ISDN access router config

ISDN アクセスルータ コンフィグ

Version 0.3

保証免責
本書は記載事項またはそれに関わる事項について、明示的あるいは暗黙的な保証はいたしておりません。
したがいまして、これらを原因として発生した損失や損害についての責任を負いません。

表記について

本書では以下の書体を使用しています。

- イタリック文字

  本文中でのコマンド、ファイル名、変数など可変なパラメータ値を表します。

- 等幅文字

  ファイルの内容やコマンドの入出力例に使います。入力の場合にはボールドで表します。

```
$ cd /usr/src/sys/i386/conf
$ ls
GENERIC         Makefile      OLDCARD       SMP
GENERIC.hints   NOTES         PAE           gethints.awk
$
```

- 省略文字

  ファイルの内容やコマンドの入出力例を省略する場合に'...'を使います。

```
$ vi /etc/rc.conf
  ...
sshd_enable="YES"
named_enable="YES"
  ...
$
```

- プロンプト

  一般または、管理権限を持った実行環境をそれぞれ、'$'(ドル)、'#'(シャープ)のプロンプトで表します。

```
$ su
Password: root's passwd
#
```

目次

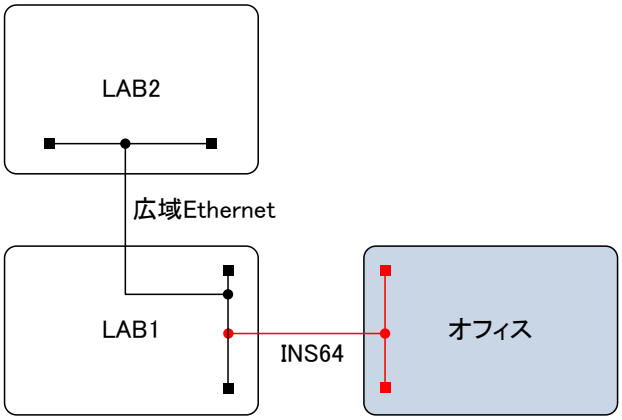
1. 概要 1
1.1. はじめに 1
1.2. 参考文献 1
1.3. 謝辞 1
2. ネットワーク概要 2
2.1. 全体図(抜粋) 2
2.2. アクセスルータ 3
3. IOS コンフィグレーション 4
3.1. WAN 側 I/F 4
3.2. PPP/CHAP 認証 4
3.3. DDR 4
3.4. 静的経路 5
3.5. パケットフィルタリング 5
3.6. startup-config 5
4. 添付資料 8
4.1. サーバの静的経路 8
4.2. フラッシュ IOS の復旧 8

1. 概要

1.1. はじめに

本書は ISDN 回線で接続された検証環境のネットワーク構成、アクセスルータの設定等について記述したものです。

下図は極めてシンプルな拠点間接続を表していますが、LAB1～オフィスまでが本書の守備範囲となっています。また、アクセスルータの設定についてはオフィス側のみを記述します。



1.2. 参考文献

下記の文書も併せてご参照ください。

文書名	リンク
Cisco 1812J ソフトウェア コンフィギュレーション ガイド	http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/rt/1812/1800sscg/index.shtml
統合デジタル通信網サービス (ISDN) – 設定例とテクニカル ノーツ	http://www.cisco.com/JP/support/public/nav/lll_268435524_10_236.shtml

