

実機演習資料(初級編) ~UNIVERGE IX2215~

第20.1版 (Ver.10.2対応) 日本電気株式会社 NECプラットフォームズ株式会社

Orchestrating a brighter world

未来に向かい、人が生きる、豊かに生きるために欠かせないもの。
それは「安全」「安心」「効率」「公平」という価値が実現された社会です。
NECは、ネットワーク技術とコンピューティング技術をあわせ持つ 類のないインデグレーターとしてリーダーシップを発揮し、
卓越した技術とさまざまな知見やアイデアを融合することで、
世界の国々や地域の人々と協奏しながら、
明るく希望に満ちた暮らしと社会を実現し、未来につなげていきます。

目次

(1) 基本操作(IX2215)
 (2) 演習1 PPPoE回線でのインターネット接続
 (3) 演習2 PPPoE回線でのインターネットVPN
 (4) 演習3 PPPoE回線でのレイヤ2 VPN
 (5) 参考演習 IPv6回線でのネットワーク接続



(1) 基本操作(IX2215)



UNIVERGE IX2215外観図



● PWRランプ	電源ON時に <mark>緑点灯</mark>	● VPNランプ	IPsecSAが1つ以上確立している時に <mark>緑点灯</mark>
● ALMランプ	ハード異常検出時、及び 温度・電圧異常検出時に <mark>赤点灯</mark>	PPPランプ	PPPセッションが1つ以上確立しているときに <mark>緑点灯</mark> 接続中は <mark>緑点滅</mark> します。
● BSYランプ	Flashメモリ書き込み時に <mark>橙点滅</mark>	● BAKランプ	ネットワークモニタ機能により、障害を検出すると <u>緑点灯</u> させることが可能。
●USB1,2,3ランプ	USB0 ポートに取り付けたデータ通信端末等の状態を <u>緑点灯、点滅、消灯</u> の組み合わせで表示。		



UNIVERGE IX2215外観図



コンソール端末の接続





電源の投入(ハードウェア自己診断)

NEC Diagnostic Software Copyright (c) NEC Corporation 2001-2019. All rights reserved.						
%DIAG-INFO: Starting System	POST(Power On Se	lf Test)				
DRAM TEST 1: DRAM TEST 2: NVRAM TEST: CPU TEST: PLD TEST: GE0 TEST: GE1 TEST: GE2(SW-HUB)1-8 TEST: BRI TEST: USB TEST: 1.0 VOLTAGE STATUS: 1.5 VOLTAGE STATUS: 2.5 VOLTAGE STATUS: 3 3 VOLTAGE STATUS:	Pass Pass Pass Pass Pass Pass Pass Pass	<u>デバイスの診断結果</u> <u>Passであれば正常な状態である</u> <u>表しています。</u>	<u>る事を</u>			
5.0 VOLTAGE STATUS: TEMPERATURE STATUS:	4.914V Pass +50.0degC Pass	↓ ≻ <u>設置環境の診断結果</u>	▼次ページへ続く			

◆自己診断表示例

- 異常検出時は「<u>Fail</u>」と表示されます。
 - ・ALARMランプ点灯(赤色)・NVRAM(不揮発性メモリ)に記録: show error-logコマンドで表示。
 - •「DRAM TEST 1」~「VOLTAGE STATUS」はデバイスの診断結果が表示されます。 デバイスの診断で Fail 表示があった場合は、修理または交換が必要になります。 「TEMPERATURE STATUS」で Fail となった場合は、設置環境の温度を見直す必要があります。

ソフトウェアの起動

NEC Bootstrap Software ▼前ページの続き Copyright (c) NEC Corporation 2001-2019. All rights reserved. %BOOT-INFO: Trying flash load, exec-image [ix2215-ms-10.2.16.ldc]. ↑プログラムファイルの起動中 ################## [OK] Starting at 0x20000 Configuring router subsystems (before IDB proc): done. Constructing IDB (Interface Database): done. Configuring router subsystems (after IDB proc): done. Initializing router subsystems: done. Starting router subsystems: done. All router subsystems coming up. <省略> Router# ←ソフトウェアの起動が終了するとプロンプトが表示されます。

┃ プログラムファイルの起動中は「#」を連続表示。

● [Ctrl] + [c]を押下するとブートモニタモードに移行。



コマンド入力について

■コマンド入力

本装置は、CLI (Command Line Interface) でコマンドを受け付けます。



コマンドは、表示されているプロンプトに続けて、1つまたは複数のコマンドをスペースで 区切って入力します。

また、パラメータが必要なコマンドも、コマンドとの間をスペースで区切って入力します。 入力は、1バイト文字(半角)の英数字、記号で行います。

一部のコマンド(ログイン、パスワード等)を除いて、大文字、小文字の区別はありません。

■コマンド入力時のエラーメッセージ

コマンドが間違っていたり、ユーザ権限で認められていないコマンドの場合は、エラーメッセージを 出力します。

Router# show varsion Enter % varsion -- Invalid command. Router#



コンソール操作 便利機能(1)

■コマンド補完機能

「Tab」キーにより、数文字を入力しただけで完全な形のコマンドに補完することができます。 入力した文字列で始まるコマンドが1つだけの場合、Tabキーを押すとそのコマンドの残りの 文字列が補完されます。

Router# en **Tab** → Router# enable-config

★入力した文字列で始まるコマンドが複数ある場合に Tabキーを押すと、コマンドは補完されません。 入力途中の文字列で始まる補完可能なコマンドが表示されます。

Router# e Tab	
enable-config	Enter configuration mode
exit	Exit from the router
Router# e	

★「?」キーでも同様の動作になります。その状態で利用可能なコマンドまたはパラメータの説明が 表示されます。



コンソール操作 便利機能(2)



入力した文字列で始まるコマンドが1つだけの場合、そのまま Enterキーでコマンドを投入 することができます。

Router# en Enter Enter configuration commands, one per line. End with CNTL/Z. Router(config)#

★複数の単語を組み合わせたコマンドの場合も、単語毎の省略入力が可能です。

▼例1 「write memory」 コマンド(設定保存)を省略して入力しています。

Router(config) # wr mem Enter Building configuration... % Warning: do NOT enter CNTL/Z while saving to avoid config corruption. Router(config)#

▼例2 「show running-config」 コマンド(設定確認)を省略して入力しています。

Router(config)# sh run Enter ! NEC Portable Internetwork Core Operating System Software ! IX Series IX2215 (magellan-sec) Software, Version 10.0.14, RELEASE SOFTWARE . .



コンソール操作 便利機能(3)

コマンド補完/省略	 [Tab]キーで補完(複数の補完候補がある場合は、その候補を一覧表示) 他に補完候補のない文字列は省略入力可能 Router(config)# write memory → wr mem Router(config)# show interface → sh int 		
コマンドのヘルプ	• [?]キーでヘルプ表示		
コマンドの履歴	 ・過去に実行したコマンドの履歴を[↑]キー、[↓]キーで表示。 ・履歴保持数:9コマンド 		
ショートカットキー	[Ctrl] + [p]	1つ前に入力したコマンドを表示	
	[Ctrl] + [n]	1つ後に入力したコマンドを表示	
	[Ctrl] + [b]	1文字(カーソルの左)に移動	
	[Ctrl] + [f]	1文字(カーソルの右)に移動	
	[Ctrl] + [a]	行の先頭ヘジャンプ	
	[Ctrl] + [c]	コマンドラインの内容をキャンセル	
	[Ctrl] + [e]	行の終わりヘジャンプ	
	[Ctrl] + [d]	カーソル位置の文字を1文字削除	
	[Ctrl] + [k]	カーソル位置から行末まで削除	
	[Ctrl] + [t]	カーソル位置の文字とその前の文字を入れ替え	
	[Ctrl] + [z]	オペレーションモードに移動	





-画面に収まらない行数を表示する場合、表示の途中で「--More--」が表示されます。

<u>!</u>		
interface GigaEthernet0.0		
no ip address		
shutdown		
!		
interface GigaEthernet1.0		
no ip address		
shutdown		
!		
!		
More ←出力結果が多いときは 「More」で表示が止まります。		

More表示時の操作

- [space]キー : 次の数行を表示します。
- [Enter]キー : 次の1行を表示します。
- [Ctrl] + [c] もしくは [Q]キー
 - :表示を中止し、プロンプトに戻ります。
- [/]キー: 残りの表示から、指定の文字列検索を行います。



モード移行のイメージ



コンフィグモードへの移行

①オペレーションモードからグローバルコンフィグモードへの移行

コマンド「enable-config」 ※省略「en」

Router# enable-config Enter configuration commands, one per line. End with CNTL/Z. Router(config)#

コマンド「configure」 ※省略「con」

どのモードからでもグローバルコンフィグモードに 移行するコマンドです。

Router# configure Enter configuration commands, one per line. End with CNTL/Z. Router(config)#

②グローバルコンフィグモードからオペレーションモードへの移行

コマンド「exit」 ※省略「ex」

Router(config)# exit Router#

もしくは、キーボードの[Ctrl]+[z]キーでもオペレーションモードへ移行

Router(config)# [Ctrl]+[z] <u>※表示しません</u> Router#





バージョンの表示



製造番号の表示

製造番号の表示

Router(config) # show hardware IX Series IX2215 Hardware Platform

S/N: ******** (1)

Processor board: Processor board ID <0> CPU/DDR3/CSB/LBUS clock frequencies are 792/792/396/99 MHz P1010E processor (revision 0x80f90010) 262144K bytes of main memory 1024K bytes of non-volatile configuration memory 32768K bytes of processor flash memory: S29GL256

```
TPsec accelerator:
 on board security engine (SEC4.4), revision 0x100
```

Onboard interface unit GigaEthernet0: GigaEthernet Transceiver is VSC8552 Onboard interface unit GigaEthernet1: GigaEthernet Transceiver is VSC8552 Onboard interface unit GigaEthernet2: GigaEthernet Switch with Transceivers is VSC7424 Onboard interface unit BRIO: BRI Transceiver is YTD439

LED information: PWR: On ALM: Off BSY: Off VPN: Off PPP: Off BAK: Off

① S/N番号 (装置底面の銘版ラベルに表示している「製造番号」と同一)





ホスト名の入力

Router(config) # hostname <u>ROUTER-A</u> ROUTER-A(config) #

ホスト名を入力すると、プロンプトの文字列がホスト名になります。 デフォルト(初期値)は「Router」になっています。







ログイン名の入力

ROUTER-A(config) # username <u>admin-user</u> password plain 1 <u>admin-pwd</u> administrator

% User 'admin-user' has been added.

% Password strength estimation: score 3(strong)

ROUTER-A(config) #

装置のログイン名とパスワードを設定

username [ログイン名] password [パスワードタイプ][ハッシュ方式][パスワード][ログイン権限]

- パスワードタイプ
 - plain: 平文で入力
 - hash:コンフィグ表示時はパスワードをハッシュ化して表示します
- ハッシュ方式
 - 0:強度[普通]
 - 1:強度[強]
- ログイン権限

•

•

- administrator : 全コマンド実行可能
 - operator : 設定情報の変更は実行不可。設定情報の表示、統計情報の表示・クリアは可能
 - monitor : 設定情報の表示・変更は実行不可。統計情報の表示・クリアは可能
- パスワードの強度評価結果 (IX2105を除く)
 - ・ score O(very poor): 非常に弱い
 - score 1(poor):弱い
 - score 2(normal): 普通
 - ・ score 3(strong): 強い
 - ・ score 4(very strong): 非常に強い
- ┃ ログイン タイマの設定

terminal timeout □ <u>←パラメータは「分」で入力します。</u>

- コンソール無操作時間が指定時間継続したときに、ログインセッションを切断
- ◎セキュリティ機能
 - ログインアカウントの外部サーバ(RADIUS)による管理に可能(AAA機能)
 - ログイン/ログアウト時、ログイン失敗時にSNMPトラップの生成が可能





時刻の入力

ROUTER-A(config) # clock 11 5 0 8 nov 2018 ROUTER-A(config) #



ROUTER-A(config) # show clock Wednesday, 8 November 2018 11:05:21 +09 00 ROUTER-A(config) #

IXルータは納入時の時点で時刻情報が設定されています。

◎カレンダー機能

- SNTPクライアント機能に対応しており、NTPサーバ(SNTPサーバ)からのカレンダー情報取得が可能。
- IXルータ自身がSNTPサーバになることも可能。



LANインタフェースの設定(1)



通信速度と通信方向をともに固定設定で使用した場合、GE0、GE1はMDI、GE2(SW-HUB)は MDI-Xとして動作します。 MDI/MDI-Xは、mdi-mdixコマンドにより変更することも可能です。



LANインタフェースの設定(2)



● speed [auto | 1000 | 100 | 10]: オートネゴシエーション(default)、もしくは10M/100/1000M固定に設定

- duplex [auto | full | half]: オートネゴシエーション(default)、もしくは全二重/半二重固定に設定
- exit で上位モードに復帰

★特定のSW-HUBポートに対して設定する例

ROUTER-A(config) # device GigaEthernet2 ROUTER-A(config-GigaEthernet2) # port 1 speed 1000 ROUTER-A(config-GigaEthernet2) # port 8 speed 1000 ROUTER-A(config-GigaEthernet2) # port 1 duplex full ROUTER-A(config-GigaEthernet2) # port 8 duplex full







LANインタフェースの設定(3)

GigaEthernet2.0

LANインタフェースの設定(インタフェースコンフィグモード)



ROUTER-A(config) # interface GigaEthernet2.0 ROUTER-A(config-GigaEthernet2.0) # ip address 192.168. 254/24 ROUTER-A(config-GigaEthernet2.0) # no shutdown ROUTER-A(config-GigaEthernet2.0) # exit

LANインタフェースの設定

- IPアドレスの設定
- no shutdownコマンドでインタフェース有効化
- exit で上位モードに復帰

★IPアドレスの第3オクテット目には、<mark>拠点番号(1~10)</mark>を設定してください。

LANインタフェースの設定が完了した方は、IX2215のGE2とPC をLANケーブルで接続後、PCのIPアドレスを変更してください。

【PCのIPアドレス】 IPアドレス **192.168**. \[\.1] サブネットマスク 255.255.255.0 デフォルトゲートウェイ









Pingによる疎通の確認

Pingによる疎通の確認 (ping 宛先)

PCとIXルータ間の疎通確認を行います。 コマンドプロンプトを起動し、Pingコマンドを実行します。 コマンド : ping 192.168.□.254[Enter] _{□: 拠点番号(1~10)}





