
EIGRP/HSRP settings by Cisco router

Cisco ルータによる EIGRP/HSRP 設定

Version 0.2

Copyright © 2008 LA TIGRE.

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。したがって、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。

著作権

本書および本書に記載されておりますソフトウェア等は、著作権により保護されております。また非商用以外に本書を、複製、再頒布することをかたく禁止いたします。

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. 拠点間接続.....	1
1.3. 参考文献・謝辞.....	1
2. ネットワーク概要.....	2
2.1. ルータ冗長構成.....	2
2.2. ネットワーク構成.....	3
2.3. 経路の広報.....	4
2.4. サーバ構成.....	4
2.5. アクセスコントロール.....	5
2.6. アクセスルータ.....	5
3. IOS コンフィグレーション.....	6
3.1. 1号機の startup-config.....	6
3.2. 2号機の startup-config.....	9
3.3. サーバ上の静的経路.....	12
4. ルータ保守.....	13
4.1. ログイン方法.....	13
4.2. ログの表示.....	13
4.3. HSRP の状態確認.....	14
4.4. トラッキングの状態確認.....	14
4.5. インタフェースの状態確認.....	15
4.6. 経路の状態確認.....	15
4.7. S/W、H/W の状態確認.....	15
5. 添付資料.....	16
5.1. フラッシュ IOS の復旧.....	16

1. 概要

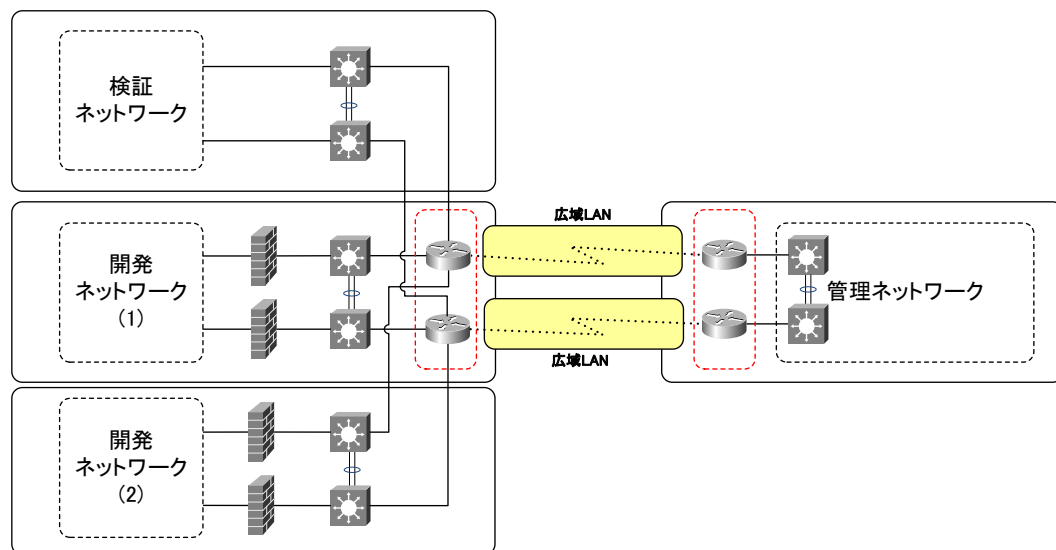
1.1. はじめに

本書はいくつかの拠点間を専用線で結び、管理拠点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。

管理拠点の対向には、検証、開発環境のネットワークが存在し、Cisco ルータを用いた EIGRP による経路交換、HSRP による耐障害性の向上について主要な設定をまとめたものとなっています。

1.2. 拠点間接続

本書では管理拠点の各種構成について記述しています。ネットワーク間は下図のように接続されています。



1.3. 参考文献・謝辞

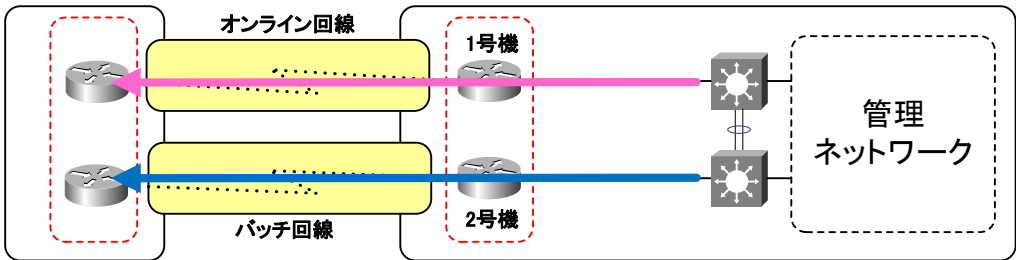
下記の文書も併せてご参照ください。本書の作成にあたり、古くからの友人 **sh** 様より多大な助言を賜りました。ここに感謝の意を表明します。

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/1812/1800sscsg/index.shtml
Cisco ルーターIP ルーティング Black Book	Innokenty Rudenko 著 岡 利章 訳