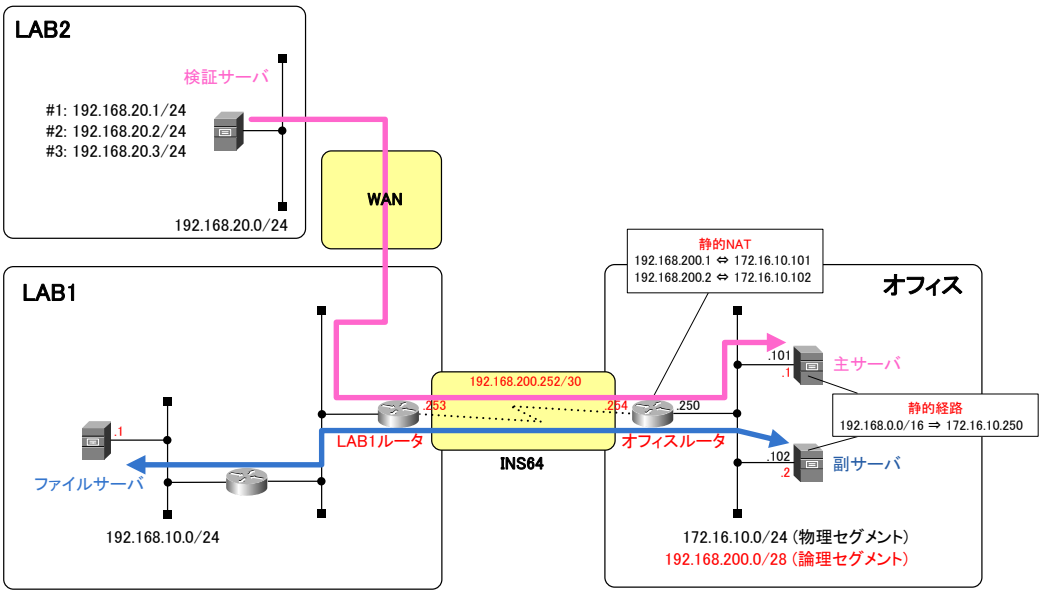
1.3. 謝辞

本書の作成にあたり、古くからの友人 **sh** 様より多大な助言を賜りました。ここに感謝の意を表明します。

2. ネットワーク概要

2.1. 全体図(抜粋)

オフィス拠点から見て隣接している拠点は LAB1 拠点となりますが、この拠点間は INS64 回線で接続されています。



オフィス拠点のネットワークは対向ネットワークから見て異なる論理セグメントとなっています。

すなわち、LAB2、LAB1 拠点からオフィス側へ通信する場合、宛先ネットワークは 192.168.200.0/28 としてオフィスルータへ到達し、実際の到達ネットワークである 172.16.10.0/24 へ NAT されます。

また、オフィス拠点から対向拠点へ通信する場合、サーバ上のデフォルト経路はインターネット側に向いているため、明示的な静的経路を設定し、パケットがオフィスルータへ向くようにします。

2.2. アクセスルータ

拠点間接続のエッジルータとして Cisco 1812J を導入しています。詳細は Cisco 1812J ハードウェア インストレーション ガイドを参照してください。

機器背面の各ポートを下表のように直収します。

番号	コメント
①	ISDN S/T ポートです。 RJ-11 モジュラケーブルによって、匡体 S/T ポートと搭載ラック下に配置している DSU の TERMINAL1 ポートに結線します。また、DSU の LINE ポートには構内配線された ISDN 回線を結線します。
②	イーサネットポートです。 RJ-45 モジュラケーブルによって匡体 FE0 ポートとラック内 L2 スイッチ間を結線します。

試験環境用のアクセスルータですので冗長構成等を考慮していません。

3. IOS コンフィグレーション

3.1. WAN 側 I/F

CDP(Cisco Discovery Protocol)とは、Cisco 独自のデータリンク層プロトコルで隣接デバイスの情報を交換するものです。Cisco 製品以外のデバイスとは互換性がありません。

設定パラメータ	設定内容
CDP	CDP を有効化しない。
IP アドレス	192.168.200.254/30

3.2. PPP/CHAP 認証

ホスト名、パスワードは対向ルータ上にも同様の設定を行いますので、無断で変更してはなりません。

設定パラメータ	設定内容
データリンク層カプセルタイプ	PPP
PPP 認証方式	CHAP
ホスト名	任意。LAB1 側ルータの CHAP 認証に使用されます。
パスワード	任意。LAB1 側ルータの CHAP 認証に使用されます。

3.3. DDR

DDR(Dial on Demand Routing)とは、必要なトラフィックが LAN から WAN 側へ流れた際に、ISDN 回線を発呼する手段です。

下表要件により、通常 ISDN 回線は切断されていますが、LAN から IP パケットが WAN 側に通過する際に、ISDN 回線を接続します。

設定パラメータ	設定内容
発呼回線 ID	オフィス側の回線(電話)番号。
着呼回線 ID	LAB1 側の回線(電話)番号。着呼制限に使用されます。
ISDN スイッチタイプ	ISDN 交換機タイプ。本邦では NTT 東日本となります。
ネクストホップ	LAB1 側ルータの IP アドレス。
インタレスティングパケット	IP

