.100.1」,ネットマスクに「255.255.255.128」を設定します。



[Ethernet1の設定]

IP アドレスに「10.10.10.1」, ネットマスクに「255.255.255.252」を設定しています。

⑧ 固定ア	シレスで使用
IPアドレス	10.10.10.1
ネットマスク	255.255.255.252
MTU	1500
	トーバから取得
ホオ名	
марти,	2
IPマス (この)	カレードûp masq) ボートで使用するIPアドレスに変換して通信を行います)
77-	トフルパケットインスペクション(spi)
s	PI で DROP したパケットのLOGを取得
proxy	arp
Direct	ed Broadcast

<<各種サービスの設定>>

【ダイナミックルーティング】-> <BGP4>

BGP4 設定前に BGP4 サービスを起動しておきます。

BGP4	〇 停止 💿 起動

<ダイナミックルーティング> -> <BGP4>

[BGP 機能設定]

AS 番号およびルータ ID を設定します。

AS Number	65010 (1-65535)		
Router-10	10.100.100.1 (ex:192.158.0.1)		
Soan Time	5 (s-so)		
connected再配信	○ 有效 ● 無效 raute-map設定		
static儿~卜再配信	○有効 ● 無効 route-mep設定		
RIPルート再配信	○有効 ● 無効 route-map設定		
DSPFルート再配信	○ 有效 ● 無效 route-mop設定		
Distance for routes external to the AS	20 (1-255)		
Distance for routes internal to the AS	200 (1-255)		
Distance for local routes	200 (1-255)		
network import-check	○ 有效 ● 無效		
always-compare-med	○ 有效 ④ 無效		
enfarge-first-as	○ 有效 ④ 無效		
Bestpath AS-Path ignore	○ 有效 ● 無效		
Bestpath med missing-as-worst	○ 有效 ● 無效		
default local-pref	(0-4294967295)		

[BGP4 Neighbor 設定]

対向の BGP スピーカの IP アドレス, AS 番号を設定します。

Neighbor Address	10.10.10.	2	(ex192.168.1.1)
Remote AS Number	65001 (1-65		535)
Keepalive interval	60	60 (0-65535)	
Holdtime	180	(0,3-6	5535)
Next Connect Timer	120	(0-65	535)
default-originate	○有効	○ 有効 ④ 無効	
nexthop-self	○ 有効 ④ 無効		
update-source	(interfaceを指定)		ceを指定)
ebgp-multihop	0	-255)	
soft-reconfiguration inbound	〇有効	⊙無効	
Apply map to incoming routes			(routemap名指定)
Apply map to outbound routes			(routemap名指定)
Filter incoming updates			(ACL名指定)
Filter outgoing updates			(ACL名指定)

[BGP4 Network 設定]

BGP で配信したいネットワークを設定します。

Speficy a network to announce via BGP	10.10.100.0/24	(e×192.168.0.0/24)
backdoor	○ 有効 ④ 無効	

【ダイナミックルーティング】-> <BGP4>

BGP4 を再起動します。



<<各種サービスの設定>>

<VRRP サービス>

[VRRP の設定]

BGPのNeighbor state が Established 以外の時の VRRP 優先度を設定します。

No	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	P7Fレス	インターバル	Auth_Type	password
1	Ether 0 💌	使用しない 💌	51	100	10.10.100.10	1	指定しない 💌	

【VRRP サービス】

VRRP サービスを起動します。

※動作中の場合は、一度「停止」→「起動」を行ってください。

VRRPU-EZ	○停止	⊙起動	

<<ネットワークイベント設定>>

[BGP4 切断監視設定]

監視する BGP スピーカの IP アドレスを指定します。

これがトリガとなります。

ND	enable	トリガー番号	BGP4 Neighbor Address
1		1	10.10.10.2

[VRRP 優先度変更設定]