2. ネットワーク概要

2.1. ルータ冗長構成

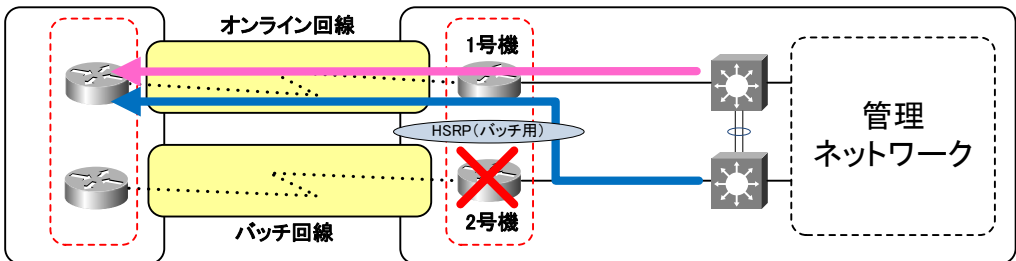
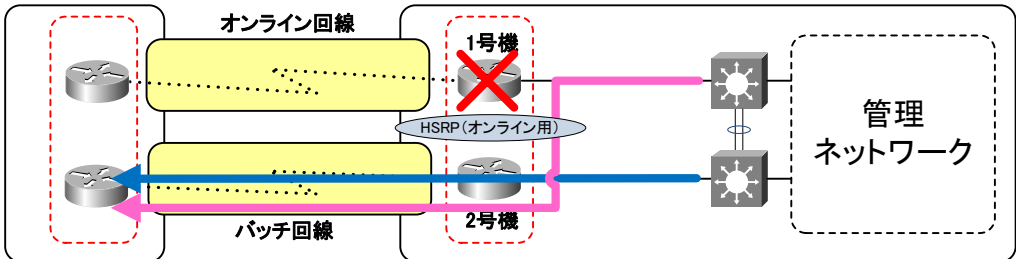
通信内容には、オンライン処理系とバッチ処理系があります。



片系の障害発生時には、通信可能な経路を選択できるよう、**HSRP**(Hot Standby Router Protocol)で構成します。それぞれの待機系を負担させる形で設定します(MHSRP)。

通常時(アクティブ)	ルータ	回線	障害時(スタンバイ)
オンライン通信時	1号機	オンライン回線	2号機(バッチ回線)
バッチ通信時	2号機	バッチ回線	1号機(オンライン回線)

下図は障害発生時の通信経路を示しています。



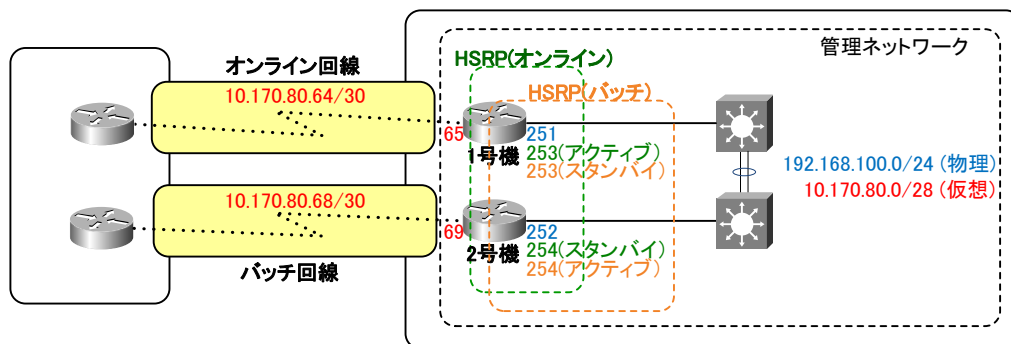
管理拠点だけではなく、対向拠点側でも上述の経路迂回に対応できるよう内部ネットワーク内で経路制御が行われています。

2.2. ネットワーク構成

管理拠点のネットワークは対向ネットワークから見て仮想的なセグメントとなっています。

すなわち、検証、開発(1)、および開発(2)拠点から管理拠点へ通信する場合、宛先ネットワークは **10.170.80.0/28** として管理拠点のルータへ到達し、実際の到達ネットワークである **192.168.100.0/24** へ NAT されます。

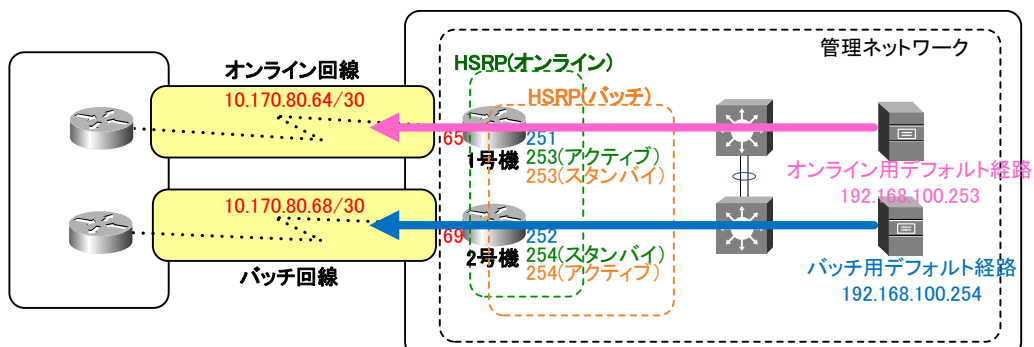
また、管理拠点から対向拠点へ通信する場合、サーバ上のデフォルト経路はインターネット側に向いているため、明示的な静的経路を設定し、パケットが管理拠点ルータへ向くようにします。