3.4. 静的経路

下表の通信要件により、経路設定を行います。

ネットワーク ID	ネクストホップ	備考
デフォルトルート	172.16.10.254	LAN 側。
192.168.10.0/24	192.168.200.253	LAB1 サイト。
192.168.20.0/24	192.168.200.253	LAB2 サイト。

3.5. パケットフィルタリング

下表の通信要件により、ACL を作成します。

送信元	送信先	プロトコル	通信可否	備考
192.168.20.0/24	192.168.200.0/28	443	許可	LAB2→オフィス
192.168.10.0/24	192.168.200.0/28	21	許可	LAB1→オフィス
192.168.10.0/24	192.168.200.0/28	20	許可	LAB1→オフィスの戻り
192.168.200.0/28	192.168.10.0/24	21	許可	オフィス→LAB1 の戻り
192.168.200.0/28	192.168.10.0/24	20	許可	オフィス→LAB1
—	—	icmp	許可	
—	—	ip	拒否	上記以外は全て拒否

3.6. startup-config

実際のコンフィグレーションは下記のとおりです。

主だった設定箇所に番号を採番していますので、説明はコンフィグレーション以降の下表を参照してください。

```
!
! Last configuration change at 09:54:54 JST Wed Jul 16 2008
! NVRAM config last updated at 10:20:49 JST Tue Jul 15 2008
!
version 12.4
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname office                                                    ①
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 debugging
logging console informational
enable secret 5 $1$mkLRe35sj9Q/st$Xk53I6qzFaEY
!
no aaa new-model
!
resource policy
!
clock timezone JST 9
!
!
ip cef
!
!
no ip domain lookup
!
isdn switch-type ntt
!
!
username lab1 password 7 1995AA3B0201236                           ②
!
```

```
!
interface FastEthernet0                                                    ③
 ip address 172.16.10.250 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface BRI0                                                             ④
 ip address 192.168.200.254 255.255.255.252
 ip access-group LAB1-IN in
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 dialer map ip 192.168.200.253 name lab1 03XXXXXXXX
 dialer-group 1
 isdn switch-type ntt
 isdn caller 03XXXXXXXX
 no keepalive
 no cdp enable
 ppp authentication chap
!
interface FastEthernet2
!
interface FastEthernet3
!
interface FastEthernet4
!
interface FastEthernet5
!
interface FastEthernet6
!
interface FastEthernet7
!
interface FastEthernet8
!
interface FastEthernet9
!
interface Vlan1
 no ip address
!
ip route 0.0.0.0 0.0.0.0 172.16.10.254                                     ⑤
ip route 192.168.10.0 255.255.255.0 192.168.200.253
ip route 192.168.20.0 255.255.255.0 192.168.200.253
!
!
no ip http server
no ip http secure-server
ip nat inside source static 172.16.10.101 192.168.200.1                    ⑥
ip nat inside source static 172.16.10.102 192.168.200.2
!
ip access-list extended LAB1-IN                                            ⑦
  permit tcp 192.168.20.0 0.0.0.255 192.168.200.0 0.0.0.15 eq 443
  permit tcp 192.168.10.0 0.0.0.255 192.168.200.0 0.0.0.15 eq ftp
  permit tcp 192.168.10.0 0.0.0.255 192.168.200.0 0.0.0.15 eq ftp-data establi
shed
  permit tcp 192.198.10.0 0.0.0.255 eq ftp 192.168.200.0 0.0.0.15 established
  permit tcp 192.168.10.0 0.0.0.255 eq ftp-data 192.168.200.0 0.0.0.15
  permit icmp any any
  deny   ip any any log
!
dialer-list 1 protocol ip permit                                           ⑧
!
!
control-plane
```

```
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0
 exec-timeout 0 0
 password 7 051837A072B11E175C
 login
line vty 1 4
 password 7 051837A072B11E175C
 login
!
ntp clock-period 17180302
ntp server 172.16.10.201 prefer
!
webvpn context Default_context
 ssl authenticate verify all
 !
 no inservice
!
end
```