指定したBGPスピーカとのNeighbor stateがEstablishedになったときのVRRPの優先度を設定します。

NO	ルータロ	優先度		
1	51	200		

[イベント実行テーブル設定]

実行イベントとして「VRRP 優先度」を選択します。

ND	実行イベト設定	オプション設定		
1	VRRP優先度 🛛 🐱	1		

[ネットワークイベント設定]

「トリガ番号」は、この例では「BGP4 切断監視設定」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。

ND	トリガー番号	実行イベントテーブル番号
1	1	1

[ネットワークイベントサービス設定]

この設定例では、「ネットワークイベント」と「BGP4 切断監視」を使用しますので、この二つを起動します。

<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>	⊙ 停止 ○ 起動
<u>MRFP監視</u>	⊙ 傍止 ○ 起動
BGP4切断監視	〇 停止 ④ 起動

<<スタティックルート設定>>

宛先 IP アドレスが「10.10.100.128/25」の時は、配下のルータへパケットを転送するように設定します。

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>
10.10.100.128	255.255.255.128	10.10.100.3	1

《XR_B の設定》

<<インタフェース設定>>

[Ethernet0の設定]

IPアドレスに「10.10.100.2」,ネットマスクに「255.255.255.128」を設定します。



[Ethernet1の設定]

IP アドレスに「10.10.10.5」,ネットマスクに「255.255.255.252」を設定しています。

⑧ 固定アド	レスで使用
IPアドレス	10.10.10.5
ネットマスク	255.255.255.252
мто	1500
	ーバから取得
ホスト名	
мартыра	3
□ IPマズ (この)	カレード(ip masa) ドートで使用するIPアドレスに変換して通信を行います) トラリックセット クィフックロション(mi)
	F プロハウサインスペンションGDD FI で DROP したパケットのLOGを取得
proxy :	arp
Directe	ed Broedcest

<<各種サービスの設定>>

【ダイナミックルーティング】-> <BGP4>

BGP4 設定前に BGP4 サービスを起動しておきます。

BGP4	〇 停止 🧿 起動

<ダイナミックルーティング> -> <BGP4>

[BGP 機能設定]

AS 番号およびルータ ID を設定します。

AS Number	65010 (1-85535)
Rauter-ID	10.100.100.2 (ex 192.166.0.1)
Soan Time	5 (5-60)
connected再配信	○ 有效 ● 無效 raute-map設定
static儿~卜再配信	○ 有效 ● 無效 raute-map設定
RIPルート再配信	○ 有效 ● 無効 raute-map設定
DSPFルート再配信	○ 有效 ● 無效 route-mon設定
Distance for routes external to the AS	20 (1-255)
Distance for routes internal to the AS	200 (1-255)
Distance for local routes	200 (1-255)
network impart-check	○ 有效 ④ 無效
always-compare-med	○ 有效 ● 無效
enforge-first-as	○ 有效 ● 無效
Bestpath AS-Path ignore	○ 有效 ● 無效
Bestpath med missing-as-worst	○ 有效 ● 無效
default lacal-pref	(0-4294967295)

[BGP4 Neighbor 設定]

対向の BGP スピーカの IP アドレス, AS 番号を設定します。

Neighbor Address	10.10.10.6		(ex192.168.1.1)
Remote AS Number	65001 (1-65535)		35)
Keepalive interval	60	60 (0-65535)	
Holdtime	180 (0,3-65535)		5535)
Next Connect Timer	120	(0-655	35)
default-originate	○ 有効 ④ 無効		
nexthop-self	○ 有効 ⊙ 無効		
update-source	(interfaceを指定)		>>を指定)
ebgp-multihop	0-2	255)	
soft-reconfiguration inbound	○ 有効 ④	無効	
Apply map to incoming routes			(routemap名指定)
Apply map to outbound routes			(routemap名指定)
Filter incoming updates			(ACL名指定)
Filter outgoing updates			(ACL名指定)

[BGP4 Network 設定]