前節で記述した HSRP について、まとめると下表のようになります。

機器名	通常時(アクティブ)	ルータ仮想 IP	障害時(スタンバイ)	ルータ物理 IP
1 号機	オンライン通信時	192.168.100.253/24	192.168.100.254/24	192.168.100.251/24
2 号機	パッチ通信時	192.168.100.254/24	192.168.100.253/24	192.168.100.252/24

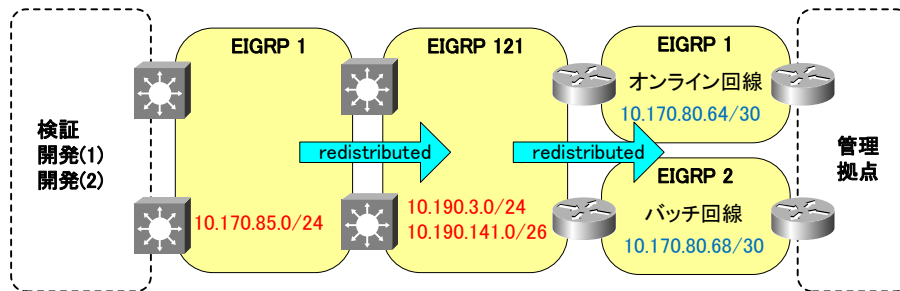
サーバ上から対向拠点向けに静的経路を指定する場合は、通常通信時のゲートウェイとして定められる IP アドレス(HSRP 仮想 IP)を指定すればよく、障害発生時の切り替えについてサーバは関知する必要はありません。



2.3. 経路の広報

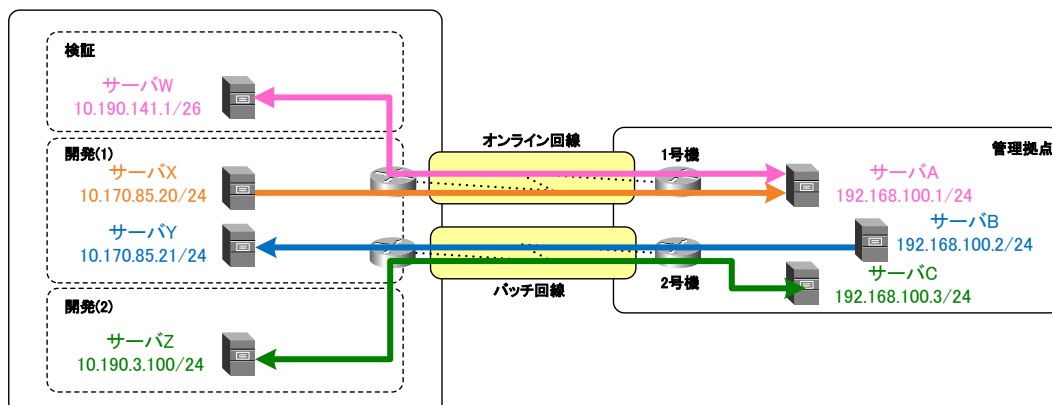
管理拠点から見て、対向拠点には多数の内部ネットワークが構築されています。

このため、管理拠点ルータには、動的な経路がいくつか EIGRP により広報されるようになっていきます。



2.4. サーバ構成

エンド・ツー・エンドの通信は下図のとおりです。



対向拠点から見て、管理拠点のサーバは 10.170.80.0/28 の仮想ネットワーク上に点在するのに見えます。管理拠点のルータ上で物理ネットワークに NAT します。

サーバ名	仮想 IP アドレス	物理 IP アドレス
aaa.mng.local	10.170.80.1/28	192.168.100.1/24
bbb.mng.local	10.170.80.2/28	192.168.100.2/24
ccc.mng.local	10.170.80.3/28	192.168.100.3/24

2.5. アクセスコントロール

管理拠点のルータには下表のポリシーに基づいたフィルタリングを設定します。

No	ACT	PROTO	SRC address	S port	DST address	D port	備考
1	許可	tcp	10.190.3.0/24	—	10.170.80.0/28	21	サーバZ→管理拠点(FTP)
2	許可	tcp	10.190.3.0/24	—	10.170.80.0/28	20	サーバZ→管理拠点(FTP)の戻り
3	許可	tcp	10.190.3.0/24	21	10.170.80.0/28	—	管理拠点→サーバZ(FTP)の戻り
4	許可	tcp	10.190.3.0/24	20	10.170.80.0/28	—	サーバZ→管理拠点(FTP)
5	許可	tcp	10.190.141.0/26	—	10.170.80.0/28	443	サーバW→管理拠点(HTTPS)
6	許可	tcp	10.170.85.0/24	—	10.170.80.0/24	443	サーバX→管理拠点(HTTPS)
7	許可	tcp	10.170.85.0/24	443	10.170.80.0/24	—	管理拠点→サーバY(HTTPS)の戻り
8	許可	eigrp	Any	—	Any	—	EIGRP
9	許可	icmp	Any	—	Any	—	ICMP
10	拒否	ip	Any	—	Any	—	上記以外の通信を拒否