番号	説明
①	オフィスルータのホスト名を定義します。 このホスト名は対向の LAB1 ルータがオフィスルータへ発呼する場合の CHAP 認証に使用されます。
②	LAB1 ルータのホスト名とパスワードを定義します。 オフィスルータが対向の LAB1 ルータへ発呼する場合の CHAP 認証に使用されます。
③	LAN 側 I/F を定義します。この I/F は NAT する際の内部と位置づけます。
④	WAN 側 I/F を定義します。この I/F は NAT する際の外部と位置づけます。 この I/F は ISDN 回線に接続され、パケット交換機が NTT 仕様であることを明示します。また、パケットのカプセル化を PPP によって行い、認証方式に CHAP を選択します。 後述する⑧により、この I/F に IP パケットが転送された場合に、LAB1 ルータへ発呼し回線を接続します。 逆にオフィスルータが着呼を受け付ける対向を LAB1 ルータにのみ限定します。 この I/F を通過する通信に対して後述する⑦のアクセスリスト LAB1-IN を定義します。また、この I/F では CDP を有効化しません。
⑤	デフォルトルートは LAN 側の 172.16.10.254 とします。 また、LAB2 サイト、LAB1 サイト宛のパケットを WAN 側へ転送します。
⑥	オフィスルータの内側(LAN)を往来す下記の送信元に該当するパケットは 1:1 の NAT を行います。 172.16.10.101 ⇔ 192.168.200.1 172.16.10.102 ⇔ 192.168.200.2
⑦	「3.5. パケットフィルタリング」の要件に基づき、ACL を定義します。 ip access-list standard では送信元アドレスのみを条件としたフィルタリングルールしか記述できないため、ip access extended を定義します。extended では送信元、送信先に加えてポート番号によるフィルタが可能となります。
⑧	LAB1 ルータ宛に発呼する通信を IP のみとします。

4. 添付資料

4.1. サーバの静的経路

「2.1. 全体図(抜粋)」で前述したように、オフィス拠点から対向拠点へパケットが向う場合、サーバからオフィスルータへ到達できるようにサーバ上にも静的経路を設定しなくてはなりません。

下記のように、172.16.10.101、172.16.10.102 へ経路を設定します。

```
# route add -net 192.168.0.0 mask 255.255.0.0 172.16.10.250 metric 1
# netstat -rn
  ...
192.168.0.0   172.16.10.250  255.255.0.0     UG     0 0       0 eth1
  ...
#
```

恒久的な設定とするために/etc/sysconfig/network-scripts/route-eth1 ファイルに下記の設定を行っておくとよいでしょう。

```
# vi /etc/sysconfig/network-scripts/route-eth1
  ...
192.168.0.0/16 via 172.16.10.250 metric 1
  ...
```

4.2. フラッシュ IOS の復旧

試験環境用のアクセスルータを設定する際に、コンパクトフラッシュ(32MB)が破損して IOS をロードできない現象が発生しました。本節では、その際の復旧手順を記述しておきます。

① IOS イメージの用意

通常、IOS イメージは自由に入手できるものではないため、保守ベンダから入手しておきます。Cisco 1812J 用のイメージファイルは c181x-advipservicesk9-mz.124-6.T7.bin です。

② tftp サーバの用意

tftp 経由で IOS イメージをルータのフラッシュへ書込むため、イメージファイルを所定ディレクトリ上へ配置します。

本書では、xinetd 経由で tftp デーモンを起動する方式に基づいて、下記のように設定を行いました。

```
# cat /etc/xinetd.d/tftp
service tftp
{
     disable      = no
     socket_type  = dgram
     protocol     = udp
     wait         = yes
     user         = root
```

```
      server        = /usr/sbin/in.tftpd
      server_args   = -s /tftpboot
      per_source    = 11
      cps           = 100 2
      flags         = IPv4
}
#
```

IOS イメージを下記のディレクトリへコピーしておきます。

```
# cd /tftpboot
# ls
c181x-advipservicesk9-mz.124-6.T7.bin
#
```