BGP で配信したいネットワークを設定します。

Speficy a network to announce via BGP	10.10.100.0/24	(ex192.168.0.0/24)	
backdoor	○ 有効 ⊙ 無効		

【ダイナミックルーティング】-> <BGP4>

BGP4 を再起動します。

BGP4	○ 停止 ⊙ 起動	動作中	再起動
------	-----------	-----	-----

<<各種サービスの設定>>

<VRRP サービス>

[VRRP の設定]

XR_AのBGP Neighbor state が Established 以外の時に Master になるように VRRP 優先度を設定します。

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	PFFLA	インターバル	Auth_Type	password
Ether 0 💌	使用しない 💌	51	150	10.10.100.10	1	指定しない 💌	

【VRRP サービス】

VRRP サービスを起動します。

※動作中の場合は、一度「停止」→「起動」を行ってください。

VRRPH-EZ	○停止	⊙起動	

<<スタティックルート設定>>

宛先 IP アドレスが「10.10.100.128/25」の時は、配下のルータへパケットを転送するように設定します。

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>
10.10.100.128	255.255.255.128	10.10.100.3	1

13. URL フィルタ設定

13-1. URL フィルタの利用

URL フィルタ機能では、ユーザから外部への HTTP アクセスを制御することで、管理者がユーザにアクセ スさせたくないサイトの HTTP を遮断し、ユーザにアクセスできなくさせることが可能です。 XR シリーズの URL フィルタ機能は、XR と NetSTAR 社の外部データベースが連携してユーザの HTTP アク セスを制御します。

13-1-1. 構成図



13-1-2. 設定例

XR で URL フィルタを行い、ユーザにアクセスさせたくないサイトの HTTP アクセスを遮断します。

<<インタフェース設定>>

[Ethernet0の設定]

IPアドレスに「192.168.10.1」を設定します。

⊙固定アト	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		
	ーバから取得		
ホスト名			
MACTELS	2		
 			
🔲 ステートフルパケットインスペクション(spi)			
SPI で DROP したパケットのLOGを取得			
proxy :	arp		
Directo	ed Broadcast		

[Ethernet1の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※PPPoE で接続する場合には "ppp" という論理インタフェースを自動的に生成し、この論理インタフェ ースを使って PPPoE 接続を行います。

③固定アト	レスで使用
IPアドレス	0
ネットマスク	255.255.255.0
MTU	1500
OHOPH	ーバから取得
ホ가名	
мартир	2
IPマス (この)	カレード(ip masq) ドートで使用するIPアドレスに変換して通信を行います)
77-	トフルパケットインスペウション(spi)
□ s	PI で DROP したパケットのLOGを取得
proxy	anp
Directo	ed Broadcast

<<PPP/PPPoE 設定>>

[接続先設定1]

PPPoE 接続(主回線)で使用するユーザ ID とパスワードを設定します。

ユーザロ	test1@centurysys
パスワード	test1pass

[接続設定]

PPPoE(主回線)に関する設定をします。

本設定例では、ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」 にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有 効」に設定します。

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 Ether O Ether O Ether O BRI(54K) O BRI MP(128K) O Leased Line(54K) O Leased Line(128K) O 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	 ● 通常 ○ On-Demand接続
IPマスカレード	○無効 ◎ 有効
ステートフルパケット インスペクション	○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。

FPPcE特殊オプション (全回線共通)	
	→非接款SessionのLCP-EchoRequest受信時门之ADIを強制進出

接続が完了した場合、回線状態が以下のように表示されます。

国際状態 主国際で教校しています

【DNS キャッシュ】

URL フィルタのライセンスサーバに対しての名前解決を可能にするため、DNS キャッシュ機能を起動します。

DNS±+v=/2」 ○停止 ●起動

<<URL フィルタ設定>>

[基本設定]

URL フィルタ設定機能の使用と、フィルタリングをおこなうインタフェースを設定します。 本設定では URL フィルタを行うインタフェースとして Ethernet0 を設定しています。