応答がない場合は、show running-configコマンドにより、設定情報に誤りがないかを確認してください。





設定の削除(コマンドの削除)

★ホスト名の削除

ROUTER-A(config) # no hostname
Router(config) #

show running-configに表示されているコマンドを削除するときは、そのコマンドの頭に 「no」を付けて再投入します。

★IPアドレスの削除

ROUTER-A(config) # interface GigaEthernet2.0 ROUTER-A(config-GigaEthernet2.0) # no ip address <u>192.168.1.254/24</u> ROUTER-A(config-GigaEthernet2.0) #

特定のモードへ移行しないと削除できないものもあります。

例えば、IPアドレスのように、インタフェースモードで設定したコマンドは、該当のモードへ移行してから noコマンドで削除します。

※アドレスの赤文字部分は省略することも可能です。





コンフィグの保存

ROUTER-A(config) # write memory
Building configuration...
% Warning: do NOT enter CNTL/Z while saving to avoid config corruption.
ROUTER-A(config) #

write memory

- running-config(動作コンフィグ)をstartup-config(保存コンフィグ)にコピー
- コマンド「copy running-config startup-config」と同等

◎参考(その他の保存コマンド)

- startup-configを装置内のファイルシステムに名前を付けて保存
 - copy startup-config <FILE-NAME>
- startup-configをTFTPサーバへ送信
 - copy startup-config <TFTP-SERVER-ADDR>:<FILE-NAME>
- TFTPサーバからstartup-configをコピー
 - copy <TFTP-SERVER-ADDR>:<FILE-NAME> startup-config



設定の初期化

設定の初期化(保存されている設定情報をすべて削除)

ROUTER-A(config) # erase startup-config Are you sure you want to erase the startup-configuration? (Yes or [No]): **yes** ROUTER-A(config) #

erase startup-config

● startup-config(保存されているコンフィグ)の削除

erase startup-configコマンドを実行し、装置を再起動することにより、装置を工場出荷時の設定に戻すことができます。

▼実行イメージ

ROUTER-A(config) # erase startup-config Are you sure you want to erase the startup-configuration? (Yes or [No]): yes ROUTER-A(config) # reload % Warning: current running-configuration is not saved yet. Notice: The router will be RELOADED. This is to ensure that the peripheral devices are properly initialized. Are you sure you want to reload the router? (Yes or [No]): yes





スーパーリセット

ブートモードでのスーパーリセット

設定したパスワードを忘れてしまい装置にログインできなくなった場合などで、装置の設定を 工場出荷時の状態に戻したい場合に、スーパーリセット機能を使用します。



設定情報の表示(1)

running-config、startup-configの表示

Router(config) # show running-config

! NEC Portable Internetwork Core Operating System Software

! IX Series IX2215 (magellan-sec) Software, Version 10.2.16, RELEASE SOFTWARE (1)

! Compiled Sep 18-Wed-2019 17:01:26 JST #2

! <u>Current time Oct 09-Wed-2019 14:22:00 JST</u> (2)

<以降、現在の設定情報を表示>

Router(config) # show startup-config Using 879 out of 1048576 bytes ①

! NEC Portable Internetwork Core Operating System Software

! IX Series IX2215 (magellan-sec) Software, **Version 10.2.16**, RELEASE SOFTWARE **(2)**

! Compiled Sep 18-Wed-2019 17:01:26 JST #2

! <u>Last updated Oct 09-Wed-2019 12:12:16 JST</u> ③

<以降、保存されている設定情報を表示>

表示内容

- show running-config
 - 現在の設定情報と、①バージョン、②このコマンドを実行したときの時刻を表示
- show startup-config
 - 保存されている設定情報と、①コンフィグのサイズ、②バージョン、③最後に設定保存した時刻を表示



設定情報の表示(2)

show running-config コマンドにパラメータを指定することで、特定の部分のみを表示させることも可能です。 (例)

◆ show running-config device ・・・ デバイス情報表示 ◆ show running-config access-list ・・・ アクセスリスト表示 ◆ show running-config interface ・・・ インタフェース情報表示 ◆ show running-config security ・・・ IPsec/IKE 情報表示





コンフィグチェック

```
Router(config) # check configuration
Check access-list configuration
  [IPSec autokey-map]
    "seclist" on "ipsec1" is not registered
  [IPSec dynamic-map]
    No error
  [route-map]
    No error
  [class-map]
    No error
  [IPv4 filter]
    No error
Check ppp-profile configuration
  Profile name is not bound on BRI0.0
  Profile name is not bound on USB-Serial0.0
Check ngn-connect-group configuration
  No error
Check configuration status
  configuration status is not saved yet.
  configuration status will not need restart.
```

┃ 作成したアクセスリストやポリシーが正常に関連付けられているかを確認。

● IPsec、IPv4フィルタ、ルートマップ、QoSクラスマップ、PPPoEプロファイル、NGNのチェック が可能。





テクニカルサポートの表示

<省略>

34

show tech-support [no-pausing]

- 障害発生時の一次解析に必要な統計情報等を一括収集
- no-pausingをつけると、--More--で区切ることなく、ログを収集することが可能
- [Ctrl]+[c]押下で表示を中断

terminal length LINES

- コンソール表示行数の変更(デフォルト 24行)
- 0に設定すると--More--で区切らずに表示

|補足| 障害発生時、開発側に解析を依頼する際には、一次情報として以下3種類のデータ提出をお願いしています。

- 1) show tech-support出力データ
- 2) ネットワーク構成図
- 3) 障害の内容



主な保守・管理コマンド

ping (指定した宛先までの疎通確認)

Router# ping 10.10.10.2

pingコマンドはオペレーションモード以下で実行可能 ※グローバルコンフィグモードでも実行可能 送信元アドレスの指定、送信サイズなどを1行のコマンドで指定可能

ping 192.168.0.254 <u>source 192.168.1.254</u> <u>size 1000</u> <u>count 0</u>
 送信元アドレス 送信サイズ 送信回数

traceroute (指定した宛先までの経路情報確認)

Router# traceroute 10.10.10.2

tracerouteコマンドはオペレーションモード以下で実行可能 ※グローバルコンフィグモードでも実行可能 UDPを使用。

送信元アドレスの指定などを1行のコマンドで指定可能

traceroute 192.168.0.254 <u>source 192.168.1.254</u>
 送信元アドレス

telnetクライアント (telnetクライアント機能の有効化)

Router# telnet 10.10.10.2

telnetコマンドはオペレーションモードで実行可能 ※グローバルコンフィグモードでは実行不可能

リモートコンソール(Telnetサーバ)

telnetサーバの有効化

Router(config) # telnet-server ip enable

telnetサーバ機能はデフォルト無効。

telnetサーバのポート番号を変更することも可能。

• Router(config)# telnet-server ip port 20000

telnetでの接続を許可するIPアドレスをACLで制限可能

• Router(config)# telnet-server ip access-list *admin-user-list*

[注意]

telnetで同時ログイン可能なユーザ数: <u>最大4ユーザ</u>

ローカルコンソール含め、同時にコンフィグモードに存在できるユーザ数:<u>最大1ユーザ</u>

- 2ユーザ目がログインを試みた場合、以下エラーメッセージを表示 Router# enable-config
 <u>% CONFIG process is occupied.</u>
 <u>% You may use `svintr-config' command with administrator privilege.</u>
- 最初のユーザを追い出す場合はsvintr-configコマンドを実行 Router# svintr-config Enter configuration commands, one per line. End with CNTL/Z. Router(config)#

※より安全に遠隔からの操作が可能なSSHサーバ機能にも対応しています。 (詳細はマニュアルをご参照ください)


Webコンソール

HTTPサーバ機能の有効化

※IX2105/IX2106/IX2207は、工場出荷時の初期状態からWebコン ソール(IPアドレス:192.168.1.254)へアクセスすることができます。

Router(config) # http-server ip enable Router(config) # interface GigaEthernet2.0 Router(config-GigaEthernet2.0) # ip address 192.168. 254/24 Router(config-GigaEthernet2.0) # no shutdown Router(config-GigaEthernet2.0) # exit

(もしあらかじめログイン名の設定を行っていた場合)

Router(config)# username <u>admin-user</u> password plain 1 <u>admin-pwd</u> administrator % User 'admin-user' has been added.

Router(config) # http-server username <u>admin-user</u>

HTTPサーバ機能はデフォルト無効。

セキュリティ対策のために、HTTPポート番号(TCP/80)の変更も可能。

Router(config)# http-server ip port 20000 HTTPサーバ機能を有効化して、ブラウザの アドレスバーにIPアドレスを指定して接続します。

[例] http://192.168.0.254/

【注意】 ブラウザにプロキシ設定が残っていると、 IXのWebコンソールにアクセスできません。 プロキシを無効化してください。



表示的

Webコンソール(かんたん設定)

┃ かんたん設定で構築できるネットワーク。

- インターネット接続
- インターネットVPNの構築
- フレッツVPNワイドを使ったVPN構築
- クラウド接続(Ver.9.3以降)
- IP電話サービス接続

■インターネットVPNの場合でも、3ステップで設定が完了します。

STEP2

STEP1

する

 I. パスワードの設定 → 2. インターネット接続の設定 → 3. VPNの設定 → 4. 設定の確認と反映 → 5. 終了 					
かんたん設定:パスワードの設定					
ログイン認証用のパスワード	を設定します。				
	現在の設定	設定の変更			
ユーザ名	admin	変更できません			
		 パスワードを変更しない パスワードを変更する 			
バスワード	パスワード設定なし	•••••			
		確認のためもう一度入力してください。			
		•••••			
		戻る次へ			

①装置の管理者パスワードを設定 ②インターネット接続に必要 なID/パスワードを設定する

1. バスワードの設定 → 5. 終了 かんたん設定:イ	2. インターネット接続の設 ンターネット接続の設	定 → 3. VPNの設定 → 4. 設定の標認と反映 → 設定
ロバイダと接続するWAN像	インタフェースを設定します。	
	現在の設定	設定の変更
接続形態	 PPPoE接続(フレッツ光回線利用の場合) IP接続(ケーブルテレビ回線利用の場合) 	
/AN1: PPPoE接続	の設定(GigaEtherno	et0.1)
	現在の設定	設定の変更
ユーザ名		プロパイダから通知されているユーザ名を設定します。 (フレッツの場合、通常はユーザ名には@を含んでいます)
		test@ix-router.com
バスワード		プロバイダから通知されているパスワードを設定します。 testpass
WAN側IPアドレス		 ● 自動取得 ○ 手動設定
DNSアドレス		 ● 自動取得 ○ 手動設定
		更る)次へ

STEP3

③VPN用のパスワード、 (拠点 の場合)拠点番号を設定する

※Ver.9.4よりIXシリーズの全機種でWebコンソールから

設定を行うことが可能となりました。

1. バスワードの語 5. 終了	淀 →	 インターネット部 	腋の政	定→3.VPI			
かんたん設定	1:1	ンターネット語	続の	設定			
プロバイダと接続する	5WAN∦	リインタフェースを設定	します。				
	現在の設定 設定の変更						
接続形態				 PPPoE接続(フレッツ光回線利用の場合) IP接続(ケーブルテレビ回線利用の場合) 			
WAN1: PPPoE接続の設定(GigaEthernet0.1)							
現在の設定 設定の変更							
プロバイダから通知されているユーザ名を設定します。							
ユーザ名							
バスワード	2 拠点 いずれか	間通信でもセンタは。 Nの拠点で必ずセンタ	が要です。 を選択し	。 ってください。	、近点の方面と		
WAN例IP7H				現在の設定	設定の変更		
DNS7FL		タイプ			 拠点 センタ 		
		拠点番号			他の拠点と同じ番号は設定しないでください。 1 •		
		バスワード			すべての拠点で共通のバスワードを設定してください。 vprpass		
	センタ	WAN側IPアFレス			センタ装置のWANに設定されているIPアドレスを入力してください。 10.1.1.1		

※NetMeisterの設定も適宜必要

ログの収集(1)

UNIVERGE IXシリーズは、4種類のイベント通知方式をサポートしています。

- 1. コンソール端末の画面に表示 (event-terminal)
- 2. 内部バッファに蓄積 (logging buffered)
- 3. SYSLOGサーバ (syslog host、IPv4/IPv6に対応)
- 4. Webブラウザから取得



ログの収集(2)

収集する ログの選択	プロトコル・ 機能単位	 ログを収集するプロトコル・機能と、ロギングレベルの選択 logging subsystem [SUBSYSTEM] [LEVEL] ロギングレベルは下記5段階から選択 少 ← 【ログの量】 → 多 error, warn, notice, info, <u>debug</u> error : エラー状態レベル warn : 警告状態レベル notice : 注意レベル info : 情報レベル <u>debug</u> : デバッグレベル 	【設定例】 logging subsystem ike debug logging subsystem all warn 1)詳細はコマンドのヘルプを参照 2)運用中、debugレベルは使用しないこと いこと info, debugレベルは、障害解析や 現調時に留めること
	パケット ダンプ	 ログを収集するポートを選択 logging packet [DEVICE-NAME] [summary] summary: サマリーモードでの出力 	【設定例】 logging packet GigaEthernet0 summary <u>1)運用中には使用しないこと</u>
タイム スタンプ	時刻	 logging timestamp timeofday (発生時刻) logging timestamp datetime (発生時刻と 年月日) 	内部バッファにログを蓄積する場合は datetimeを推奨
	稼動時間	 logging timestamp uptime (装置稼働時間) 	
ログ表示 選択	リアルタイム 表示	 event-terminal[start/stop] 	event-terminalを入力すると ログ出力開始、再度入力すると停止
	内部バッファ 蓄積表示	show loggingshow logging statistics [SUBSYSTEM]	あらかじめlogging bufferedコマンド を設定する必要があります



マニュアルとソフトウェアの情報

ソフトウェアのバージョンアップを行いたい

◆UNIVERGE IXシリーズ 取扱説明書

https://jpn.nec.com/univerge/ix/Manual/index.html

各機能の概要を知りたい

◆機能説明書(機能概要、仕様、諸元)

https://jpn.nec.com/univerge/ix/Manual/index.html

♦ F A Q

https://jpn.nec.com/univerge/ix/faq/index.html

設定事例を確認したい

◆設定事例集

https://jpn.nec.com/univerge/ix/Manual/index.html

◆ネットワークサービス毎の事例(フレッツグループなど) <u>https://jpn.nec.com/univerge/ix/Support/index.html</u>