2.6. 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
③	任意のポートを管理側スイッチへ結線します。
④	FE0 I/F を LAN 側スイッチへ結線します。 FE1 I/F を WAN 側メディアコンバータへ結線します。

3. IOS コンフィグレーション

3.1. 1 号機の startup-config

実際のコンフィグレーションは下記のとおりです(適宜マスクしている行もあります)。

主だった設定箇所にマーキングしていますので、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。

```

1  !
2  version 12.4
3  service timestamps debug datetime msec
4  service timestamps log datetime msec
5  service password-encryption
6  !
7  hostname router01
8  !
9  boot-start-marker
10 boot-end-marker
11 !
12 logging buffered 4096 debugging
13 enable secret 5 XXXXXXXXXXXXXXXXXXXXXXXXXXXX
14 !
15 no aaa new-model
16 !
17 resource policy
18 !
19 clock timezone JST 9
20 !
21 !
22 ip cef
23 !
24 !
25 no ip domain lookup
26 ip domain name mng.local
27 ip ssh time-out 60
28 ip ssh authentication-retries 2
29 ip ssh rsa keypair-name XXXXXXXXXXXX
30 ip ssh version 1
31 !
32 !
33 !
34 username admin password 7 XXXXXXXXXXXXXXXXXXXX
35 !
36 !
37 !
38 track 101 interface FastEthernet0 ip routing
39 !
40 !
41 !
42 !
43 !
44 interface FastEthernet0
45 ip address 192.168.100.251 255.255.255.0
46 ip nat inside
47 ip virtual-reassembly
48 duplex auto
49 speed auto
50 no cdp enable
51 standby 1 ip 192.168.100.253
52 standby 1 priority 105
53 standby 1 preempt
54 standby 1 track FastEthernet1
55 standby 2 ip 192.168.100.254
56 standby 2 preempt
57 standby 2 track FastEthernet1
58 !
59 interface FastEthernet1
60 bandwidth 512
61 ip address 10.170.80.65 255.255.255.252
62 ip access-group FE1-in in
63 ip nat outside
64 ip virtual-reassembly

```

```

65 speed 10
66 full-duplex
67 traffic-shape rate 512000 12800 12800 1000
68 no cdp enable
69 !
70 interface BRI0
71 no ip address
72 encapsulation hdlc
73 shutdown
74 !
75 interface FastEthernet2
76 !
77 interface FastEthernet3
78 !
79 interface FastEthernet4
80 !
81 interface FastEthernet5
82 !
83 interface FastEthernet6
84 !
85 interface FastEthernet7
86 !
87 interface FastEthernet8
88 !
89 interface FastEthernet9
90 !
91 interface Vlan1
92 ip address 172.16.200.251 255.255.255.0
93 !
94 router eigrp 1
95 redistribute static route-map Macth-D-Route
96 network 10.170.80.64 0.0.0.3
97 default-metric 512 2000 255 1 1500
98 no auto-summary
99 !
100 ip route 10.170.80.0 255.255.255.240 FastEthernet1 track 101
101 ip route 172.16.200.0 255.255.255.0 172.16.200.254
102 ip route 10.170.85.0 255.255.255.0 192.168.100.254 250
103 ip route 10.190.140.128 255.255.255.224 192.168.100.254 250
104 ip route 10.190.141.0 255.255.255.192 192.168.100.254 250
105 !
106 !
107 !
108 no ip http server
109 no ip http secure-server
110 ip nat inside source static 192.168.100.1 10.170.80.1
111 ip nat inside source static 192.168.100.2 10.170.80.2
112 ip nat inside source static 192.168.100.3 10.170.80.3
113 !
114 !
115 ip access-list standard D-Route-ACL
116 permit 10.170.80.0 0.0.0.15
117 deny any
118 !
119 ip access-list extended FE1-in
120 permit icmp any any
121 permit eigrp any any
122 permit tcp 10.170.85.0 0.0.0.255 10.170.80.0 0.0.0.255 eq 443
123 permit tcp 10.170.85.0 0.0.0.255 eq 443 10.170.80.0 0.0.0.255 established
124 permit tcp 10.190.3.0 0.0.0.255 10.170.80.0 0.0.0.15 eq ftp
125 permit tcp 10.190.3.0 0.0.0.255 10.170.80.0 0.0.0.15 eq ftp-data established
126 permit tcp 10.190.3.0 0.0.0.255 eq ftp 10.170.80.0 0.0.0.15 established
127 permit tcp 10.190.3.0 0.0.0.255 eq ftp-data 10.170.80.0 0.0.0.15
128 permit tcp 10.190.141.0 0.0.0.63 10.170.80.0 0.0.0.15 eq 443
129 !
130 !
131 !
132 logging history informational
133 snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
134 snmp-server enable traps eigrp
135 snmp-server enable traps envmon
136 snmp-server enable traps hsrp
137 snmp-server enable traps syslog
138 snmp-server host ZZZ.ZZZ.ZZZ.ZZZ openmng eigrp envmon hsrp syslog snmp
139 !
140 !
141 !
142 !
143 route-map Macth-D-Route permit 10
144 match ip address D-Route-ACL
145 !
146 !