URLフィルタ	○使用しない ⊙使用する
HTTF監視ポート	80
LANインターフェース	Ethernet0 Ethernet1 Ethernet2

[プレフィルタ設定]

NetSTAR 社の外部データベースとの連携を必要とせず、XR 単体で行うフィルタリングルールを設定します。

[ホワイトリスト/ブラックリスト設定]

外部データベースへの問い合わせとは別に、ユーザが URL を透過/遮断させるリストを、本装置内部に登録することができます。

本設定例では文字列として「centurysys」を登録し、この文字列を含む URL へのアクセスは禁止しています。

ホワイトリス	- /ブラックリスト設定	
No.	URLアドレス	動作
1	centurysys	破桒 🖌

[URL フィルタポリシー設定]

直接 IP アドレスを指定した URL へのアクセスを行う場合に、アクセスを「許可」(透過) するか、「遮断」 (遮断) するかを選択します。

本設定例では直接 IP アドレスを指定した URL へのアクセスを許可しています。

URLフィルタポリシー設定		
IPアドレスを直接指定した URLへのアクセス	◎許可 ○ 遮断	

[ルールセット設定]

ユーザグループに設定されたユーザからの HTTP アクセスに対して、HTTP リクエストのフィルタリング をおこないます。

本設定例ではフィルタリングを適用する IP アドレスとして「any」を設定しています。

ユーザグループ名	all
アドレス	any

URL カテゴリとして「企業」を選択しています。

URL カテゴリの設定では、チェックを入れたカテゴリの URL が「遮断」されます。

	URLカテゴリ	企業 💌	
 ✓ 違法と思われる行為 ✓ 違法と思われる笑物 ✓ 不適切な笑物利用 ✓ 軍事・テロ・過激派 ✓ 武器・兵器 ✓ 訓謗・中傷 ✓ 自殺・家出 ✓ 主張 - 般 	 UFLカテゴリ ✓ 金融商品・サービス ダ ギャンブルー般 ダ 宝くじ・スポーツくじ ダ 対戦型ゲーム ダ ゲームー般 ダ オークション ✓ 通信販売一般 ダ 不動産販売・賃貸 	 企業 ♥ サイドビジネス ♥ グロテスク ♥ イベント ♥ 話題 ♥ 娯楽誌 ♥ 喫煙 ♥ 飲酒 ♥ アルコール製品 	 ✓ 音楽 ✓ 占い ✓ タレント・芸能人 ● 食事・グルメ ✓ 娯楽ー般 ✓ 伝統的な宗教 ✓ 宗教一般 ✓ 政治活動・政党
 ✓ 性行為 ✓ スード画像 ✓ 性風俗 ✓ アダルト検索・リンク集 ✓ アダルト検索・リンク集 ✓ アダルト検索・リンク集 ✓ ハッキング ✓ 不正コード配布 ✓ 公開プロキシ ✓ 出会い・異性紹介 ✓ 結婚紹介 	 ✓ IT関連ショッピング ✓ ウェブチャット ✓ メッセンジャー ✓ ウェブメール ✓ メールマガジン・ML ■ 掲示板 □ IT掲示板 ✓ ダウンロード ✓ ブログラムダウンロート 	 ✓ 水者・下者・フェチ画像 ✓ 文章による性的表現 ✓ コスプレ ✓ オカルト ✓ 同性愛 ✓ プロスポーツ ✓ スポーツー般 ✓ レジャー ✓ 観光情報・旅行商品 	 ✓ 広告・パナー ✓ 感費 □ ニュー スー般
 ✓ 金融レート・投資アドバイス ✓ 投資商品の購入 ✓ 保険商品の申込 	 ✓ ストレージサービス ✓ 転職・就職 ✓ キャリアアップ 	 ✓ 公的機関による観光情報 □ 公共交通 □ 宿泊施設 	

[ログ設定]