③ ルータの調整

tftp ダウンロードの前にルータの ROMmon モードで環境変数を設定します。

要旨としては、ルータにテンポラリの IP アドレス、tftp サーバの IP アドレスとダウンロードする IOS イメージファイル名を設定しておきます。

```
rommon 1 > IP_ADDRESS=10.1.100.40
rommon 2 > IP_SUBNET_MASK=255.255.255.0
rommon 3 > DEFAULT_GATEWAY=10.1.100.254
rommon 4 > TFTP_SERVER=10.1.200.50
rommon 5 > TFTP_FILE=c181x-advipservicesk9-mz.124-6.T7.bin
rommon 6 > TFTP_VERSION=2
rommon 7 >
```

④ IOS イメージのダウンロード

下記のようにダウンロードを行います。tftp サーバからコンパクトフラッシュへ IOS イメージがコピーされます。

```
rommon 8 > tftpdnld

         IP_ADDRESS  : 10.1.100.40
      IP_SUBNET_MASK : 255.255.255.0
     DEFAULT_GATEWAY : 10.1.100.254
        TFTP_SERVER  : 10.1.200.50
          TFTP_FILE  : c181x-advipservicesk9-mz.124-6.T7.bin
       TFTP_MACADDR  : 00:13:72:4b:05:e9
       TFTP_VERBOSE  : Verbose
    TFTP_RETRY_COUNT : 18
       TFTP_TIMEOUT  : 7200
      TFTP_CHECKSUM  : Yes
            FE_PORT  : 0
      FE_SPEED_MODE  : Auto Detect

Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!
Do you wish to continue? y/n:  [n]:  y

Performing tftpdnld over Fast Enet.
Initializing interface.
ARPing for 10.1.200.50
ARP reply for 10.1.200.50 received.  MAC address 00:13:72:4b:05:e9
Receiving c181x-advipservicesk9-mz.124-6.T.bin from 10.1.200.50 !!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  ...
  ...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
File reception completed.
Validating checksum.
Copying file c181x-advipservicesk9-mz.124-6.T7.bin to flash.
program load complete, entry point: 0x80012000, size: 0xc0c0
```

```
Initializing ATA monitor library.......

Format: Drive communication & 1st Sector Write OK...
Writing Monlib sectors.
................................
........................................
..................
Monlib write complete

Format: All system sectors written. OK...
Format: Operation completed successfully.

Format of flash: complete
program load complete, entry point: 0x80012000, size: 0xc0c0

Initializing ATA monitor library.......

rommon 9 > dir flash:
program load complete, entry point: 0x80012000, size: 0xc0c0

Initializing ATA monitor library.......
Directory of flash:

2     16925304  -rw-    c181x-advipservicesk9-mz.124-6.T7.bin

rommon 10 >
```