```

```

147 !
148 !
149 control-plane
150 !
151 !
152 line con 0
153 password 7 XXXXXXXXXXXXXXXXXXXX
154 login
155 line aux 0
156 line vty 0 4
157 access-class 1 in
158 exec-timeout 0 0
159 password 7 XXXXXXXXXXXXXXXXXXXX
160 login local
161 line vty 5 15
162 login local
163 !
164 ntp clock-period 17180241
165 ntp server zzz.zzz.zzz.zzz prefer
166 !
167 webvpn context Default_context
168 ssl authenticate verify all
169 !
170 no inservice
171 !
172 end

```

行番号	説明
38	FE0 I/F(LAN 側)の IP ルーティング可否状態をトラッキングし、オブジェクト ID101 に関連付けます。
44	LAN 側 I/F の基本設定。192.168.100.251/24 のアドレスを割り当て、NAT を行う際の内部と位置づけます。
51	<p>2 つのグループについて HSRP を設定します。</p> <p>HSRP グループ 1 では 1 号機(192.168.100.251)と 2 号機(192.168.100.252)の仮想 IP アドレスを 192.168.100.253 と定義します。また、各ルータのプライオリティを 1 号機:105、2 号機:100(デフォルト)に設定し、192.168.100.253 向けの通信処理を 1 号機が行うことを明示します(通常時)。</p> <p>FE1 I/F(WAN 側)がリンクダウンした場合、1 号機のプライオリティが 10 減ぜられます(デフォルト)。この場合の各ルータのプライオリティは 1 号機:95、2 号機:100 となり、192.168.100.253 向けの通信処理を 2 号機が行うようになります。(障害時のフェイルオーバー)。</p> <p>preempt を明示的に付与することにより、FE1 I/F(WAN 側)がリンクアップした場合、1 号機は元のプライオリティ(105)を再認識し、192.168.100.253 向けの通信処理を 1 号機が行うようになります。(復旧時のフェイルバック)。</p> <p>HSRP グループ 2 では 1 号機(192.168.100.251)と 2 号機(192.168.100.252)の仮想 IP アドレスを 192.168.100.254 と定義します。また、各ルータのプライオリティを 1 号機:100(デフォルト)、2 号機:105 に設定し、192.168.100.254 向けの通信処理は通常 2 号機が行いますが、2 号機の障害時には 1 号機が行うようにします。</p>
59	WAN 側 I/F の基本設定。10.170.80.65/30 のアドレスを割り当て、NAT を行う際の外部として位置づけます。アクセス制御はこの I/F に対して行います(アクセスグループ名:FE1-in)。
91	スイッチポートを VLAN グループ 1 として定義し、管理側 I/F の基本設定として 172.16.200.251/16 を割り当てます。
94	EIGRP の AS 番号 1、広報するネットワークとして 10.170.80.64/30 を設定します。 ルータの持つ静的経路も広報しますが、ルートマップ名 Match-D-Route によりマッチするネットワークのみ広報の対象とします。
100	<p>静的経路を設定します。 10.170.80.0/28 の経路は WAN 側 I/F がリンクダウンした場合に経路表から削除されます(行番号 38 にて設定したインタフェース・トラッキング機構による)。</p> <p>また、EIGRP の経路情報が取得できなくなった場合にはフローティングスタティックルートが機能します。 EIGRP の経路情報を取得可能な場合は、10.170.85.0/24、10.190.140.128/27、10.190.141.0/26 宛の通信を 2 号機へ転送する経路情報は使用されません。</p>

行番号	説明
	これは AD 値(Administrative Distance)が 250 と EIGRP よりも高く設定されているためで、EIGRP の経路情報が取得不可能になると上述の静的経路が浮かび上がります。
110	1 対 1 の静的 NAT を行います。
115	10.170.80.0/28 にマッチするネットワークのみを EIGRP により広報するため標準 ACL を定義します。 行番号 94、143 も参照してください。
119	WAN 側 I/F に対してアクセス制御を行います。 拡張 ACL のオプション established は、TCP ヘッダの ACK または RST フラグが 1 のパケットを検出対象とします。このことは TCP において確立した通信の戻りを表しています。
133	SNMP の各種設定を行います。 SNMP Generic トラップ各種、enterprise トラップ(HSRP、EIGRP、環境モニタの状態変化、syslog 通知)を SNMP マネージャへ発報します。
143	ルートマップ名 Match-D-Route、および標準 ACL 名 D-Route-ACL と関連付け、マッチする経路のみ広報します。