最新のソフトウェアを入手したい、ログの意味を知りたい

◆ソフトウェアダウンロード(NEC/NECグループ専用イントラネット) <u>http://ix.necpf.nec.co.jp/Program/index.html</u>

社外のお客様

<u>社外のお客様用のソフトウェアダウンロードページもご用意して おります。※接続申請書へのサインが必要です。</u> 詳しくは、貴社ご担当のNEC営業、もしくは本装置をお買い上げ 頂きました販売店様にお問い合わせ下さい。



(2) 演習1 PPPoE回線での インターネット接続



演習1に登場する主な用語

★ PPPoE(Point to Point Protocol over Ethernet)

イーサネット上でPPPフレームの配送を可能にするプロトコル。 PPPプロトコルがサポートしている、IPアドレスの払い出しや、ユーザ認証などの技術を イーサネット回線で利用できるため、ADSLやFTTHなどのブロードバンド回線を使用した プロバイダ接続で広く使用される。

★ NAPT(Network Address Port Translation)

IPアドレス変換技術の1つ。

グローバルアドレスとプライベートアドレスを1対1で変換する「NAT」と異なり、更に送信元の TCP/UDPポート番号も変換することにより、1対N(複数)での変換を実現する。 社内LAN(プライベートネットワーク)から1つのグローバルアドレスを使ってインターネット アクセスする場合などに使用する。

★ Default Route

デフォルトルート

ルーティングテーブル(経路情報)に存在しない宛て先のパケットを受信した際に転送する経路。 主にインターネットアクセスする際にデフォルトルートを設定する。



目的の構成(インターネット接続)

■ プロバイダとPPPoE接続を行い、インターネット上のサーバに接続します。





LANインタフェースの設定

GigaEthernet2.0

LANインタフェースの設定 (インタフェースコンフィグモード)



LANインタフェースの設定

- IPアドレスの設定
- no shutdownコマンドでインタフェース有効化
- exit で上位モードに復帰

★IPアドレスの第3オクテット目には、<u>拠点番号(1~10)</u>を設定してください。





<u>PPPoEインタフェースの設定</u>

GigaEthernet0.1

PPPoEインタフェースの設定



Router(config)# ppp profile <u>my-profile</u>
Router(config-ppp-my-profile)# authentication myname test
Router(config-ppp-my-profile) # authentication password <u>test[]@test.com</u> <u>test[]-password</u>
Router(config-ppp-my-profile)# exit
Router(config)# interface GigaEthernet0.1
Router(config-GigaEthernet0.1)# ppp binding my-profile
Router(config-GigaEthernet0.1)# ip address 10.10.10. 🗖/32
Router(config-GigaEthernet0.1)# ip napt enable
Router(config-GigaEthernet0.1)# no shutdown
Router(config-GigaEthernet0.1)# exit
Router(config)#

PPPプロファイルの設定

- ppp profile my-profile : ユーザ名/パスワードを設定
- ppp binding my-profile: PPPoEインタフェースに関連付け
- PPPoEインタフェースの設定
 - IPアドレスの設定
 - NAPTの有効化

```
★ユーザ名・パスワード、及び、IPアドレスの第4オクテット目には拠点番号(1~10)を
設定してください。
```



ルーティング設定

デフォルトルートの設定

Router(config)# ip route default GigaEthernet0.1

▲ インターネット接続のためのデフォルトルートを設定

● GigaEthernet0.1:出力先としてWAN回線に接続するPPPoEインタフェースの名前を指定



その他設定と設定保存

UFSキャッシュの有効化/ログ収集の設定/設定の保存

Router(config)# ip ufs-cache enable
Router(config)# logging subsystem all warn
Router(config)# logging timestamp datetime
Router(config)# logging buffered
Router(config)# write memory

■ UFSキャッシュの有効化(キャッシュの検索処理を高速化) ■ ログの情報を装置の内部バッファに蓄積

Pingによる疎通の確認

Pingによる疎通の確認 (ping 宛先)

インターネット上のサーバまでの疎通確認を行います。 コマンドプロンプトを起動し、Pingコマンドを実行します。 コマンド : ping 10.10.100[Enter]



🔤 コマンド ブロン	プト		
C:¥> C:¥>ping 10.10	0.10.100		
10.10.10.100 (10.10.10.100 / 10.10.10.100 / 10.10.10.100 / 10.10.10.100 / 10.10.10.100 /	に ping を送信しています 32 バイトのデータ: からの応答: バイト数 =32 時間 <1ms TTL=62 からの応答: バイト数 =32 時間 <1ms TTL=62 からの応答: バイト数 =32 時間 <1ms TTL=62 からの応答: バイト数 =32 時間 <1ms TTL=62 の ping 統計: か: 送信 = 4 受信 = 4 損失 = 0 (0% の損失)	\int	本例ではPingを4回送信(Sent)して、 応答を4パケット受信(Received)して いる例です。 パケットロスが0であることを確認 します(Lost)。
ラウント トリ 最小 = Ome C:¥>	ップの概算時间(ミリ秒): s、最大 = Oms、平均 = Oms		

応答がない場合は、show running-configコマンドにより、設定情報に誤りがないかを確認してください。



現在の設定の表示

現在の設定の表示 (show running-config)

```
Router (config) # show running-config
                                                              interface GigaEthernet1.0
! NEC Portable Internetwork Core Operating System Software
                                                                no ip address
! IX Series IX2215 (magellan-sec) Software, Version 10.2.16,
                                                                shutdown
RELEASE SOFTWARE
! Compiled Sep 18-Wed-2019 17:01:26 JST #2
                                                              interface GigaEthernet2.0
! Current time Oct 09-Wed-2019 14:22:00 JST
                                                                ip address 192.168.1.254/24
timezone +09 00
                                                                no shutdown
logging buffered 131072
logging subsystem all warn
                                                              interface BRI0.0
logging timestamp datetime
                                                                encapsulation ppp
                                                                no auto-connect
ip ufs-cache enable
                                                                no ip address
ip route default GigaEthernet0.1
                                                                shutdown
ppp profile my-profile
                                                              interface USB-Serial0.0
 authentication myname test 10 test.com
                                                                encapsulation ppp
  authentication password test1@test.com test1-password
                                                                no auto-connect
                                                                no ip address
device GigaEthernet0
                                                                shutdown
device GigaEthernet1
                                                              interface GigaEthernet0.1
device GigaEthernet2
                                                                encapsulation pppoe
                                                                auto-connect
device BRIO
                                                                ppp binding my-profile
 isdn switch-type hsd128k
                                                                ip address 10.10.10.1/32
                                                                ip napt enable
device USB0
                                                                no shutdown
 shutdown
interface GigaEthernet0.0
                                                              interface Loopback0.0
 no ip address
                                                                no ip address
 shutdown
                                                              interface Null0.0
                                                                no ip address
                                                              Router (config) #
```

「show running-config」コマンドにより、現在の設定と、ソフトウェアバージョンの確認が可能です。

保存した設定を確認するときは「show startup-config」コマンドを使用します。



PPPoE接続状態の確認(1)

PPPoE接続状態の確認 (show ip address)

Router(config) # show ip address GigaEthernet0.1 Interface GigaEthernet0.1 is **up**, line protocol is **up** Internet address is 10.10.10.1/32 Broadcast address is 255.255.255.255 Peer address is 10.10.10.254 Address determined by config

「show ip address」コマンドにより、PPPoE接続状態の確認が可能です。

show ip address <I/F NAME>

● <u>up</u>: PPPoEセッション確立

© NEC Corporation 2019

- <u>dormant</u>: PPPoEセッション未確立(ポートup)
 - 網側とPPPoE通信が正常にできていない。
 - PPPのユーザ名/パスワードに誤りがある。
- <u>down</u>: PPPoEセッション未確立(ポートdown)

PPPランプが点滅のまま変わらない場合は、 認証が失敗している可能性があります。 設定したユーザIDとパスワード設定に誤りが ないか見直しをして下さい。

PPPoEが接続すると装置前面の PPPランプが点灯します。





PPPoE接続状態の確認(2)

PPPoE接続の統計確認 (show interfaces)







(参考) PPPoE接続のシーケンス(2)





ルーティングテーブルの表示

ルーティングテーブルの表示 (show ip route)

Router(config) # show ip route IP Routing Table - 4 entries, 2 hidden, 2042 frees Entries: 3 Connected, 1 Static, 0 RIP, 0 OSPF, 0 BGP Codes: C - Connected, S - Static, R - RIP, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, B - BGP * - Candidate default, s - Summary Timers: Age 0.0.0.0.0 [1/1] is directly connected, GigaEthernet0.1, 0:00:08 S* 10.0.0/8 is subnetted, 2 subnets 10.10.10.1/32 [0/0] is directly connected, GigaEthernet0.1, 0:00:08 С С 10.10.10.254/32 [0/0] is directly connected, GigaEthernet0.1, 0:00:08 С 192.168.1.0/24 [0/0] is directly connected, GigaEthernet2.0, 0:01:31

「show ip route」コマンドにより、IPの経路情報テーブルを表示させることが可能です。

目的の宛先に通信ができない場合に、ルータに設定したルーティングテーブル情報に誤りがないかを 確認する場合に利用します。



NAPTテーブルの表示

NAPTテーブルの表示 (show ip napt translation)



インターネットへの接続ができない場合に、動的NAPT変換の状態を確認する場合に利用します。 アドレス変換の情報は一定時間が経過すると消えてしまうため、NAPTテーブルの表示がされない場合は 再度、PCからPingを送信してください。

|補足| WANインタフェースでNAPTを有効にしている場合、インターネット側からIX2215のWANアドレスへ pingを実行しても、NAPTによりBlock(廃棄)されてしまいます。 NAPT使用時でもIXルータがPingに応答させる場合、PPPoEインタフェースに以下の設定を追加します。

ip napt static GigaEthernet0.1 <u>1</u> ← 最後の数字 $\begin{bmatrix} 1 \end{bmatrix}$ は icmp のプロトコル番号





ログの表示 (show logging)

```
Router(config) # show logging
Buffer logging enabled, 131072 bytes, type cyclic
 13 messages (1-13), 1081 bytes logged, 0 messages dropped
Log Buffer (1-13):
2019/10/09 11:25:19
                     GW.038: User anonymous@ has logged on
2019/10/09 11:25:27 ETH.031: Link status up for port 0, 100M b/s, GigaEthernet0
2019/10/09 11:25:27
                     IP.021: Interface GigaEthernet0.1, link up
2019/10/09 11:25:27 ETH.031: Link status up for port 1, 100M b/s, GigaEthernet2
2019/10/09 11:25:27
                     IP.021: Interface GigaEthernet2.0, link up
2019/10/09 11:25:27
                     IP.021: Interface GigaEthernet2.0, line protocol up
2019/10/09 11:25:27
                     IP.021: Interface GigaEthernet2.0, up
2019/10/09 11:25:58 PPOE.029: Session start, AccessCT address 00:26:99:db:b4:58, SessionID 1218,
GigaEthernet0.1
2019/10/09 11:25:58 PPP.004: LCP OPENING: state is open, opening upper-link, on GigaEthernet0.1
2019/10/09 11:25:58 PPP.001: NCP OPENING: IPCP state is open, opening upper-link, on GigaEthernet0.1
                     IP.021: Interface GigaEthernet0.1, line protocol up
2019/10/09 11:25:58
                     IP.021: Interface GigaEthernet0.1, up
2019/10/09 11:25:58
2019/10/09 11:28:19
                      GW.079: System woke up by reload, caused by power-on. System started at Oct 09-
Wed-2019 11:25:12 JST
```

ログ情報を表示します(上記は電源ONしてから、装置起動及びPPPoE接続完了までのログを表示しています)。 ログの削除には「clear logging」コマンドを使用します。

ソフトウェアダウンロードページにある 「イベントログリファレンス」で、詳細なログの意味を確認すること ができます。



(3) 演習2 PPPoE回線でのインターネットVPN



演習2に登場する主な用語(1)

★IPsec(IP Security Protocol)

アイピーヤック

IPパケットの暗号と認証を行い、IPレベルでセキュリティ機能を実現するプロトコル。

\star IKE(Internet Key Exchange)

^{アイケーイー} インターネット上で鍵の情報を生成、更新する自動鍵交換のプロトコル。 IPsecでは接続する対向装置とお互いに共通の鍵を持ちますが、この鍵の情報をインターネット上で 自動的、かつ安全に交換を行わせるためのプロトコル。 IKEには2種類存在し、はじめに策定されたものがIKEv1であり、IKEv1の課題(仕様複雑・曖昧) を見直し、シンプルな仕様に改善されたものがIKEv2となっている。本セミナーではIKEv2を使用。

\star IKE SA(Internet Key Exchange Security Association)

アイケーイー・エスエー

IKEv2メッセージの交換を保護するために使用されるSA

★ CHILD SA(CHILD Security Association)

チャイルド・エスエー

IPsecで接続した際のセキュリティを確保する単一方向のコネクション。 暗号、認証のアルゴリズムやライフタイム、事前共有鍵、SPI値(SAの識別子)などを管理する。

★事前共有鍵(Pre Shared Key)

IPsec接続する装置間で、通信の暗号化と複合化に使用する秘密鍵を生成する素材となる文字列。



演習2に登場する主な用語(2)

★ライフタイム(Lifetime)

SAの有効時間。秘密鍵の情報を定期的に更新するための時間。 定期的に秘密鍵の情報を更新することで、秘密鍵の情報が解読されたときの被害を最小限に 抑えることができる。

★ピアアドレス(Peer Address)

IPsec接続する対向装置(相手側)のアドレス。

★MTU (Maximum Transmission Unit)

インタフェースで1回の転送に送信可能なデータの最大サイズ。 MTUの値より大きなパケットの送信が必要な場合は、パケットの分割処理(フラグメント)が発生し、 ルータのパフォーマンスに影響する。

★ MSS (Maximum Segment Size)

TCPで通信を行なう際に指定するデータの送信単位(セグメント)の最大値。 MTUからTCPヘッダーとIPヘッダーの合計値(40 Bytes)を差し引いた値。



IPsecの特長

IPsec : IP Security Protocol

- ●インターネット上を流れるIPパケットにセキュリティを適用することができる プロトコル。
- <u>データの暗号化とメッセージ認証</u>による盗聴・改ざんの検出
- ●データの送信者が正当な相手であることの認証(相手認証)
- ●パケットのカプセル化による、パケット送受信者の隠蔽