URL フィルタの遮断ログおよびシステムログを取得するように設定しています。 ※ログを取得する場合は、SYSLOG サービスは必ず「起動」してください。

アクセスログ	○使用しない ◎ 遮断ログ ○ 遮断ログと透過ログ
システムログ	○使用しない [●] 使用する

13-1-3. 設定例補足1 (ルールセット設定における IP アドレス範囲指定)

URL フィルタ機能では IP アドレス毎に適用する URL カテゴリを変えることも可能です。下記例では以下の条件でルールセット設定を行います。

・「192.168.10.2」の端末ではURLカテゴリを「ルールを選択しない」とする。

・「192.168.10.0/25」の範囲の端末ではURLカテゴリを「大学」とする。

・「192.168.10.128/26」の範囲の端末ではURLカテゴリを「企業」とする。

・「any」で URL カテゴリを「全選択」とする。

※マッチングは、画面に表示されている順におこなわれますので、設定順序にはご注意下さい。

[ルールセット設定]

ユーザグループに設定されたユーザからの HTTP アクセスに対して、HTTP リクエストのフィルタリング をおこないます。

一番目のルールとして IP アドレス「192.168.10.2」を設定しています。

ユーザグループ名	192.168.10.2
アドレス	192.168.10.2

URL カテゴリとして「ルールを選択しない」を選択しています。

URL カテゴリの設定では、チェックを入れたカテゴリの URL が「遮断」されます。

	URLカテゴリ	ルールを選択しない 🚩	
□ 違法と思われる行為	金融商品 サービス	サイドビジネス	□ 音楽
□ 違法と思われる薬物	□ ギャンブルー般	□ <i>₫</i> ₽ ,,,, ,	
一不適切な業物利用	🗌 宝くじ・スポーツくじ	- 1~~~	□ タレント・芸能人
軍事・テロ・過激派	□対戦型ゲーム	□話題	🗌 食事・グルメ
□ 武器·兵器	「ゲームー般	🗌 娯楽語を	□ 娯楽-般
□ <mark>誹謗</mark> ・中傷	□ オークション	回喫煙	□ 伝統的な宗教
自殺・家出	□通信販売-般	1 飲酒	🗌 宗教一般
□主張一般	□ 不動產販売•賃貸	□アルコール製品	D 政治活動·政党
1 性行為	IT関連ショッピング	□水着・下着・フェチ画像	□広告・パナー
- ヌード画像	ロウェブチャット	□ 文章による性的表現	□ 懸賞
世風俗	□ メッセンジャー	□ コスプレ	□ニュースー般
- アダルト検索・リンク集	□ ウェブメール	动ル	
ハッキング	□ xールマガジン·ML	同性愛	
一不正コード配布	□揭示板	フロスポーツ	
□公開プロキシ	□ IT揭示板	🔲 スポーツー般	
□ 出会しい 異性紹介	□ ダウンロード	- L9+-	
1 結婚紹介		ド 🗌 観光情報・旅行商品	
金融レート・投資アドバイス	🗆 ストレージサービス	□ 公的機関による観光情報	
投資商品の購入	□ 転職·就職	🗌 公共交通	
保険商品の申込	= キャリアアップ	🔲 宿泊施設	