3.2. 2 号機の 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マーキングしていますので、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。1 号機と同様のコンフィグレーションについては説明を省略しています。

```

1  !
2  !
3  !
4  !
5  version 12.4
6  service timestamps debug datetime msec
7  service timestamps log datetime msec
8  service password-encryption
9  !
10 hostname router02
11 !
12 boot-start-marker
13 boot-end-marker
14 !
15 logging buffered 4096 debugging
16 logging console informational
17 enable secret 5 YYYYYYYYYYYYYYYYYYYYYYYYYYYY
18 !
19 no aaa new-model
20 !
21 resource policy
22 !
23 clock timezone JST 9
24 !
25 !
26 ip cef
27 !
28 !
29 no ip domain lookup
30 ip domain name mng.local
31 ip ssh time-out 60
32 ip ssh authentication-retries 2
33 ip ssh rsa keypair-name YYYYYYYYYYYY
34 ip ssh version 2
35 !
36 !
37 !
38 username admin password 7 YYYYYYYYYYYYYYYY
39 !
40 !
41 !
42 track 101 interface FastEthernet0 ip routing
43 !
44 !
45 !
46 !
47 !
48 interface FastEthernet0

```

```
49 ip address 192.168.100.252 255.255.0.0
50 ip nat inside
51 ip virtual-reassembly
52 duplex auto
53 speed auto
54 no cdp enable
55 standby 1 ip 192.168.100.253
56 standby 1 preempt
57 standby 1 track FastEthernet1
58 standby 2 ip 192.168.100.254
59 standby 2 priority 105
60 standby 2 preempt
61 standby 2 track FastEthernet1
62 !
63 interface FastEthernet1
64 bandwidth 512
65 ip address 10.170.80.69 255.255.255.252
66 ip access-group FE1-in in
67 ip nat outside
68 ip virtual-reassembly
69 speed 10
70 full-duplex
71 traffic-shape rate 512000 12800 12800 1000
72 no cdp enable
73 !
74 interface BRI0
75 no ip address
76 encapsulation hdlc
77 shutdown
78 !
79 interface FastEthernet2
80 !
81 interface FastEthernet3
82 !
83 interface FastEthernet4
84 !
85 interface FastEthernet5
86 !
87 interface FastEthernet6
88 !
89 interface FastEthernet7
90 !
91 interface FastEthernet8
92 !
93 interface FastEthernet9
94 !
95 interface Vlan1
96 ip address 172.16.200.252 255.255.0.0
97 !
98 router eigrp 2
99 redistribute static route-map Match-D-Route
100 network 10.17.80.68 0.0.0.3
101 default-metric 512 2000 255 1 1500
102 no auto-summary
103 !
104 ip route 10.170.80.0 255.255.255.240 FastEthernet1 track 101
105 ip route 172.16.200.0 255.255.255.0 172.16.200.254
106 ip route 10.170.85.0 255.255.255.0 192.168.100.253 250
107 ip route 10.190.3.0 255.255.255.0 192.168.100.253 250
108 !
109 !
110 !
111 no ip http server
112 no ip http secure-server
113 ip nat inside source static 192.168.100.1 10.170.80.1
114 ip nat inside source static 192.168.100.2 10.170.80.2
115 ip nat inside source static 192.168.100.3 10.170.80.3
116 !
117 !
118 ip access-list standard D-Route-ACL
119 permit 130.171.84.0 0.0.0.15
120 deny any
121 !
122 ip access-list extended FE1-in
123 permit icmp any any
124 permit eigrp any any
125 permit tcp 10.170.85.0 0.0.0.255 10.170.80.0 0.0.0.255 eq 443
126 permit tcp 10.170.85.0 0.0.0.255 eq 443 10.170.80.0 0.0.0.255 established
127 permit tcp 10.190.3.0 0.0.0.255 10.170.80.0 0.0.0.15 eq ftp
128 permit tcp 10.190.3.0 0.0.0.255 10.170.80.0 0.0.0.15 eq ftp-data established
129 permit tcp 10.190.3.0 0.0.0.255 eq ftp 10.170.80.0 0.0.0.15 established
130 permit tcp 10.190.3.0 0.0.0.255 eq ftp-data 10.170.80.0 0.0.0.15
```

```

131 permit tcp 10.190.141.0 0.0.0.63 10.170.80.0 0.0.0.15 eq 443
132 !
133 logging history informational
134 snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
135 snmp-server enable traps eigrp
136 snmp-server enable traps envmon
137 snmp-server enable traps hsrp
138 snmp-server enable traps syslog
139 snmp-server host ZZZ.ZZZ.ZZZ.ZZZ tbox eigrp envmon hsrp syslog snmp
140 !
141 !
142 !
143 !
144 route-map Match-D-Route permit 10
145 match ip address D-Route-ACL
146 !
147 !
148 !
149 !
150 control-plane
151 !
152 !
153 line con 0
154 exec-timeout 0 0
155 password 7 YYYYYYYYYYYYYYYYYY
156 login
157 line aux 0
158 line vty 0 4
159 exec-timeout 0 0
160 password 7 YYYYYYYYYYYYYYYYYY
161 login local
162 transport input none
163 line vty 5 15
164 login local
165 !
166 ntp clock-period 17180292
167 ntp server zzz.zzz.zzz.zzz prefer
168 !
169 webvpn context Default_context
170 ssl authenticate verify all
171 !
172 no inservice
173 !
174 end