● <u>VPN(トンネリング)</u>の構築が可能



IKEによるIPsecで使用する鍵の生成 (IKEv2)

■ IKEv2のプロトコル動作

- IKE SA INIT交換: IKE SAの折衝と秘密鍵の共有 ※IKE_SAは、IKE_AUTH交換の保護(暗号化)に使用。
- ●IKE AUTH交換 : 相手認証とCHILD SAの折衝。 ※CHILD SAにて、IPsecで暗号化されたデータが通信されます。





ブロードバンド回線を使用したVPN

ブロードバンド回線を使用して、安価で高速なインターネットVPNを構築する ことが可能です。



目的の構成(インターネットVPN)

■ プロバイダとPPPoE接続、及び、拠点~本社間でのインターネットVPNを構築します。



確認ポイント

64

✔ 状態表示ランプのPPPランプ/VPNランプが点灯することを確認します。 ✔ 手元のPCから本社のPC「192.168.0.1」宛にpingが通ることを確認します。 ✔ コマンドによりIKE/CHILD SAが確立していることを確認します。

LANインタフェースの設定

GigaEthernet2.0

LANインタフェースの設定 (インタフェースコンフィグモード)



■ LANインタフェースの設定

- IPアドレスの設定
- no shutdownコマンドでインタフェース有効化
- exit で上位モードに復帰

★IPアドレスの第3オクテット目には、<u>拠点番号(1~10)</u>を設定してください。



PPPoEインタフェースの設定

GigaEthernet0.1

PPPoEインタフェースの設定



Router(config)# ppp profile <u>my-profile</u>
Router(config-ppp-my-profile)# authentication myname <u>test[]@test.com</u>
Router(config-ppp-my-profile)# authentication password <u>test[]@test.com</u> <u>test[]-password</u>
Router(config-ppp-my-profile)# exit
Router(config)# interface GigaEthernet0.1
Router(config-GigaEthernet0.1)# ppp binding my-profile
Router(config-GigaEthernet0.1)# ip address 10.10.10. 🔲 / 32
Router(config-GigaEthernet0.1)# no shutdown
Router(config-GigaEthernet0.1)# exit
Router(config)#

PPPプロファイルの設定

- ppp profile my-profile : ユーザ名/パスワードを設定
- ppp binding my-profile: PPPoEインタフェースに関連付け

PPPoEインタフェースの設定

● IPアドレスの設定

★PPPの認証ID/パスワード、及び、WAN側アドレスの第4オクテット目には拠点番号(1~10)を 設定してください。



ルーティング設定

スタティックルートの設定

Router(config) # ip route default Tunnel0.0

■ トンネル経由で接続先のLANへ到達するためのスタティックルートを設定

- Tunnel0.0:出力先として本社との接続に使用する仮想トンネルインタフェースの名前を指定
- トンネルインタフェースをdefaultルートとして指定することで、各拠点からの通信は全て本社経由で行われる。



IPsec/トンネルインタフェースの設定

トンネルインタフェース(IPsec)の設定

Router(config)# interface Tunnel0.0 Router(config-Tunnel0.0)# tunnel mode ipsec-ikev2 Router(config-Tunnel0.0)# ip unnumbered GigaEthernet2.0 Router(config-Tunnel0.0)# ip tcp adjust-mss auto Router(config-Tunnel0.0)# no shutdown Router(config-Tunnel0.0)# exit Router(config)#

Tunnelインタフェースの設定

- tunnel mode ipsec-ikev2 : トンネルモードの選択
- ip unnumbered : TunnelインタフェースのIPアドレス設定(本例ではunnumbered設定)
- ikev2 peer :接続先の情報を設定

TCP MSS調整(ip tcp adjust-mss auto)

● IPsecトンネルを経由するTCPパケットのサイズをTunnelインタフェースのMTU長以下に調整





IKEv2 認証情報の登録

Router(config)# ikev2 authentication psk id keyid <u>kyoten -id</u> key char <u>kyoten -key</u> Router(config)# ikev2 authentication psk id keyid <u>center-id</u> key char <u>center-key</u>

●自装置と対向装置の認証情報を登録

- ikev2 authentication [認証方式] id [ID種別] ID値 key [鍵入カタイプ] <u>事前共有鍵</u>
 - ▶ 認証方式 psk : Pre-Shared Key方式 eap-md5 : EAP MD5(Message Digest 5)方式
 - ID種別 fqdn、ipv4、ipv6、keyid、rfc822-addr
 - ・鍵入力タイプ char : キャラクター入力

 hex : 16進入力

 secret : 暗号化済みの鍵を入力



自装置の認証設定

自装置の認証設定

Router(config)# ikev2 default-profile Router(config-ikev2-dprof)# local-authentication psk id keyid <u>kyoten[]-id</u> Router(config-ikev2-dprof)# exit Router(config)#

IKEv2デフォルトプロファイルに自装置の認証設定する

- ikev2 default-profile
- Iocal-authentication
- : IKEv2デフォルトプロファイルを作成
 - :IKEv2自装置情報を設定

p69で登録した認証情報のうち自装置の情報を

デフォルトプロファイルに設定する



対向装置の認証設定

対向装置の認証設定と自動接続設定

Router(config) # interface Tunnel0.0 Router(config-Tunnel0.0) # ikev2 peer 10.10.10.100 authentication psk id keyid <u>center-id</u> Router(config-Tunnel0.0) # ikev2 connect-type auto Router(config-Tunnel0.0) # ikev2 outgoing-interface GigaEthernet0.1 Router(config-Tunnel0.0) # exit Router(config) #

トンネルインターフェースに対向装置の認証設定する ikev2 peer [PEER-ADRESS] authentication [認証タイプ] id [ID種別] 事前共有鍵 > 認証タイプ : Pre-Shared Key方式 psk : EAP MD5(Message Digest 5)方式 eap-md5 : RSA暗号方式(デジタル署名) rsa ➢ ID種別 fqdn、ipv4、ipv6、keyid、rfc822-addr 自動接続設定 ikev2 connect-type auto : IPsecオートコネクトの設定。 通信の有無に関わらず10秒間隔でトンネルを周期的に監視し、 SA が存在しない場合にIKEv2 を動作させてSA を自動的に 牛成します。 IKEv2パケットの出力インタフェース設定 ikev2 outgoing-interface [INTERFACE] : IKEv2パケットの出力インタフェースを固定。 これにより意図しないインタフェースからのIPsec/IKE パケット送信 を抑制できます。





フィルタの設定

Router(config)# ip access-list <u>f-list</u> permit ip src 10.10.10.100/32 dest 10.10.10. \square /32 Router(config)# interface GigaEthernet0.1 Router(config-GigaEthernet0.1)# ip filter <u>f-list</u> 1 in Router(config-GigaEthernet0.1)# exit

IP-VPN側から受信するパケットを、送信元がトンネルの接続先のパケットに限定 受信パケットの条件をアクセスリスト(ACL)で指定

● 送信元 10.10.10.100、宛先 10.10.10.

ACLにマッチしなかったパケットは廃棄(暗黙のdeny)

ip filterコマンドでインタフェースにin方向で適用

★アクセスリストで設定する宛先アドレスの第4オクテット目には拠点番号(1~10)を 設定してください。


その他の設定と設定保存

UFSキャッシュの有効化/ログ収集の設定/設定の保存

Router(config) # ip ufs-cache enable Router(config) # logging subsystem all warn Router(config) # logging timestamp datetime Router(config) # logging buffered Router(config) # write memory

UFSキャッシュの有効化(キャッシュの検索処理を高速化) ■ ログの情報を装置の内部バッファに蓄積



Pingによる 疎通の 確認

Pingによる疎通の確認 (ping 宛先)

IPsecを確立した本社ルータ配下のPCまでの疎通確認を行います。 コマンドプロンプトを起動し、Pingコマンドを実行します。 コマンド : ping 192.168.0.1 [Enter]



応答がない場合は、show running-configコマンドにより、設定情報に誤りがないかを確認してください。



PPPoE接続状態の確認

PPPoE接続状態の確認 (show ip address)

```
Router(config)# show ip address GigaEthernet0.1
Interface GigaEthernet0.1 is up, line protocol is up
Internet address is 10.10.10.1/32
Broadcast address is 255.255.255.255
Peer address is 10.10.10.254
Address determined by config
```

「show ip address」コマンドにより、PPPoE接続状態の確認が可能です。

show ip address <I/F NAME>

- <u>up</u>: PPPoEセッション確立
- <u>dormant</u>: PPPoEセッション未確立(ポートup)
 - 網側とPPPoE通信が正常にできていない。
 - PPPのユーザ名/パスワードに誤りがある。
- <u>down</u>: PPPoEセッション未確立(ポートdown)

PPPランプが点滅のまま変わらない場合は、 認証が失敗している可能性があります。 設定したユーザIDとパスワード設定に誤りが ないか見直しをして下さい。

PPPoEが接続すると装置前面の PPPランプが点灯します。





IKE_SAの表示





CHILD_SAの表示





CHILD SAの表示

```
Statistics

Outbound

0 packets, 0 octets

0 cipher failure, 0 out of memory, 0 ts unacceptable

0 misc error

Inbound

0 packets, 0 octets

0 invalid sa, 0 replay detected, 0 integrity failure

0 cipher failure, 0 packet truncated, 0 invalid padding,

0 unknown protocol, 0 out of memory, 0 ts unacceptable

0 misc error

History

Time Event

2015/09/16 16:38:29 Create
```

● Statistics --- 統計情報

● History --- 過去のSA生成/削除履歴

消灯:未接続



CHILD SAが確立すると装置前面の VPNランプが点灯します。 点灯:接続 VPNランプが点灯しない場合、前のページで設定した内容に誤りがないか見直して下さい。



IKE_SAの簡易表示

Router(config)# show ikev2 sa brief					
IKEv2 SA - 1 created					
Interface	SPI(I)	SPI(R)	Lifetime[sec]		
Tunnel0.0	0x8bc86ad4934c9204	0xf96de8b9d68cfc08	84765		

●確立中のIKE_SAの情報(cookie、ライフタイムなど)を1行で表示。

CHILD_SAの簡易表示

Router(config)# show ikev2 child-sa brief					
Child SA - 1 connected					
Interface	Prot	SPI(IN)	SPI(OUT)	Lifetime[sec]	
Tunnel0.0	ESP	0xbb69128b	0xed5d7a9b	28533	

●確立中のCHILD_SAの情報(cookie、ライフタイムなど)を1行で表示。

briefオプションを付加することにより、簡易表示モードに切り替わります。 センタ側装置で、各接続先とのSA確立状態を一覧表示したいときに便利





ルーティングテーブルの表示

ルーティングテーブルの表示 (show ip route)

Router(config) # show ip route IP Routing Table - 5 entries, 2 hidden, 2041 frees Entries: 3 Connected, 2 Static, 0 RIP, 0 OSPF, 0 BGP Codes: C - Connected, S - Static, R - RIP, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, B - BGP * - Candidate default, s - Summary Timers: Age 0.0.0.0/0 [1/1] is directly connected, Tunnel0.0, 0:05:52 S* 10.0.0/8 is subnetted, 3 subnets С 10.10.10.1/32 [0/0] is directly connected, GigaEthernet0.1, 0:13:29 10.10.10.100/32 [1/1] is directly connected, GigaEthernet0.1, 0:12:45 S 10.10.10.254/32 [0/0] is directly connected, GigaEthernet0.1, 0:13:30 С С 192.168.1.0/24 [0/0] is directly connected, GigaEthernet2.0, 0:15:02

「show ip route」コマンドにより、IPの経路情報テーブルを表示させることが可能です。

目的の宛先に通信ができない場合に、ルータに設定したルーティングテーブル情報に誤りがないかを 確認する場合に利用します。



ログの表示 (show logging)

```
Router(config) # show logging
Buffer logging enabled, 131072 bytes, type cyclic
18 messages (1-18), 1389 bytes logged, 0 messages dropped
Log Buffer (1-13):
2019/10/09 14:19:19 GW.038: User anonymous@ has logged on
2019/10/09 14:19:27 ETH.031: Link status up for port 0, 100M b/s, GigaEthernet0
2019/10/09 14:19:27 IP.021: Interface GigaEthernet0.1, link up
2019/10/09 14:19:27 ETH.031: Link status up for port 1, 100M b/s, GigaEthernet2
2019/10/09 14:19:27 IP.021: Interface GigaEthernet2.0, link up
2019/10/09 14:19:27 IP.021: Interface GigaEthernet2.0, line protocol up
2019/10/09 14:19:27 IP.021: Interface GigaEthernet2.0, up
2019/10/09 14:19:27 IP.021: Interface GigaEthernet2.0, up
2019/10/09 14:19:58 PPOE.029: Session start, AccessCT address 00:26:99:db:b4:58, SessionID 1218,
GigaEthernet0.1
```

ログ情報を表示します(上記では電源ON時のログ)。

ログの削除には「clear logging」コマンドを使用します。

ソフトウェアダウンロードページにある 「イベントログリファレンス」で、詳細なログの意味を確認すること ができます。

IKE/CHILD SAが正常に確立しない場合、その理由を確認することができます。

フィルタでパケットが廃棄されている場合、フィルタ(FLT)のログにBLOCKと出力されます。



(4) 演習3 PPPoE回線でのレイヤ2 VPN



演習3に登場する主な用語

★ EtherIP(Ethernet over IP)

イーサアイピー、 イーサネットフレームをIPでカプセル化(トンネリング)することにより、非IPのトラフィックを IPネットワーク上で転送できるようにするプロトコル。

物理的に離れた拠点間を、IPネットワークを介して同一LANとして接続するL2-VPNの構築にも 使われる。

★L2-VPN(Layer2 Virtual Private Network)

レイヤー2 ブイピーエヌ

イーサネットなどのレイヤ2フレームを配送することのできるVPN(仮想的な閉域網)のこと。 EtherIPやL2TPなどがある。

一方、インターネットVPNの構築で一般的に使われるIPsec(トンネルモード)はレイヤ3プロト コルであるIPのみ扱うことが可能なため、L3-VPNに分類される。

\star IRB(Integrated Routing and Bridging)

アイアールビー

異なるブリッジのグループ間、及びブリッジではないインタフェース間の通信(ルーティング)を 実現する機能。

 \star BVI(Bridging Virtual Interface)