二番目のルールとして IP アドレス「192.168.10.0/25」を設定しています。

ユーザグループ名	192.168.10.0/25	
アドレス	192.168.10.0/25	

URL カテゴリとして「大学」を選択しています。

URL カテゴリの設定では、チェックを入れたカテゴリの URL が「遮断」されます。

✓ 違法と思われる行為 金融商品・サービス サイドビジネス 音楽 ✓ 違法と思われる笑物 ダ ギャンブルー般 ダ グロテスク 占い ✓ 不適切な菜物利用 宝くじ・スポーッくじ ダ イベット タレント・芸術 ✓ 軍事・テロ・通激派 ダ 対戦型ゲーム ビ 話題 食事・グルッ ダ 武器・兵器 ダ ゲームー般 娯楽記録 「 オークション」 喫煙 伝統的な宗 ダ 諸器・中傷 ダ オークション 喫煙 「 伝統的な宗 「 合統・家出 ジ 通信販売一般 「 飲酒 ダ 自殺・家出 ダ 通信販売・般 ● 飲酒 アルコール製品 政治活動・改 ダ 生張ー般 ダ 不動産販売・賃貸 アルコール製品 政治活動・説 ダ 性行為 □ ITI関連ジョッピング 水 茶・下 茶・フェチ画像 広告・バナー ダ っド画像 ダ ウェブチャット □ 文章による性的表現 受数賞 ダ 性風俗 ダ ッッセンジャー □ コスブレ ニュー スー領		URLカテゴリ	大学	
✓ ヌード画像 ✓ サニブチャット ✓ 性風俗 ✓ 性風俗 ✓ アグロレト始先をレビックは ✓ アグロレト始先をレビックは ✓ アグロレト始先をレビックは	 ✓ 違法と思われる行為 ✓ 違法と思われる疾物 ✓ 不適切な葉物利用 ✓ 軍事・テロ・過激派 ✓ 武器・兵器 ✓ 訓謗・中傷 ✓ 自殺・家出 ✓ 主張一般 ✓ 性行為 	 URLカテゴリ 金融商品・サービス ダキャンブルー般 宝くじ・スポーツくじ 対戦型ゲーム ゲームー般 ダームー般 オークション 通信販売ー般 不動産販売・賃貸 ITI関連ショッピング 	 大学 サイドビジネス ダ グロテスク ダ イベント ✓ 活題 娯楽誌 喫煙 (炊酒 アルコール製品 水老・下老・フェチ画像 	音楽 占い タレント・芸能人 食事・グルメ 娯楽ー般 伝統的な宗教 宗教ー般 政治活動・政党
□ ノッキング □ ノシン ハ □ 400 M ☑ ハッキング ☑ メールマガジン・ML ☑ 同性愛 ☑ 不正コード配布 ☑ 掲示板 □ プロスボーツ ☑ 公開プロキシ □ rl掲示板 □ スボーツー般 ☑ 出会い・異性紹介 ☑ ダウンロード □ ジャー ☑ 結婚紹介 □ プログラムダウンロード □ 観光情報・旅行商品 □ 金融レート・投資アドバイス ☑ スレージサービス □ 公的機関による観光情報 ☑ 投資商品の購入 □ 転職・就職 □ 公共交通	 マード画像 ピ 性風俗 ピ アダルト検索・リンク集 ピ アダルト検索・リンク集 ピ ハッキング ビ 不正コード配布 ピ 公開プロキシ ピ 出会い 異性紹介 ご 結婚紹介 二 金融レート・投資アドバイク ピ 投資商品の購入 	 ✓ ウェブチャット ✓ メッセンジャー ● ウェブメール ダ メールマガジン・ML ✓ 掲示板 □ IT掲示板 ✓ ダウンロード ○ プログラムダウンロー ✓ ストレージサービス ● 転職・銃職 	 ○ 文章による性的表現 □ コスプレ マオカルト ジ 有カルト ジ 同性愛 □ フロスボーツ □ スポーツー般 □ レジャー ド ● 観光情報・旅行商品 □ 公的機関による観光情報 □ 公共交通 	 ● 振賞 □ ニュー スー般