```

行番号	説明
48	LAN 側 I/F の基本設定。192.168.100.252/16 のアドレスを割り当て、NAT を行う際の内部と位置づけます。
55	<p>2 つのグループについて HSRP を設定します。</p> <p>HSRP グループ 1 では 1 号機(192.168.100.251)と 2 号機(192.168.100.252)の仮想 IP アドレスを 192.168.100.253 と定義します。また、各ルータのプライオリティを 1 号機:105、2 号機:100(デフォルト)に設定し、192.168.100.253 向けの通信処理は通常 1 号機が行いますが、1 号機の障害時には 2 号機が行うようにします。</p> <p>HSRP グループ 2 では 1 号機(192.168.100.251)と 2 号機(192.168.100.251)の仮想 IP アドレスを 192.168.100.254 と定義します。また、各ルータのプライオリティを 1 号機:100(デフォルト)、2 号機:105 に設定し、192.168.100.254 向けの通信処理を 2 号機が行うことを明示します(通常時)。</p> <p>FE1 I/F(WAN 側)がリンクダウンした場合、2 号機のプライオリティが 10 減ぜられます(デフォルト)。この場合の各ルータのプライオリティは 1 号機:100、2 号機:95 となり、192.168.100.254 向けの通信処理を 1 号機が行うようになります。(障害時のフェイルオーバー)。</p> <p>preempt を明示的に付与することにより、FE1 I/F(WAN 側)がリンクアップした場合、2 号機は元のプライオリティ(105)を再認識し、192.168.100.254 向けの通信処理を 2 号機が行うようになります。(復旧時のフェイルバック)。</p>
63	WAN 側 I/F の基本設定。10.170.80.69/30 のアドレスを割り当て、NAT を行う際の外部として位置づけます。アクセス制御はこの I/F に対して行います(アクセスグループ名:FE1-in)。
95	スイッチポートを VLAN グループ 1 として定義し、管理側 I/F の基本設定として 172.16.200.252/16 を割り当

行番号	説明
	てます。
98	EIGRP の AS 番号 2、広報するネットワークとして 10.170.80.68/30 を設定します。 ルータの持つ静的経路も広報しますが、ルートマップ名 Match-D-Route によりマッチするネットワークのみ広報の対象とします。
104	静的経路を設定します。 10.170.80.0/28 の経路は WAN 側 I/F がリンクダウンした場合に経路表から削除されます(行番号 42 にて設定したインタフェース・トラッキング機構による)。 また、EIGRP の経路情報が取得できなくなった場合にはフローティングスタティックルートが機能します。 EIGRP の経路情報を取得可能な場合は、10.170.85.0/24、10.190.3.0/24 宛の通信を 1 号機へ転送する経路情報は使用されません。 これは AD 値(Administrative Distance)が 250 と EIGRP よりも高く設定されているためで、EIGRP の経路情報が取得不可能になると上述の静的経路が浮かび上がります。

3.3. サーバ上の静的経路

管理拠点から対向拠点へパケットが向う場合、サーバから管理拠点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。

サーバ名	IP アドレス	追加経路	ゲートウェイ
aaa.mng.local	192.168.100.1	10.170.0.0/16 10.190.141.0/26 10.190.140.128/27	192.168.100.253
bbb.mng.local	192.168.100.2	10.170.0.0/16	192.168.100.254
ccc.mng.local	192.168.100.3	10.190.3.0/24	192.168.100.254

下記のように経路を設定します。上表より *add-network*、*network's mask*、*gateway* を適宜読替えてください。

```
# route add -net add-network mask network's mask gateway metric 1
```

恒久的な設定とするために/etc/sysconfig/network-scripts/route-eth*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-eth*
...
add-network via gateway metric 1
...
```

4. ルータ保守

4.1. ログイン方法

前述のとおり、ルータには複数の IP アドレスが下表のように割り当てられています。

ルータ名	LAN 側 IP	WAN 側 IP	HSRP 用仮想 IP	管理用 IP
router01	192.168.100.251/24	10.170.80.65/30	192.168.100.253/24	172.16.200.251/24
router02	192.168.100.252/24	10.170.80.69/30	192.168.100.254/24	172.16.200.252/24

ルータを保守する際には、**管理用 IP アドレス**でログインします。直接ログインできない場合には、IP 到達性のあるサーバ等を踏み台にして telnet してください。

```
$ telnet 172.16.200.251
Trying 172.16.200.251...
Connected to 172.16.200.251 (172.16.200.251).
Escape character is '^]'.