ビーブイアイ インタフェース

ブリッジモードで動作するインタフェースにおいて、IPトラフィックの送受信を行うための インタフェース。

★IPsecトランスポートモード

EtherIPとIPsecを併用する場合、EtherIPのカプセル化処理によりトンネル用IPヘッダが 付与されるため、IPsecはデータ部のみ暗号化するトランスポートモードを使用することができる。 (IPsecトンネルモードを使用すると、トンネル用のIPヘッダが二重に付与されるためオーバ ヘッドが増える。)

EtherIP機能 (Ethernet over IP)

■ 離れた拠点間をインターネットを介してブリッジ接続することが可能です。
 ■ インターネットVPNやIP-VPNサービスに非IP端末を収容できるようになります。
 ■ IPパケットの転送が可能であれば、回線種別を問わず利用可能です。



<u>Ver.8.9以降、Ether over GREにも対応</u>

EtherIPによるL2-VPNネットワーク

EtherIP(EtherフレームをIPヘッダでカプセル化する技術)を使用して、インターネットのような「IPネットワーク」上で、L2-VPNを実現することが可能です。
 また、IPsecとの併用も可能なのでセキュリティを保護できます。



IXルータのEtherIPの特長

高速転送性能	IX3315/最大10Gbps、IX3110/最大2.3Gbps、IX3015/最大200Mbps、 IX2215/最大2.0Gbps、 IX2207/最大2.0Gbps、IX2106/最大2.0Gbps の転送性能を実現。また、IPsec併用時でも高速転送が可能です。
セキュリティ	IPsecとの併用が可能で、インターネット上でも安心してブリッジ網の構築が可能です。また、MACフィルタリングにより、ブリッジしたくないフレームを遮断することも可能です。
ブリッジとの併用	従来のブリッジ機能と併用して利用可能です。 ブリッジに属するLANインタフェースとEtherIPトンネルをグループ分けす ることで、VLANの形成が可能です。
低コスト	トンネルの一方が動的IPの構成でもEtherIPトンネルの確立が可能です。 (IPsec/IKEとの併用が必須)
対地数	IX3315で <mark>最大300対地、</mark> IX3110で <mark>最大200対地、</mark> IX3015で <mark>最大50対地</mark> までの収容が可能です。 IX2215/IX2207/IX2106/IX2105は10対地 ※1ブリッジグループあたり
QoS	EtherIPトンネルでカプセル化したフレームに対しても、カプセル化前のフ レームの情報を基に優先制御することが可能です。



目的の構成(EtherIP with IPsec)

■ プロバイダとPPPoE接続、及び、拠点~本社間でのL2-VPN(EtherIP)を構築します。



確認ポイント

✓ 状態表示ランプのPPPランプ/VPNランプが点灯することを確認します。 ✓ 手元のPCから本社のPC「192.168.0.1」宛にpingが通ることを確認します。 ✓ コマンドによりIKE/IPsec SAとEtherIP(ブリッジ)の状態を確認します。



LAN/BVIインタフェースの設定

LANインタフェース/BVIインタフェースの設定 (インタフェースコンフィグモード)

GigaEthernet2.0



Router(config)# bridge irb enable
Router(config)# interface GigaEthernet2.0
Router(config-GigaEthernet2.0)# bridge-group 1
Router(config-GigaEthernet2.0)# no shutdown
Router(config-GigaEthernet2.0)# exit
Router(config)# interface BVI0
Router(config-BVI0)# bridge-group 1
Router(config-BVI0)# ip address 192.168.0. <mark>ロ</mark> /24 Router(config-BVI0)# no shutdown Router(config-BVI0)# exit Router(config)#

ブリッジ機能の有効化(bridge irb enable)

LANインタフェースの設定

- ブリッジグループの設定(同じグループに属するインタフェースは同一LANとなる)
- no shutdownコマンドでインタフェース有効化
- exit で上位モードに復帰

BVIインタフェースの設定(ブリッジ動作時の保守用インタフェース)

- ブリッジグループの設定
- IPアドレス設定
- no shutdown

★BVIインタフェースに設定するIPアドレスの第4オクテット目には「拠点番号(1~10)+200」を設定してください。

BVIインタフェースのIPアドレス

192.168.0.201/24

192.168.0.202/24

192.168.0.203/24

192.168.0.204/24

192.168.0.205/24

192.168.0.206/24

192.168.0.207/24

192.168.0.208/24

192.168.0.209/24

192.168.0.210/24

- 拠点 1

- 拠点 2

- 拠点 3

- 拠点 4

拠点 5

- 拠点 6

- 拠点 7

- 拠点 8

拠点10

PPPoEインタフェースの設定

GigaEthernet0.1

PPPoEインタフェースの設定



Router(config)# ppp profile <u>my-profile</u>
Router(config-ppp-my-profile)# authentication myname
Router(config-ppp-my-profile)# authentication password <u>test[]@test.com</u> test[]-password
Router(config-ppp-my-profile)# exit
Router(config)# interface GigaEthernet0.1
Router(config-GigaEthernet0.1)# ppp binding <u>my-profile</u>
Router(config-GigaEthernet0.1)# ip address 10.10.10.10.12
Router(config-GigaEthernet0.1)# no shutdown
Router(config-GigaEthernet0.1)# exit
Router(config)#

PPPプロファイルの設定

- ppp profile my-profile : ユーザ名/パスワードを設定
- ppp binding my-profile: PPPoEインタフェースに関連付け
- PPPoEインタフェースの設定
 - IPアドレスの設定

```
★PPPの認証ID/パスワード、及び、WAN側アドレスの第4オクテット目には<mark>拠点番号(1~10)</mark>を
設定してください。
```



トンネルインタフェースの設定

トンネルインタフェース(Etherip with IPsec)の設定

Router(config)# interface Tunnel0.0 Router(config-Tunnel0.0)# tunnel mode ether-ip ipsec-ikev2 Router(config-Tunnel0.0)# bridge-group 1 Router(config-Tunnel0.0)# bridge ip tcp adjust-mss 1300 Router(config-Tunnel0.0)# no shutdown Router(config-Tunnel0.0)# exit Router(config)#

Tunnelインタフェースの設定

- tunnel mode etherip ipsec-ikev2 : トンネルモードの選択
- bridge-group 1 : LANインタフェースと同じブリッジグループに設定

TCP MSS調整(bridge ip tcp adjust-mss 1300)

- IPsecトンネルを経由するTCPパケットのサイズをTunnelインタフェースのMTU長以下に調整
- ip tcp adjust-mssコマンドと異なり、MSS値は手動設定にのみ対応。





IKEv2 認証情報の登録

Router(config)# ikev2 authentication psk id keyid <u>kyoten -id</u> key char <u>kyoten -key</u> Router(config)# ikev2 authentication psk id keyid <u>center-id</u> key char <u>center-key</u>

●自装置と対向装置の認証情報を登録

- ikev2 authentication [認証方式] id [ID種別] ID値 key [鍵入カタイプ] <u>事前共有鍵</u>
 - ▶ 認証方式 psk : Pre-Shared Key方式 eap-md5 : EAP MD5(Message Digest 5)方式
 - ID種別 fqdn、ipv4、ipv6、keyid、rfc822-addr
 - > 鍵入力タイプ char : キャラクター入力
 hex : 16進入力
 secret : 暗号化済みの鍵を入力



自装置の認証設定

自装置の認証設定

Router(config)# ikev2 default-profile Router(config-ikev2-dprof)# local-authentication psk id keyid <u>kyoten[]-id</u> Router(config-ikev2-dprof)# exit Router(config)#

IKEv2デフォルトプロファイルに自装置の認証設定する

- ikev2 default-profile
- Iocal-authentication
- : IKEv2デフォルトプロファイルを作成
 - :IKEv2自装置情報を設定

p91で登録した認証情報のうち自装置の情報を

デフォルトプロファイルに設定する

対向装置の認証設定

対向装置の認証設定と自動接続設定

Router(config)# interface Tunnel0.0
Router(config-Tunnel0.0)# ikev2 peer 10.10.10.100 authentication psk id keyid <u>center-id</u>
Router(config-Tunnel0.0)# ikev2 connect-type auto
Router(config-Tunnel0.0)# ikev2 outgoing-interface GigaEthernet0.1
Router(config-Tunnel0.0)# ikev2 ipsec-mode transport
Router(config-Tunnel0.0)# exit
Router(config)#

トンネルインターフェースに対向装置の認証設定する

- ikev2 peer [PEER-ADRESS] authentication [認証タイプ] id [ID種別] <u>事前共有鍵</u>
 - 認証タイプ psk : Pre-Shared Key方式 eap-md5: EAP MD5(Message Digest 5)方式 rsa : RSA暗号方式(デジタル署名)
 ID種別 fqdn、ipv4、ipv6、keyid、rfc822-addr

自動接続設定

93

- ikev2 connect-type auto
- :IPsecオートコネクトの設定。

通信の有無に関わらず10秒間隔でトンネルを周期的に監視し、SA が存在しない場合にIKEv2 を 動作させてSA を自動的に生成します。

IKEv2パケットの出力インタフェース設定

• ikev2 outgoing-interface [INTERFACE]: IKEv2パケットの出力インタフェースを固定。

これにより意図しないインタフェースからのIPsec/IKE パケット送信を抑制できます。

IPsecの通信モードを設定

• ikev2 ipsec-mode transport

: EtherIP時のIPsecではtransportを設定する必要があります。 (設定しない場合はtunnelがデフォルトで設定されています)



フィルタ設定

フィルタの設定

Router(config)# ip access-list <u>f-list</u> permit ip src 10.10.10.100/32 dest 10.10.10.10. Router(config)# interface GigaEthernet0.1 Router(config-GigaEthernet0.1)# ip filter <u>f-list</u> 1 in Router(config-GigaEthernet0.1)# exit

IP-VPN側から受信するパケットを、送信元がトンネルの接続先のパケットに限定 受信パケットの条件をアクセスリスト(ACL)で指定

● 送信元 10.10.10.100、宛先 10.10.10.

ACLにマッチしなかったパケットは廃棄(暗黙のdeny) ip filterコマンドでインタフェースにin方向で適用

★アクセスリストで設定する宛先アドレスの第4オクテット目には<u>拠点番号(1~10)</u>を 設定してください。



その他の設定と設定保存

UFSキャッシュの有効化/ログ収集の設定/設定の保存

Router(config)# ip ufs-cache enable
Router(config)# logging subsystem all warn
Router(config)# logging timestamp datetime
Router(config)# logging buffered
Router(config)# write memory

■ UFSキャッシュの有効化(キャッシュの検索処理を高速化) ■ ログの情報を装置の内部バッファに蓄積



Pingによる 疎通の 確認

Pingによる疎通の確認 (ping 宛先)

EtherIP with IPsecを確立した本社ルータ配下のPCまでの疎通確認を行います。 コマンドプロンプトを起動し、Pingコマンドを実行します。 コマンド : ping 192.168.0.1 [Enter]



応答がない場合は、show running-configコマンドにより、設定情報に誤りがないかを確認してください。



IKE_SAの表示





CHILD_SAの表示





CHILD SAの表示

```
Statistics

Outbound

0 packets, 0 octets

0 cipher failure, 0 out of memory, 0 ts unacceptable

0 misc error

Inbound

0 packets, 0 octets

0 invalid sa, 0 replay detected, 0 integrity failure

0 cipher failure, 0 packet truncated, 0 invalid padding,

0 unknown protocol, 0 out of memory, 0 ts unacceptable

0 misc error

History

Time Event

2015/09/16 16:38:29 Create
```

● Statistics --- 統計情報

● History --- 過去のSA生成/削除履歴

消灯:未接続



CHILD SAが確立すると装置前面の VPNランプが点灯します。 点灯:接続 VPNランプが点灯しない場合、前のページで設定した内容に誤りがないか見直して下さい。

ブリッジの動作状態の表示

ブリッジ状態の表示

Router(config)# show bridge IRB Group 1 Forwarding Cache - 3 entries, 4093 frees, 338 flybys, 0 overflows								
Codes: P - permanent,	B – BVI							
BG Address	Interfac	ce	Timeout	-	RX coun	t	TX count	
1 00:60:b9:4e:b5:40	d Tunnel0.	0	262	1	1	3	13	
B 1 00:60:b9:4e:fd:9a	a BVIO		-	-		1	0	
1 fc:61:98:0c:29:3	6 GigaEthe	ernet2.0	262	1	35	3	22	
IRB Group 1: Interface BVI0 GigaEthernet2.0 Tunnel0.0	Status <u>forward</u> <u>forward</u> <u>forward</u>	Address 00:60:b9:4e 00:60:b9:4e	e:fd:9a e:fd:9a 	RX	count 11 353 13	ΤX	count 340 24 46	

ブリッジに設定したインタフェースの状態が全て「forward」になっていることを確認 状態が「forward」になっているにも関わらず、通信不可の場合には、パケット送受信の 統計(RX/TX count)を見てトラフィックの状態を確認



(5) 参考演習 IPv6回線での ネットワーク接続



参考演習に登場する用語

\star RA(Router Advertisement) アールエー

IPv6機能を有したルータが、プレフィックスなどの情報を広告する際に出力するメッセージ。 メッセージには、フラグやMTU長、ルータライフタイムなどが含まれる。

★ND(Neighbor Discovery)

ネイバーディスカバリー

同一セグメント上の隣接装置の情報を探索する機能。 IPv4のARP相当の機能などが含まれる。

★ネットワークID

IPv4でのネットワークアドレス相当。 IPv6アドレスの前半64bit(4オクテット)で構成。

★インタフェースID

IPv4でのホストアドレス相当。 IPv6アドレスの後半64bit(4オクテット)で構成。

★VRRPv3(Virtual Router Redundancy Protocol version3)

VRRPのIPv6対応版。 IAN側でIPv6を使用している場合のゲートウェイ冗長化時に使用。



IPv4アドレスの現状

IPv4アドレスの枯渇とIPv6対応

- 2011年2月のIPv4アドレスのセンタ在庫(IANA在庫)枯渇に続き、
 2011年4月には、日本のIPv4アドレスを管理するJPNICの在庫が枯渇しました。
- ▶ IPv4ネットワークのパフォーマンス劣化が叫ばれています。
- ▶ 企業ネットワークのIPv6対応が喫緊の課題となっています



世界中で、IPv6に対応中です

ネットワークをIPv6に対応させていく必要があります



IPv6アドレス

IPv6アドレスの特徴

- ➢ IPv6アドレスは、16進 16bit(4桁)8オクテットの128bitで構成。
 区切り文字は":"(コロン)を使用
- ▶ 先頭4オクテットをネットワークID、後半4オクテットをインタフェースIDで構成。

▼ IPv6アドレスの表記

・ 128bit を 16bit 毎に 8分割後、各フィールドを 16進数表記にして":"(コロン)で区 切る。

2001:0db8:0000:0000:0206:29ff:fe1e:482e

・先行する 0 は省略可能。ただし、各フィールドには少なくとも 1つの数値を含むこと。 2001:0db8:0000:0000:0206:29ff:fe1e:482e

2001:db8:0:0:206:29ff:fe1e:482e

 ・ 16bit の 0 または、16bit の 0 が複数連続するフィールドを1箇所のみ":: "を用いて 省略可能。

2001:db8:0:0:206:29ff:fe1e:482e

2001:db8::206:29ff:fe1e:482e



IXルータを使用したIPv6への移行シナリオ(1)

Step1:WAN回線のIPv6化 既存のIPv4ネットワークアドレスを そのままご使用できます。 【IPv6インターネットを利用したVPN構築】 LAN(IPv4)IPv6インターネット LAN(IPv4) SHOP IPv4 over IPv6 IPsecトンネル LAN(IPv4)SHOP -LAN(IPv4)

今のうちにIPv6に対応しておけば安心。 また、フレッツ光ネクストご利用中であれば<mark>追加コストがかかりません</mark>。



IXルータを使用したIPv6への移行シナリオ(2)

Step2 : LAN内へのIPv6導入



VRRPv3やネットワークモニタ機能を使用して、 IPv4と同等の高信頼ネットワークを提供可能!!