⑤ IOS のブート

下記のようにダウンロードを行います。tftp サーバからコンパクトフラッシュへ IOS イメージがコピーされます。

```
rommon 11 > boot
program load complete, entry point: 0x80012000, size: 0xc0c0

Initializing ATA monitor library.......
program load complete, entry point: 0x80012000, size: 0xc0c0

Initializing ATA monitor library.......

program load complete, entry point: 0x80012000, size: 0x101999c
Stack pointer       : 0x08000000
monstack            : 0x8000549C
monra               : 0x00000000
edata               : 0x800167D0
magic               : 0xFEEDFACE
memsize             : 0x08000000
uncomp_size         : 0x03299C54
comp_size           : 0x010151B6
STACK_BYTES         : 0x00008000
COPY_CODE_BUF       : 0x00000800
_end                : 0x8003F044
comp_checksum       : 0x10E5B470
comp_checksum       : 0x10E5B470
uncomp_checksum     : 0x253667B2
Self decompressing the image : ########################################################
########################################################################################
########################################################################################
########################################################################################
################################ [OK]
Source elf_hdr->e_shnum = 0x00000009
Setting up to copy ELF section 0x00000001
 to image_info section 0x00000000
 sh_name = 0x0000000B
 sh_type = 0x00000001
 sh_flags = 0x00000007
 sh_addr = 0x80012000
 sh_offset = 0x00000060
 sh_size = 0x01F0ACEC
 sh_link = 0x00000000
 sh_info = 0x00000000
 sh_addralign = 0x00000020
 sh_entsize = 0x00000000
Setting up to copy ELF section 0x00000002
```

```
 to image_info section 0x00000001
 sh_name = 0x00000011
 sh_type = 0x00000001
 sh_flags = 0x00000002
 sh_addr = 0x81F1CCEC
 sh_offset = 0x01F0AD4C
 sh_size = 0x01054F9C
 sh_link = 0x00000000
 sh_info = 0x00000000
 sh_addralign = 0x00000008
 sh_entsize = 0x00000000
Setting up to copy ELF section 0x00000004
 to image_info section 0x00000002
 sh_name = 0x00000021
 sh_type = 0x00000001
 sh_flags = 0x00000003
 sh_addr = 0x82F71C88
 sh_offset = 0x02F5FCE8
 sh_size = 0x00339B98
 sh_link = 0x00000000
 sh_info = 0x00000000
 sh_addralign = 0x00000008
 sh_entsize = 0x00000000
Setting up to copy ELF section 0x00000005
 to image_info section 0x00000003
 sh_name = 0x00000027
 sh_type = 0x00000001
 sh_flags = 0x00000003
 sh_addr = 0x832AB820
 sh_offset = 0x03299880
 sh_size = 0x00000230
 sh_link = 0x00000000
 sh_info = 0x00000000
 sh_addralign = 0x00000004
 sh_entsize = 0x00000000
cpu type            : 0x00000013
uncomp_size                   : 0x03299C54
monstack                      : 0x8000549C

image_info.entry_point        = 0x80012000
image_info.section_count      = 0x00000004
image_info.monstack           = 0x8000549C
image_info.monra              = 0x00000000
image_info.param0             = 0x00000002
image_info.param1             = 0x00000000
image_info.param2             = 0x00000000
image_info.param3             = 0x00000000
Section Index       = 0x00000000
   source           = 0x8003F1A4
   dest             = 0x80012000
   bytes            = 0x01F0ACEC
Section Index       = 0x00000001
   source           = 0x81F49E90
   dest             = 0x81F1CCEC
   bytes            = 0x01054F9C
Section Index       = 0x00000002
   source           = 0x82F9EE2C
   dest             = 0x82F71C88
   bytes            = 0x00339B98
Section Index       = 0x00000003
   source           = 0x832D89C4
   dest             = 0x832AB820
   bytes            = 0x00000230

            Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

         cisco Systems, Inc.
         170 West Tasman Drive
         San Jose, California 95134-1706



Cisco IOS Software, C181X Software (C181X-ADVIPSERVICESK9-M), Version 12.4(6)T,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
```

```
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Wed 22-Feb-06 21:22 by ccai
Image text-base: 0x80012124, data-base: 0x81F1CCEC


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Installed image archive
Cisco 1812-J (MPC8500) processor (revision 0x400) with 118784K/12288K bytes of memory.
Processor board ID FHK1019226G, with hardware revision 0000

10 FastEthernet interfaces
1 ISDN Basic Rate interface
31360K bytes of ATA CompactFlash (Read/Write)


        --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no


Press RETURN to get started!

Router>
```

上記のように Router>プロンプトが表示されるところまで遷移すれば起動に問題はありません。

⑥ コンフィグレーションレジスタの変更

ルータ再起動時に IOS が自動的に立ち上がるように、コンフィグレーションレジスタ値を 0x2102 に変更します。

```
Router>
Router>enable
Router#conf t
Router(config)#config-register 0x2102
Router(config)#^Z
Router# reload

System configuration has been modified. Save? [yes/no]: yes
Building configuration...
[OK]
Proceed with reload? [confirm]ENTER
  ...
  ...
```

ISDN access router config

改版履歴

Version 0.1	2008/10/29	新規作成。
Version 0.2	2009/01/28	「2.2. アクセスルータ」節を修正。
Version 0.3	2009/02/03	「4.2. フラッシュ IOS の復旧」節を修正。

製作

LA TIGRE

本書は 2009 年 2 月現在の情報を元に作成されております。本書に記載されております内容は、許可なく変更されることがあります。