三番目のルールとして IP アドレス「192.168.10.128/26」を設定しています。

ユーザグループ名	192.168.10.128/26
	192.168.10.128/26
アドレス	

URL カテゴリとして「企業」を選択しています。

URL カテゴリの設定では、チェックを入れたカテゴリの URL が「遮断」されます。

	URLカテゴリ	企業 💌	
 ✓ 違法と思われる行為 ✓ 違法と思われる行為 ✓ 違法と思われる疾物 ✓ 不適切な莱物利用 ✓ 軍事・テロ・通激派 ✓ 武器・兵器 ✓ 武器・兵器 ✓ 試器・兵器 ✓ 試器・兵器 ✓ 試器・兵器 ✓ 試器・兵器 ✓ 計請・中傷 ✓ 自殺・家出 ✓ 主張一般 ✓ 性行為 ✓ タード画像 ✓ 性見合 ✓ アダルト検索・リンク集 ✓ ハッキング ✓ 不正コード配布 ✓ 公開プロキシ ✓ 出会い・異性紹介 ✓ は約2000 	URLカテゴリ	 企業 ✓ サイドビジネス ✓ グロテスク ✓ グロテスク ✓ イベント ✓ 話題 ✓ 娯楽誌 ✓ 喫煙 ✓ 飲酒 ✓ アルコール製品 ✓ 水老・下老・フェチ画像 ✓ 文章による性的表現 ✓ コスプレ ✓ オカルト ✓ 同性愛 ✓ プロスポーツ ✓ スポーツー般 ✓ レジャー ✓ ジャー 	 ✓ 音楽 ✓ 占い ✓ タレント・芸能人 ● 食事・グルメ ✓ 候楽 一般 ✓ 伝統的な宗教 ✓ 宗教 一般 ✓ 政治活動・政党 ✓ 広告・パナー ✓ 感賞 ニュース一般
 ■ 4028+037 ▼ 金融レート・投資アドバイス ▼ 投資商品の購入 ▼ 保険商品の申込 	 ✓ ストレージサービス ✓ 転職・就職 ✓ キャリアアップ 	 ○ 公的機関による観光情報 ○ 公共交通 ○ 宿泊施設 	

最後のルールとして IP アドレスとして「any」を設定しています。

ユーザグループ名	other
דירא	any

URL カテゴリとして「全選択」を選択しています。

URL カテゴリの設定では、チェックを入れたカテゴリの URL が「遮断」されます。

	URLカテゴリ	全選択 💌	
 ✓ 違法と思われる行為 ✓ 違法と思われる笑物 ✓ 不適切な笑物利用 ✓ 軍事・テロ・遅激派 ✓ 武器・兵器 ✓ 誹謗・中傷 ✓ 自殺・家出 ✓ 主張 - 般 ✓ 非につき 	URLカテゴリ	全選択 ✓ サイドビジネス ✓ グロテスク ✓ イベント ✓ 話題 ✓ 娯楽誌 ✓ 喫煙 ✓ 飲酒 ✓ アルコール製品 ✓ レルコール製品	 ✓ 音楽 ✓ 占い ダレント・芸能人 ✓ 食事・グルメ ✓ 娯楽 一般 ✓ 伝統的な宗教 ✓ 家教 一般 ✓ 政治活動・政党
 ■ 主張 - 報 ✓ 性行為 ✓ ヌード画像 ✓ 性風俗 ✓ アダルト検索・リンク集 ✓ ハッキング ✓ オーンドスキ 	 ▲ 不動産販売・賃貸 ✓ IT関連ショッピング ✓ ウェブチャット ✓ メッセンジャー ✓ ウェブメール ✓ メールマガジン・ML ✓ メールマガジン・ML 	 アルコール製品 水素・下素・フェチ画像 文章による性的表現 コスフレ オカルト 同性愛 	 ○ 政治活動・政党 ▽ 広告・バナー ▽ 振賀 ▽ ニュースー般
 □ 小正コーF部布 ☑ 公開プロキシ ☑ 出会い・異性紹介 ☑ 結婚紹介 ☑ 金融レート・投資アドバイス ☑ 投資商品の購入 ☑ 保険商品の申込 	 □ 拍示板 □ IT 掲示板 □ ダウンロード □ ブログラムダウンロード □ ブレージサービス □ 「転職・就職 □ キャリアアップ 	 ビ クロスホーツ ジ スポーツー般 ジ レジャー ジ 観光情報・旅行商品 ✓ 公的機関による観光情報 ✓ 公共交通 ✓ 宿泊施設 	