目的の構成(IPv6)

■ WAN、及び、LANをIPv6アドレスを使用して構築します。



確認ポイント ✓ コマンドプロンプトから、PCにアドレスが自動設定されていることを確認します。 ✓ 手元のPCから本社のPC「2001:db8:100::ace」宛にpingが通ることを確認しま す。

108

WANインタフェースの設定



★インタフェースに設定するIPアドレス第8オクテット目には「拠点番号(1~10)+10」を 設定してください。

GigaEthernet0.0


LANインタフェースの設定

LANインタフェース (インタフェースコンフィグモード)		
Router(config)# interface GigaEthernet2.0 Router(config-GigaEthernet2.0)# ipv6 enable Router(config-GigaEthernet2.0)# ipv6 address 2001:db8:□::cafe/64 Router(config-GigaEthernet2.0)# ipv6 nd ra enable	· · · · · · · · · · · · · · · · · · ·	

■ LANインタフェースの設定

- IPv6機能の有効化
- アドレスの設定
- ルータ通知メッセージ送信の設定
- no shutdownコマンドでインタフェース有効化
- exit で ト 位 モ ー ド に 復 帰

★インタフェースに設定するIPアドレスの第3オクテット目には「拠点番号 (1~10)」を 設定してください。

109





GigaEthernet2.0

ルーティング設定

スタティックルートの設定

Router(config) # ipv6 route 2001:db8:100::/64 2001:db8::beef

接続先(2001:db8:100::/64)へ到達するためのスタティックルートを設定

● 出力先としてWAN回線のピアアドレスを指定



IPv6アドレスの確認

端末のIPアドレスの確認

端末のアドレス確認を行います。 コマンドプロンプトを起動し、ipconfigコマンドを実行します。 コマンド: ipconfig [Enter]



Command Prompt	
Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved.	
C:¥Users¥ix1000>ipconfig	1
Windows IP 構成	
イーサネット アダプター ローカル エリア接続: 接続固有の DNS サフィックス : IPv6 アドレス : 2001:db8:1:0:14cd:3dc9:ad27:739d 一時 IPv6 アドレス : 2001:db8:1:0:75ad:603b:8d75:9932 リンクローカル IPv6 アドレス : fe80::14cd:3dc9:ad27:739d%11 IPv4 アドレス : 192.168.1.1 サブネット マスク : 255.255.255.0	
デフォルト ゲートウェイ : fe80::260:b9ff:fe4e:6a7e%11 192.168.1.254	
Tunnel adapter isatap.{7B5754ED-E85C-4C13-A7F6-0BF5268620C2}:	
メディアの状態 : メディアは接続されていません 接続固有の DNS サフィックス :	
C:¥Users¥ix1000>	10000



Pingによる 疎通の 確認

Pingによる疎通の確認 (ping 宛先)

本社側の端末までの疎通確認を行います。 コマンドプロンプトを起動し、Pingコマンドを実行します。 コマンド: ping 2001:db8:100::ace [Enter]



- - X Command Prompt Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved. C:¥Users¥ix1000>ping 2001:db8:100::ace 2001:db8:100::ace に ping を送信しています 32 バイトのデータ: 本例ではPingを4回送信して、 2001:db8:100::ace からの応答: 時間 <1ms 応答を4パケット受信している例です。 2001:db8:100::ace からの応答: 時間 <1ms パケットロスが0であることを確認 2001:db8:100::ace からの応答: 時間 <1ms 2001:db8:100::ace からの応答: 時間 <1ms します。 2001:db8:100::aceの ping 統計: = 4、損失 = 0(0%の損失 バケット数: 送信 = 4 受信 ラウンド トリッブの概算時間 (ミリ秒): 最小 = Oms、最大 = Oms、平均 = Oms C:¥Users¥ix1000> 111

応答がない場合は、show running-configコマンドにより、設定情報に誤りがないかを確認してください。



現在の設定の表示

現在の設定の表示 (show running-config)

```
Router (config) # show running-config
! NEC Portable Internetwork Core Operating System Software
! IX Series IX2215 (magellan-sec) Software, Version 10.2.16, RELEASE SOFTWARE
! Compiled Sep 18-Wed-2019 17:01:26 JST #2
! Current time Oct 09-Wed-2019 14:22:00 JST
timezone +09 00
ipv6 route 2001:db8:100::/64 2001:db8::beef
interface GigaEthernet0.0
  no ip address
  ipv6 enable
                        ↓ 拠点番号+10を入力
 ipv6 address 2001:db8::<u>11</u>/64
  no shutdown
interface GigaEthernet2.0
  no ip address
  ipv6 enable
                       ↓ 拠点番号を入力
  ipv6 address 2001:db8:1::cafe/64
  ipv6 nd ra enable
  no shutdown
```

「show running-config」コマンドにより、現在の設定と、ソフトウェアバージョンの確認が可能です。 保存した設定を確認するときは「show startup-config」コマンドを使用します。

ルーティングテーブルの表示

ルーティングテーブルの表示 (show ipv6 route)

```
Router(config) # show ipv6 route
IPv6 Routing Table - 7 entries, unlimited
Codes: C - Connected, L - Local, S - Static
       R - RIPng, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2,
       s - Summary
Timers: Uptime/Age
С
       2001:db8::/64 global [0/1]
        via ::, GigaEthernet0.0, 0:49:02/0:00:00
       2001:db8::/128 global [0/1]
L
         via ::, GigaEthernet0.0, 0:49:03/0:00:00
       2001:db8::11/128 global [0/1]
L
         via ::, GigaEthernet0.0, 0:49:02/0:00:00
С
       2001:db8:1::/64 global [0/1]
         via ::, GigaEthernet2.0, 1:06:26/0:00:00
       2001:db8:1::/128 global [0/1]
L
         via ::, GigaEthernet2.0, 1:06:27/0:00:00
       2001:db8:1::cafe/128 global [0/1]
L
         via ::, GigaEthernet2.0, 1:06:26/0:00:00
S
       2001:db8:100::/64 global [1/1]
         via 2001:db8::beef, GigaEthernet0.0, 0:49:03/0:00:00
```

「show ipv6 route」コマンドにより、IPv6の経路情報テーブルを表示させることが可能です。 目的の宛先に通信ができない場合に、ルータに設定したルーティングテーブル情報に誤りがないかを 確認する場合に利用します。



IPv6インタフェース確認

IPv6 インタフェース情報の表示(show ipv6 interface)

```
Router(config) # show ipv6 interface GigaEthernet2.0
Interface GigaEthernet2.0 is up, line protocol is up
Global address(es):
    2001:db8:1::cafe prefixlen 64
    2001:db8:1:: prefixlen 64 anycast
Neighbor discovery variable(s):
    Neighbor cache garbage time 0 seconds
  Router advertisement variable(s):
    Sending RA is enabled
    Max transmit interval 600 seconds
    Min transmit interval 198 seconds
   Reachable time 0 seconds
    Life time 1800 seconds
    Retrans timer 0 milliseconds
    Current hop limit 64 hops
    Managed address configuration flag is off
    Other stateful configuration flag is off
    Prefix is auto-prefix11 address 2001:db8:1:: prefixlen 64
```

IPv6インタフェースの状態を確認する際に利用します。 装置に設定したプレフィックスやRAで広告する情報も確認出来ます。

お知らせ/付録





UNIVERGE IXシリーズでは、実機セミナーを開催しております。

少人数制!(最大10名まで) 機能概要からコマンドまで丁寧に説明! 一人一台の実機を使用することができます!





運用中に障害が発生してしまった場合に、IXルータ上で判断可能な障害切り分け方法についてご紹介します。 主にIPsec/QoS/ネットワークモニタ/VRRP機能使用時の切り分けをご説明します。

■ お申し込みはこちらをご確認ください。

社内 営業/SE向け : <u>http://www.cnse.mt.nec.co.jp/index.html#tabs-2</u> 販売店様 : <u>https://www.mmb.nec.co.jp/univergesolution/index.html#tabs-2</u>

お知らせ

Webサイトのご案内

製品情報やコンフィグ設計を支援する各種情報をWebに掲載しています。

IX製品サイト(一般向け)

https://jpn.nec.com/univerge/ix/index.html

∞ VPN対応高速アクセスルー	
→ C]jpn.nec.	com/univerge/ix/index.html 역 ☆ @
NEC \Orchestrati	ng a brighter world 主張い会わせ <u>サポート・ダウンロード</u> NECサイト内候素 Q <u>Japan</u> ⊕ country & Region
ソリューション・サー	ビス 製品 導入事例 企業情報
ホーム > 製品 > 企業・官公庁(UNIVERCE 1X>/11	8/計場合=長 > UNIVERGE IXシリーズ VPN対広高速アクセスルータ UNIVERGE IXシリーズ
創品将要	
製品ラインナップ	お問い合わせ
ハードウェア仕様	→ 特長
ソフトウェア仕様	○ 「UNIVERGE IXシリーズ」は、高速化が進むブロードバンド回線でのVPN構築に適した、企業向け
技術情報/お知らせ	 ──の高速アクセスルーダです。 > 小型ルータとしては業界最高クラスの転送性能・暗号化(IPsec)性能を実現。また、ブロードバン
SDN Ready	► 「回線の他にも、ISDNやデータコネクト (NGN)、ワイヤレス回線(無線WAN)、光ファイバー 持持など、多様な回線サービスに対応、お客様の様々などジネスコープに対して、高いパフォーマン
マニュアル	スと信頼性で応える製品です。
ダウンロード	> <u>さらに詳しく</u>
FAQ	>
保守サービス	> センタ用ルータ (IX3000シリーズ)
価格	>
ゼロコンフィグモデル	
企業・官公庁・通信事業者 のお客さま	・ ハレ語がとなれていませんでの「正形に ビングガルゲータ ・ IPv4基本性能 2.6Gbps. IPsec性能 920Mbps. IPsec最大1,024対地
中堅・中小企業のお客さま	>
個人のお客さま	
80.0 0	・シネルベビ国際ではスローラルでは、ビンラカルレージ ・IPv4基本性能 200Mbps、IPsec性能 200Mbps、IPsec最大512対地
ラウノロート 11 カタログ(PDF)	
設定ツール・設定例	拠点用ルータ (IX2000シリーズ)
 コンフィグ作成ツール フレッツリノクト 	UNIVERGE IX2215
<u>リモートアクセスVPN</u>	 ・ギガビット回線とワイヤレス回線に対応した拠点用オールインワンルータ ・IPv4基本性能 2Gbps、IPsec性能 1.3Gbps、IPsec最大128対地
- 仕	_様一覧
_ 患	品マーュアル
- +	いい、――、 シャート
– F.	AUなど

NECグループ限定

http://ix.necpf.nec.co.jp/

			~ ~
UNIVERG	UNIVERGE IX Serie Site (IX1000/IX2000/IX	es Portal デルデンデン 第175 第1	NTTRE*
921935 通知会社 協力資料 ジントウェアダウノロード 製品でヨッアル 製品でヨッアル 日本 日本		供をお願いします。 上する予定です。詳細はは、nowsをご参照 を了です。リブレースの促進をお願いします 内 の、家以上加入方法 川のご客的 二人新教能説明会を東京、大阪/名言	ください。 ト。 古屋で閉催い
性能情報 問、ら <u>たりせ先一覧</u> <u>ac-QandA過去記事検索</u> 達<u>い</u> 支援サービス 客先同行支援サービス 拠器回出サービス	TOPROS [13] また) TOPROS [13] また) 2014年09月02日 ・ 000-21 最新ワントウェア「Ver90」リリースなり 2014年09月27日 ・ 127日年08月27日	リースしました。詳しくは <u>こちら</u> 会のセミナー演判を掲載しました。 <u>グ</u> ウンロード	14 <u></u>
後し時による 本米-クルケイト内検索 ● サイト内検索 ● 社内検索 検索	 1:セミナー JA 2020、9/3/37/00新報酬記号号会の第 2014年09月27日 1:53/01 ビリ 150N Ready製品」としてDC/リーズが 2014年09月25日 1:セミナー 30/32公司:実現セミナー(70級編)、9/1 1:25/+ 30/32/200編 1:セミナー 30/32/200編 2:12/200編 3:12/200編 4:12/200編 4:12/200編 5:12/200編 5:12/200編 5:12/2004 5	にまた茶袷かめります。詳細ま <u>こちら</u> 紹介されました。詳細まこちら → <u>ブレスリリー</u> 9(金)に実機セミナー(IPsec編)を開催いたします。	<u>ス</u> す。お申し
実 <u>構セミナー 情報</u> 0/19(金) 初級編 9/19(金) IPSec編 ノ フトウェア情報	2日間連情報	<u> 技販ツール</u>	
最新パージョン: ・0.110:27:27:27:27:27:27:27:27:27:27:27:27:27:		SR-SATA (2014-09-07) New Schröft, 低社議業との機能比較/性前 Lichoing (1983)を33 Lichoing (1983)を33 Lichoing (1983)を33 Lichoing (1983)を33 Lichoing (1983)を34 Lichoing (1983)を34 Lichoing (1983)を34 Lichoing (1983)	北較 <u> 動連</u> 書回答例、 ホル登録証など

- 製品マニュアル
- 製品紹介資料、性能情報
- 過去Q&A検索 など



^{お知らせ} Webサイト サンプルコンフィグ作成ツール(1)

■ コンフィグを自動生成するツールを用意しています(IX2000シリーズ)



設定パラメータ

▪ 変更必須

〈ルータ選択〉	
機種名 🕜	DX2215 V
〈ルータ管理者ユーザ登録〉	
管理者ユーザ名 🕜	admin
管理者バスワード* 📀	secret
〈WAN設定〉	
WAN側ボートのIPアドレス 🥝	自動設定
〈LAN設定〉	
LAN側ボートのIPアドレス 🥝	192.168.1.254 /24
〈インターネット接続設定〉	
ブロバイダ(ISP)接続のユーザ名* 🥝	user-A@example.com
ブロバイダ(ISP)接続のバスワード* 🥹	password-1



製品ポータルで公開しています。 基本設定の作成、確認に 是非ご活用ください。

▌拠点1用サンブルコンフィグ

! site1 sample configuration

hostname Router1

username admin password plain secret administrator

ip route 192.168.1.0/24 Tunnell.O ip ufs-cache enable

ip access-list sec-list permit ip src any dest any ike proposal ikeprop encryption aes-256 hash sha ike policy ngnike-1 peer ngn-dynamic key secret mode aggressive ikeprop ike local-id ngnike-1 keyid ngnid-router1 ike ramote-id ngnike-1 keyid ngnid-router2 ike nat-traversal force ipsec autokey-proposal secprop esp-aes-256 esp-sha ipsec dynamic-map ngnsec-1 sec-list secprop ike-binding ngnike-1 ipsec local-id ngnsec-1 192.168.0.0/24 ipsec remote-id ngnsec-1 192.168.1.0/24

コンフィグが作成できます!