User Access Verification

Username: admin
Password: login passwd
router01>enable
Password: enable passwd
router01#
```

4.2. ログの表示

ルータが収集しているログを表示させるには下記のコマンドを実行します。

```
router01#show logging
Syslog logging: enabled (1 messages dropped, 1 messages rate-limited,
0 flushes, 0 overruns, xml disabled, filtering disabled)
  Console logging: level debugging, 148 messages logged, xml disabled,
    filtering disabled
  Monitor logging: level debugging, 0 messages logged, xml disabled,
    filtering disabled
  Buffer logging: level debugging, 148 messages logged, xml disabled,
    filtering disabled
Logging Exception size (4096 bytes)
Count and timestamp logging messages: disabled

No active filter modules.

ESM: 0 messages dropped

  Trap logging: level informational, 151 message lines logged

Log Buffer (4096 bytes):
322: %HSRP-6-STATECHANGE: FastEthernet0 Grp 1 state Speak -> Standby
*Oct 17 05:39:40.322: %HSRP-6-STATECHANGE: FastEthernet0 Grp 1 state Standby -> Active
...
*Oct 20 14:46:22.485: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.170.80.66
(FastEthernet1) is up: new adjacency
*Nov 5 02:37:57.225: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.170.80.66
(FastEthernet1) is down: holding time expired
*Nov 5 07:21:00.541: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.170.80.66
(FastEthernet1) is up: new adjacency
...
```

EIGRP の経路変更や機器異常、その他 I/F の linkUp/linkDown 等もログとして出力されます。

4.3. HSRP の状態確認

HSRP の状態を確認するには下記のコマンドを実行します。

```
router01#show standby
FastEthernet0 - Group 1
  State is Active
    18 state changes, last state change 18w6d
  Virtual IP address is 192.168.100.253
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.860 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.100.252, priority 100 (expires in 9.132 sec)
  Priority 105 (configured 105)
    Track interface FastEthernet1 state Up decrement 10
  IP redundancy name is "hsrp-Fa0-1" (default)
FastEthernet0 - Group 2
  State is Standby
    23 state changes, last state change 18w6d
  Virtual IP address is 192.168.100.254
  Active virtual MAC address is 0000.0c07.ac02
    Local virtual MAC address is 0000.0c07.ac02 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.856 secs
  Preemption enabled
  Active router is 192.168.100.252, priority 105 (expires in 9.128 sec)
  Standby router is local
  Priority 100 (default 100)
    Track interface FastEthernet1 state Up decrement 10
  IP redundancy name is "hsrp-Fa0-2" (default)
router01#
```

4.4. トラッキングの状態確認

インタフェース・トラッキングの状態を確認するには下記のコマンドを実行します。

```
router01#show track
Track 1 (via HSRP)
  Interface FastEthernet1 line-protocol
  Line protocol is Up
    9 changes, last change 19w1d
  Tracked by:
    HSRP FastEthernet0 1
    HSRP FastEthernet0 2
Track 101
  Interface FastEthernet0 ip routing
  IP routing is Up
    8 changes, last change 18w6d
  Tracked by:
    STATIC-IP-ROUTING 0
router01#
```

4.5. インタフェースの状態確認

FE0、FE1 等の I/F の状態を確認するには下記のコマンドを実行します。

```
router01#show interfaces fastEthernet 1
FastEthernet1 is up, line protocol is up
Hardware is PQ3 TSEC, address is 001b.d49d.c2c7 (bia 001b.d49d.c2c7)
Internet address is 10.170.80.65/30
MTU 1500 bytes, BW 512 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 10Mb/s, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:03, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 1000 bits/sec, 1 packets/sec
5 minute output rate 1000 bits/sec, 1 packets/sec
 12572788 packets input, 1436448854 bytes
   Received 2400863 broadcasts, 0 runts, 0 giants, 0 throttles
  1 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 watchdog
  0 input packets with dribble condition detected
13948385 packets output, 3392793567 bytes, 0 underruns
  0 output errors, 0 collisions, 4 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier
  0 output buffer failures, 0 output buffers swapped out
router01#
```

4.6. 経路の状態確認

経路表の内容を確認するには下記のコマンドを実行します。

```
router01# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, 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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 172.16.254.254 to network 0.0.0.0

C    192.168.100.0/ is directly connected, FastEthernet0
    10.170.0.0/16 is variably subnetted, 3 subnets, 3 masks
C    10.170.80.64/30 is directly connected, FastEthernet1
D EX 10.170.85.0/24 [170/5537536] via 10.170.80.66, 7w0d, FastEthernet1
S    10.170.80.0/28 is directly connected, FastEthernet1
C    172.16.200.0/24 is directly connected, Vlan1
S    172.16.200.0/24 [1/0] via 172.16.200.254
router01#
```

Codes が **D EX** の経路は、対向拠点より EIGRP で広報された経路となります。

4.7. SW、HW の状態確認

テクニカルサポートが必要とするあらゆる情報を採取します。

```
router01# show tech-support
```

5. 添付資料

5.1. フラッシュ IOS の復旧

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.T7.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 (fcl)
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
...
...
```

EIGRP/HSRP settings by Cisco router

改版履歴

Version 0.1	2008/12/21	新規作成。
Version 0.2	2009/02/09	「1.1. はじめに」を修正。

製作

LA TIGRE

本書は 2008 年 12 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。