ルールセット設定設定後は、以下のようになります。

No.	ユーザグループ	URLカテゴリ
1	192.168.10.2 <u>設定</u>	設定
2	192.168.10.0/25 <u>設定</u>	<u>設定</u>
3	192.168.10.128/26 設定	<u>設定</u>
4	other <u>設定</u>	設定

13-1-4. 設定例補足2(ライセンス認証とフィルタによる遮断)

URL フィルタ機能では NetSTAR 社の外部データベースを利用する場合、NetSTAR 社のライセンスサーバに対し、ライセンス認証有効の可否について問い合わせを行います。

なおライセンス認証は、以下のタイミングで行われます。

- ・ユーザが URL フィルタの使用を開始した場合
- ・URL フィルタの使用を開始してから一定時間(48時間)経過した場合
- ・本装置を再起動した場合

ライセンス認証に成功した場合は、以下のような画面が表示されます。



URL フィルタで遮断対象の URL ヘアクセスした場合は、以下の画面をユーザの Web ブラウザに表示する と共に http アクセスを遮断します。

Access Denied

指定したURLへのアクセスは管理者によって禁止されています。

13-1-5. 設定例補足3 (URL フィルタのログ)

URL フィルタ機能では http アクセスを透過・遮断した際のログを取得することも可能です。 以下はログ表示例です。

・プレフィルタ設定

www.centurysys.co.jp への http アクセスを透過した場合 urlfilterd: [prefilter][accept]src ip[192.168.10.100], url[www.centurysys.co.jp/].

www.centurysys.co.jp への http アクセスを遮断した場合 urlfilterd: [prefilter][drop]src ip[192.168.10.100], url[www.centurysys.co.jp/].

・URL カテゴリ設定(外部データベース) www.centurysys.co.jp への http アクセスを透過した場合 urlfilterd: [url category][accept]src ip[192.168.10.100], url[www.centurysys.co.jp/].

www.centurysys.co.jp への http アクセスを遮断した場合 urlfilterd: [url category][drop]src ip[192.168.10.100], url[www.centurysys.co.jp/].

14. サポートデスクへのお問い合わせ

14-1. サポートデスクへのお問い合わせに関して

サポートデスクにお問い合わせ頂く際は、以下の情報をお知らせ頂けると効率よく対応させて頂くこと が可能ですので、ご協力をお願い致します。

- ご利用頂いている XR 製品の機種名, バージョン番号
- ご利用頂いている XR 製品を含んだネットワーク構成
- 不具合の内容および不具合の再現手順(何を行った場合にどのような問題が発生したのかをできる だけ具体的にお知らせ下さい)
- ご利用頂いている XR 製品での不具合発生時のログ
- ご利用頂いている XR 製品の設定ファイル,各種ステータス情報(取得方法に関しましては、ご利 用頂いている製品のユーザーズガイドをご参照下さい)

14-2. サポートデスクのご利用に関して

電話サポート

電話番号: 0422-37-8926

電話での対応は以下の時間帯で行います。

- 月曜日 ~ 金曜日 10:00 AM 5:00 PM
- ただし、国の定める祝祭日、弊社の定める年末年始は除きます。

電子メールサポート

E-mail: <u>support@centurysys.co.jp</u>

FAXサポート

FAX番号:0422-55-3373

電子メール、FAX は 毎日 24 時間受け付けております。

ただし、システムのメンテナンスやビルの電源点検のため停止する場合があります。 その際は弊社ホームページ等にて事前にご連絡いたします。

FutureNet XR シリーズ 設定例集 Ver1.2.0 2008 年 10 月 発行 センチュリー・システムズ株式会社 Copyright(c) 2008 Century Systems Co., Ltd. All Rights Reserved.