Webサイト サンプルコンフィグ作成ツール(2) お知らせ

| コンフィグ作成補助(<u>https://jpn.nec.com/univerge/ix/Support/tool2/index.html</u>) ●本サイトで作成したコンフィグをUSBメモリに保存し、初期設定に適用できます。







LANポートのモード設定

- mdi-mdix [mdi | mdix]: MDI/MDI-X固定設定(speed/duplexともに固定設定時のみ有効)
- exit で上位モードに復帰

★特定のSW-HUBポートに対して設定する例

ROUTER-A(config) # device GigaEthernet2 ROUTER-A(config-GigaEthernet2) # port 1 mdi-mdix mdi ROUTER-A(config-GigaEthernet2) # port 8 mdi-mdix mdi



LANインタフェースの設定(高機能)



VLANグループでグループ分けすることで 複数のセグメントを構成することができます。



物理ポートのシャットダウン(デバイスコンフィグモード)

★ GigaEthernet0をシャットダウンする例

ROUTER-A(config) # device GigaEthernet0
ROUTER-A(config-GigaEthernet0) # shutdown

★ SW-HUBポート(GigaEthernet2)全体をシャットダウンする例

ROUTER-A(config) # device GigaEthernet2 ROUTER-A(config-GigaEthernet2) # shutdown

★特定のSW-HUBポートをシャットダウンする例

ROUTER-A(config) # device GigaEthernet2 ROUTER-A(config-GigaEthernet2) # port 1 shutdown ROUTER-A(config-GigaEthernet2) # port 8 shutdown



123

付録

- ・使用していないポートをシャットダウンすることで、無駄な消費電力を抑えることができます。
 - 使用していないポートの不正な利用を防止することもできます。









NetMeisterはクラウド上で顧客単位・拠点単位でのネットワーク機器管理が可能な 基本無料のサービスです。運用管理者は各ユーザ毎の装置情報を一元管理出来ます。





■NetMeister(クラウド)側での準備

1. ユーザアカウントの作成

● NetMeisterホームページからログイン画面に遷移し「新規ユーザーアカウント作成」からユーザ登録します。 メールアドレスをIDとして登録する形。フリーメールアドレスは利用不可です。

2. ログインし、グループIDを作成

● グループID・グループ名・パスワードを入力し作成します。管理対象にするお客様につき、グループIDを 1つ作成する形で使います。自社のネットワーク管理を行う方は1つだけ作る形です。

3. 拠点IDを作成

「拠点」画面から拠点を「追加」ボタンをクリックして登録します。拠点ID・拠点名・郵便番号・住所・メモなど









NetMeister セミナー

付録



NetMeisterのセミナーを開催する予定です。

少人数制!(最大10名まで) NetMeisterの概要から操作方法まで工寧に説明! ー人一台のPCで受講することができます!



NetMeister セミナー(2h)

NetMeisterのサービスの概要、基本操作を習得していただくためのセミナーになります。 サービスの概要説明の他、①活用シーン、②登録方法、③装置の監視、④装置の統計情報の取得など 操作体験もご用意しています。



NetMeister管理画面







各種公開情報

■社外サイト

https://www.necplatforms.co.jp/product/netmeister

■操作ガイド

https://www.manuals.nec.co.jp/contents/netmeister/manual/



競合他社 比較一覧(小規模拠点用ルータ)

			NEC IX2105	NEC IX2106	A社小規模拠点用ルータ	B社小規模拠点用ルータ	C社小規模拠点用ギガルー タ	D社小規模拠点用ギガルー タ
希望小売価格(税別)		別)	81,000円	81,000円	75,000円	80,000円	9,8000円	82,000円
性能(公	:称値)		最大1.3Gbps	最大2.0Gbps	最大2.0Gbps	-	-	最大1.08Gbps
IPsec性	能(公称值	直)	最大397.2Mbps (AES)	最大1.35Gbps	最大1.0Gbps	-	最大1.0Gbps	最大 248Mbps
FastEt	nernetポ-	ート(10/100)	-	-	-	4 HUB	-	-
Gigabit	Ethernet	ポート	1+4(SW-HUB)	1+4(SW-HUB)	1+4(SW-HUB)	2port	1+4 (SW-HUB)	2port
八 上	消費電力	 ხ	最大7W(14VA)	最大7W(14VA)	最大11W	最大30W	最大16.7W (*5)	最大9.4W
ド 仕	騒音		0dB(ファンレス)	0dB(ファンレス)	0dB(ファンレス)	不明	0dB(ファンレス)	不明
怺	環境への	の配慮	RoHS対応	RoHS対応	RoHS対応	不明	RoHS対応	RoHS対応
	温度条件 湿度条件	牛 牛(非結露)	0~50℃ 90%以下	0~50℃ 90%以下	0∼50℃ 15∼80%	0~40℃ 10~85%	0~40℃ 15~85%	0~40℃ 80%以下
設置性			横置き、縦置き、 19インチラック(*1)、 壁掛け(マグネット	横置き、縦置き、 19インチラック(*1)、 壁掛け(*2)、マグネット (*3)	横置き、19インチラック (*4) 壁掛け(*4)	横置き	横置き 横置き、縦置き 壁掛け	
ブリッシ	ジ機能		0	0	0	-	0	0
VLAN			IEEE802.1QタグVLAN (32/ポート) ポートベースVLAN	IEEE802.1QタグVLAN (32/ポート) ポートベースVLAN	IEEE802.1QタグVLAN (16) ポートベースVLAN	IEEE802.1QタグVLAN (5) ポートベースVLAN	IEEE802.1QタグVLAN ポートベースVLAN	-
データ	コネクト対	讨応	0	0	0	-	-	-
ルーティング (IPv4)		対応方式	RIP/RIPv2、OSPFv2、 BGP4、 ポリシールーティング	RIP/RIPv2、OSPFv2、 BGP4、 ポリシールーティング	RIP/RIPv2、OSPFv2、 BGP4、 ポリシールーティング	RIP/RIPv2、OSPFv2、 BGP4、 EIGRP、ポリシールーティ ング	RIP/RIPv2、OSPFv2、 BGP4、 ポリシールーティング	RIP/RIPv2、OSPFv2、 BGP4 ポリシールーティング
		OSPFネイバ数	128	128	10	不明	50	不明
		BGPピア数	64	64	32	不明	不明	4
		マルチキャスト	スタティック, IGMPv1/v2, IGMPプロキシ, PIM-SM	スタティック, IGMPv1/v2, IGMPプロキシ, PIM-SM	IGMPv2/v3, PIM-SM	IGMPv1/v2/v3, PIM-DM, PIM-SSM	IGMPv2, PIM-DM, PIM-SMv2	-



競合他社 比較一覧(小規模拠点用ルータ)

		NEC IX2105	NEC IX2016	A社小規模拠点用ルータ	B社小規模拠点用ルータ	C社小規模拠点用ギガルー タ	D社小規模拠点用ギガルー タ
冗長機能	冗長機能 機能 VRRPv2		VRRPv2	VRRP	VRRP、HSRP	VRRP	VRRP
	ICMP Echo 監視による 経路制御	Staticルート隠蔽, ポリシールーティング隠蔽, 任意のコマンド実行, VRRP停止	Staticルート隠蔽, ポリシールーティング隠蔽, 任意のコマンド実行, VRRP停止	Staticルート隠蔽, VRRP停止	Staticルート隠蔽, ポリシールーティング隠蔽, VRRP停止	Staticルート隠蔽, VRRP停止	任意のスクリプト実行
QoS		PQ、CBQ、LLQ、 ToS/CoS制御、 シェーピング	PQ、CBQ、LLQ、 ToS/CoS制御、 シェービング	PQ, CBQ, WFQ、 ToS/CoS制御、 シェーピング, 適応型QoS (帯域検出, 負荷通知, DTC)	LLQ, CBWFQ、 ToS/CoS制御、 シェーピング (Class-Based Shaping)	WFQ ToS/CoS制御、 シェーピング	優先制御、 シェーピング
拡張機能	パケット フィルタ (静的)	MACアドレス, IPアドレス, プロトコル, MACアドレス, IPアドレス, プロトコル, M. URLフィルタリング(内部DB 型) URLフィルタリング(内部DB 型) エ		MACアドレス, IPアドレス , プロトコル, ポート番号	MACアドレス, IPアドレス, プロトコル	MACアドレス, IPアドレス, プロトコル	MACアドレス, IPアドレス, プロトコル
	パケット フィルタ (動的)	ステートフル・インスペクシ ョン(TCP/UDP/ICMP), URLフィルタリング(外部DB 型) (*3)	ステートフル・インスペクシ ョン(TCP/UDP/ICMP), URLフィルタリング(外部DB 型) (*3)	ステートフル・インスペク ション, Winnyフィルタ, Shareフ ィルタ, URL(内部DB参照型)	ステートフル・インスペク ション	ステートフル・インスペク ション	ステートフル・インスペク ション URLフィルタ(オプション)
VPN	対応方式 IPIP、GRE、IPSec IPIP、GRE、IPSec		IPIP、IPsec	IPIP、GRE、IPSec	IPIP、IPsec	IPIP	
	暗号 アルゴリズ ム	DES, 3DES AES(128/192/256bit)	DES, 3DES AES(128/192/256bit)	DES, 3DES, AES(128/256bit)	DES, 3DES AES(128/192/256bit)	DES, 3DES AES(128/192/256bit)	3DES, AES(128/192/256bit)
	対地数	128	128	20 10 100		100	
	IKEv2	0	0	0	0	0	0
	認証 <i>ア</i> ルゴリズ ム	MD5, SHA-1, SHA-2(256/384/512bit)	MD5, SHA-1, SHA-2(256/384/512bit)	MD5, SHA-1, SHA-256	MD5, SHA-1, SHA-2(256/384/512bit)	MD5, SHA-1, SHA-2	SHA-1, SHA-2(256/512bit)
不正端末アクセス防止,		IEEE802.1X, MACアドレス認証	IEEE802.1X, MACアドレス認証	DHCP端末認証	DHCP端末認証 IEEE802.1X, M MACアドレス認証 I		IEEE802.1X, MACアドレス認証
保守機能		SNMPv1/v2c(IPv4/IPv6) sFlow(IPv4/IPv6)	SNMPv1/v2c(IPv4/IPv6) sFlow(IPv4/IPv6)	SNMPv1/v2c/v3	SNMPv1/v2c/v3 NetFlow(IPv4)	SNMPv1/v2c/v3	SNMPv1/v2c/v3
ソフトウェア管理	幾能	プログラムファイル2面管理	プログラムファイル2面管理 、	ファームウェア多重	-	構成定義2面管理	-
		ー ・ ・ ・ ションアップ	、 自動バージョンアップ				2018年1月 当社調べ



競合他社 比較一覧(オールインワンルータ)

			NEC IX2207	NEC IX2215	A社小規模拠点用ルータ	B社小規模拠点用ルータ	C社小規模拠点用ギガルー タ	D社小規模拠点用ギガルー タ
希望小亨	売価格(税)	別)	98,000円	118,000円	125,000円	216,000円	1298000円	174,7000円
性能(公	称值)		最大2.0Gbps	最大2.0Gbps	最大2.0Gbps	-	最大2.0Gbps	最大1959Mbps
IPsec性	能(公称值	直)	最大1.08Gbps	最大1.32Gbps	最大1.5Gbps	-	最大650Mbps	最大 525Mbps
FastEtł	nernetポ-	ート(10/100)	-	-	-	-	-	-
Gigabit	Ethernet	ポート	2+4(SW-HUB)	2+8(SW-HUB)	2+8(SW-HUB)	1+8HUB+1SFP	2+8 (SW-HUB)	2+8(SW+HUB)
八 1	消費電法	ს	最大24W(35VA)	最大18W(28VA)	最大14.5W	最大60W	最大26.6W (*5)	最大19W
-ド 住	騒音		0dB(ファンレス)	0dB(ファンレス)	0dB(ファンレス)	不明	4.5dB以下	不明(ファンあり)
俅	環境への	の配慮	RoHS対応	RoHS対応	RoHS対応	不明	RoHS対応	RoHS対応
	温度条(湿度条(牛 牛(非結露)	0~45℃ 90%以下	0~50℃ 90%以下	0∼45℃ 15∼80%	0~40℃ 10~85%	0∼40℃ 15~85%	0~40℃ 80%以下
設置性			横置き、 縦置き、 19インチラック ジョイントキット	横置き、 縦置き、 19インチラック ジョイントキット	横置き、19インチラック (*4) 壁掛け(*4)	横置き 19インチラック	横置き 19インチラック	横置き, 壁設置ブラケット(*4), 19インチラック(*4)
ブリッシ	ジ機能		0	0	0	0	0	0
VLAN			IEEE802.1QタグVLAN (32/ポート) ポートベースVLAN	IEEE802.1QタグVLAN (32/ポート) ポートベースVLAN	IEEE802.1QタグVLAN (32ID/LAN) ポートベースVLAN	IEEE802.1QタグVLAN (16) ポートベースVLAN	IEEE802.1QタグVLAN (100/装置) ポートベースVLAN	IEEE802.1QタグVLAN (4094) ポートベースVLAN
データ	コネクト対	村応	⊖ (データコネクトVPN)	○ (データコネクトVPN)	0	-	-	-
ルーテ- (IPv4)	ィング	対応方式	RIP/RIPv2、OSPFv2、 BGP4、 ポリシールーティング	RIP/RIPv2、OSPFv2、 BGP4、 ポリシールーティング	RIP/RIPv2、OSPFv2、 BGP4、 ポリシールーティング	RIP/RIPv2、OSPFv2、 BGP4、 EIGRP、ポリシールーティ ング	RIP/RIPv2、OSPFv2、 BGP4、 ポリシールーティング	RIP/RIPv2、OSPFv2、 BGP4 ポリシールーティング
		OSPFネイバ数	128	128	10	不明	100	不明
		BGPピア数	64	64	32	不明	4	不明
		マルチキャス ト	スタティック, IGMPv1/v2, IGMPプロキシ, PIM-SM	スタティック, IGMPv1/v2, IGMPプロキシ, PIM-SM	IGMPv2/v3, PIM-SM	IGMPv1/v2/v3, IGMPスヌーピング, PIM-DM, PIM-SM, PIM- SSM	IGMPv2, PIM-DM, PIM-SMv2	IGMPv3, PIM-SM



競合他社 比較一覧(オールインワンルータ)

		NEC IX2207	NEC IX2215	A社小規模拠点用ルータ	B社小規模拠点用ルータ	C社小規模拠点用ギガルー タ	D社小規模拠点用ギガルー タ
冗長機能	機能	VRRPv2	VRRPv2	VRRP	VRRP、HSRP	VRRP	VRRP
	ICMP Echo 監視による 経路制御	Staticルート隠蔽, ポリシールーティング隠蔽, 任意のコマンド実行, VRRP停止	Staticルート隠蔽, ポリシールーティング隠蔽, 任意のコマンド実行, VRRP停止	Staticルート隠蔽, VRRP停止	Staticルート隠蔽, ポリシールーティング隠蔽, VRRP停止	Staticルート隠蔽, VRRP停止	任意のスクリプト実行
QoS		PQ、CBQ、LLQ、 ToS/CoS制御、 シェービング	PQ、CBQ、LLQ、 ToS/CoS制御、 シェービング	PQ、CBQ、LLQ、 ToS/CoS制御、 シェーピングPQ, CBQ, WFQ、 ToS/CoS制御、 シェーピング, 適応型QoS (帯域検出, 負荷通知, DTC)LLQ, CBWFQ、 ToS/CoS制御、 シェーピング		WFQ ToS/CoS制御、 シェービング	優先制御、 ToS/CoS制御、 シェーピング
拡張機能	パケット フィルタ (静的)	MACアドレス, IPアドレス, プロトコル, URLフィルタリング(内部DB 型)	MACアドレス, IPアドレス, プロトコル, URLフィルタリング(内部DB 型)	MACアドレス, IPアドレス, プロトコル, ポート番号	MACアドレス, IPアドレス, プロトコル	MACアドレス, IPアドレス, プロトコル	MACアドレス, IPアドレス, プロトコル
	パケット フィルタ (動的)	ステートフル・インスペクシ ヨン (TCP/UDP/ICMP), URLフィルタリング(外部DB 型) *4	ステートフル・インスペクシ ョン (TCP/UDP/ICMP), URLフィルタリング(外部DB 型) *4	ステートフル・インスペク ション, Winnyフィルタ, Shareフ ィルタ, URL(内部DB参照型)	ステートフル・インスペク ション	ステートフル・インスペク ション	ステートフル・インスペク ション URLフィルタ(オプション)
VPN	対応方式	IPIP、GRE、IPSec	IPIP、GRE、IPSec	IPIP、IPsec	IPIP、GRE、IPSec	IPIP、IPsec	IPIP、IPsec
	暗号 DES, 3DES アルゴリズ AES(128/192/256bit) AES(:		DES, 3DES AES(128/192/256bit)	DES, 3DES, AES(128/256bit)	DES, 3DES AES(128/192/256bit)	DES, 3DES AES(128/192/256bit)	3DES, AES(128/192/256bit)
	対地数	128	128	100	50	250	100
	IKEv2	0	0	0	0	0	0
	認証 アルゴリズ ム	MD5, SHA-1, SHA-2(256/384/512bit)	MD5, SHA-1, SHA-2(256/384/512bit)	MD5, SHA-1, SHA-256	MD5, SHA-1, SHA-2(256/384/512bit)	MD5, SHA-1, SHA-2	SHA-1, SHA-2(256/512bit)
不正端末アクセス防止,		IEEE802.1X, MACアドレス認証	IEEE802.1X, MACアドレス認証	DHCP端末認証	IEEE802.1X, MACアドレス認証	IEEE802.1X, MACアドレス認証	-
保守機能		SNMPv1/v2c(IPv4/IPv6) sFlow(IPv4/IPv6)	SNMPv1/v2c(IPv4/IPv6) sFlow(IPv4/IPv6)	SNMPv1/v2c/v3	SNMPv1/v2c/v3	SNMPv1/v2c/v3	SNMPv1/v2c/v3
ソフトウェア管理	機能	プログラムファイル2面管理 、	プログラムファイル2面管理 、	ファームウェア多重	-	構成定義2面管理	-
		自動バージョンアップ	自動バージョンアップ				

2018年1月 当社調べ



競合他社 比較一覧(センタルータ)

			NEC IX3015	NEC IX3310	NEC IX3315	A社小規模拠点用ルー タ	B社小規模拠点用ルー タ	C社小規模拠点用ギガ ルータ	E社小規模拠点用ギガ ルータ
希望小売価格(税別)		税別)	338,000円	798,000円	998,000円	528,000円	820,000円	999,000円	OPEN価格
性能(2	公称值)		最大200Mbps	最大2.68Gbps	最大14.8Gbps	最大4.0Gbps	不明	非公開	不明
IPsec	性能(公和	尓値)	最大195.3Mbps	最大936.7Gbps	最大5.06Gbps	最大1.5Gbps	最大550Mbps	最大500Mbps	不明
FastEt (10/1	thernet 00)	ポート	2port +4HUB	-	-	-	-	0(最大10)port	-
Gigab	itEtherr	netポート	-	2+4SFP	2port + 2SFP port + 8HUB(×2)	4+4SFP	2 port	4+2SFP port	4port
八 	消費電	力	最大25W(40VA)	最大40W(35VA)	最大75W(80VA)	最大37W(38VA)	最大40W	7 0 W	最大75W
ド 仕	騒音		50dB以下	50dB以下	50dB	不明	最大時61dB	50dB	不明(ファンあり)
惊	環境へ	の配慮	RoHS対応	RoHS対応	RoHS対応	RoHS対応	不明	不明	RoHS対応
	温度条件 湿度条件(非結露)		0℃~40℃ 90%以下	0~45℃ 90%以下	0~40℃ 90%以下	0~40℃ 15~80%	0~40℃ 10~85%	0~40℃ 15~85%	0~40℃ 10~90%
設置性			横置き 19インチラック	横置き 19インチラック	横置き、 19インチラック	横置き 19インチラック	横置き 19インチラック	横置き 19インチラック	横置き 19インチラック
ブリッ	ジ機能		0	0	0	0	0	0	0
VLAN			IEEE802.1QタグVLAN (32/ポート) ポートベースVLAN	IEEE802.1QタグVLAN (32/ポート) ポートベースVLAN	IEEE802.1QタグVLAN (1000/ポート) ポートベースVLAN	IEEE802.1QタグVLAN ポートベースVLAN	IEEE802.1QタグVLAN	IEEE802.1QタグVLAN	IEEE802.1QタグVLAN
データ	'コネク	卜対応	O (オンデマンドVPN)	○ (オンデマンドVPN)	○ (データコネクトVPN)	0	-	-	0
ルーテ グ (IPv4)	-イン)	対応方式	RIP/RIPv2、OSPFv2、 BGP4、 ポリシールーティング	RIP/RIPv2、OSPFv2、 BGP4、 ポリシールーティング	RIP/RIPv2、OSPFv2、 BGP4、 ポリシールーティング	RIP/RIPv2、OSPFv2、 BGP4、 ポリシールーティング	RIP/RIPv2、 EIGRP、IS-IS、 ポリシールーティング	RIP/RIPv2、OSPFv2、 BGP4、 ポリシールーティング	RIP/RIPv2、OSPFv2、 BGP4 ポリシールーティング
		OSPFネイ バ数	128	128	128	60	不明	100	不明
		BGPピア数	128	256	1000	60000	不明	200	不明
		マルチキャスト	スタティック, IGMPv1/v2, IGMPプロキシ, PIM-SM	スタティック, IGMPv1/v2, IGMPプロキシ, PIM-SM	スタティック, IGMPv1/v2, IGMPプロキシ, PIM- SM	IGMPv2/v3, PIM-SM	IGMPv1/v2/v3, IGMPスヌーピング, PIM-DM, PIM-SM, PIM-SSM	IGMPv2, PIM-DM, PIM-SMv2	-



競合他社 比較一覧(センタルータ)

		NEC IX3015	NEC IX3110	NEC IX3315	A社小規模拠点用ルー タ	B社小規模拠点用ルー タ	C社小規模拠点用ギガ ルータ	E社小規模拠点用ギガ ルータ
冗長機能	機能	VRRPv2	VRRPv2	VRRPv2	VRRP	VRRP、HSRP	VRRP	VRRP
	ICMP Echo監視 による経 路制御	Staticルート隠蔽, ポリシールーティング隠 蔽, 任意のコマンド実行, VRRP停止	Staticルート隠蔽, ポリシールーティング隠 蔽 任意のコマンド実行, VRRP停止	Staticルート隠蔽, ポリシールーティング隠 蔽 任意のコマンド実行, VRRP停止	Staticルート隠蔽, VRRP停止	Staticルート隠蔽, ポリシールーティング隠 蔽 VRRP停止	StaticJレート隠蔽, VRRP停止	Staticルート隠蔽, ポリシールーティング隠 蔽 VRRP停止
QoS		PQ、CBQ、LLQ、 ToS/CoS制御、 シェーピング	PQ、CBQ、LLQ、 ToS/CoS制御、 シェーピング	PQ、CBQ、LLQ、 ToS/CoS制御、 シェーピング	PQ, CBQ, WFQ ToS/CoS制御、シェー ピング, 適応型QoS	LLQ, CBWFQ、 ToS/CoS制御、 シェーピング	WFQ, ToS/CoS制御、 シェーピング	PQ, CBQ, PFIFO, TBF, SFQ、ToS/CoS制御、 帯域制御
拡張機能	パケット フィルタ (静的)	MACアドレス, IPアドレ ス, プロトコル, URLフィルタリング(内 部DB型)	MACアドレス, IPアドレ ス, プロトコル, URLフィルタリング(内 部DB型)	MACアドレス, IPアドレ ス, プロトコル, URLフィルタリング(内 部DB型)	MACアドレス, IPアドレ ス, プロトコル, ポート番号 , URL(内部DB参照型)	MACアドレス, IPアドレ ス, プロトコル	MACアドレス, IPアドレ ス, プロトコル	MACアドレス, IPアドレ ス, プロトコル
	パケット フィルタ (動的)	ステートフル・インスペ クション (TCP/UDP/ICMP), URLフィルタリング(外 部DB型) *4	ステートフル・インスペ クション (TCP/UDP/ICMP), URLフィルタリング(外 部DB型) *4	ステートフル・インスペ クション (TCP/UDP/ICMP), URLフィルタリング(外 部DB型) *4	ステートフル・インスペ クション,Winnyフィル タ, URL(外部DB参照型: デジタルアーツ,トレン ドマイクロ, NetSTAR)	ステートフル・インスペ クション	ステートフル・インスペ クション	ステートフル・インスペ クション
VPN	対応方式	IPIP、GRE、IPSec	IPIP、GRE、IPSec	IPIP、GRE、IPSec	IPIP、IPsec	IPIP、GRE、IPSec	IPIP、IPsec	IPIP、GRE、IPSec
	暗号 アルゴリ ズム	DES, 3DES, AES(128/192/256bit)	DES, 3DES AES(128/192/256bit)	DES, 3DES AES(128/192/256bit)	DES, 3DES, AES(128/256bit)	DES, 3DES AES(128/192/256bit)	DES, 3DES AES(128/192/256bit)	DES, 3DES, AES(128/192/256bit)
	対地数	512	128	5000	1000	150	1000	4096
	IKEv2	0	0	0	0	0	0	0
	認証 アルゴリ ズム	MD5, SHA-1, SHA- 2(256/384/512bit)	MD5, SHA-1, SHA- 2(256/384/512bit)	MD5, SHA-1, SHA- 2(256/384/512bit)	MD5, SHA-1, SHA- 256	MD5, SHA-1, SHA- 2(256/384/512bit)	MD5, SHA-1	MD5, SHA-1, SHA- 2(256/384/512bit)
不正端末アクセス防止		IEEE802.1X, MACアドレス認証	IEEE802.1X, MACアドレス認証	IEEE802.1X, MACアドレス認証	-	IEEE802.1X, MACアドレス認証 Port認証	IEEE802.1X, MACアドレス認証	Web認証
保守機能		SNMPv1/v2c (IPv4/IPv6)	SNMPv1/v2c (IPv4/IPv6)	SNMPv1/v2c (IPv4/IPv6)	SNMPv1/v2c/v3	SNMPv1/v2c/v3	SNMPv1/v2c/v3	SNMPv1/v2c
ソフトウェア管	理機能	プログラムファイル2面 管理、 自動バージョンアップ	プログラムファイル2面 管理、 自動バージョンアップ	プログラムファイル2面 管理、 自動バージョンアップ	ファームウェア多重	-	構成定義2面管理	レスキューファームウェ ア

2018年1月 当社調べ

Empowered by Innovation

