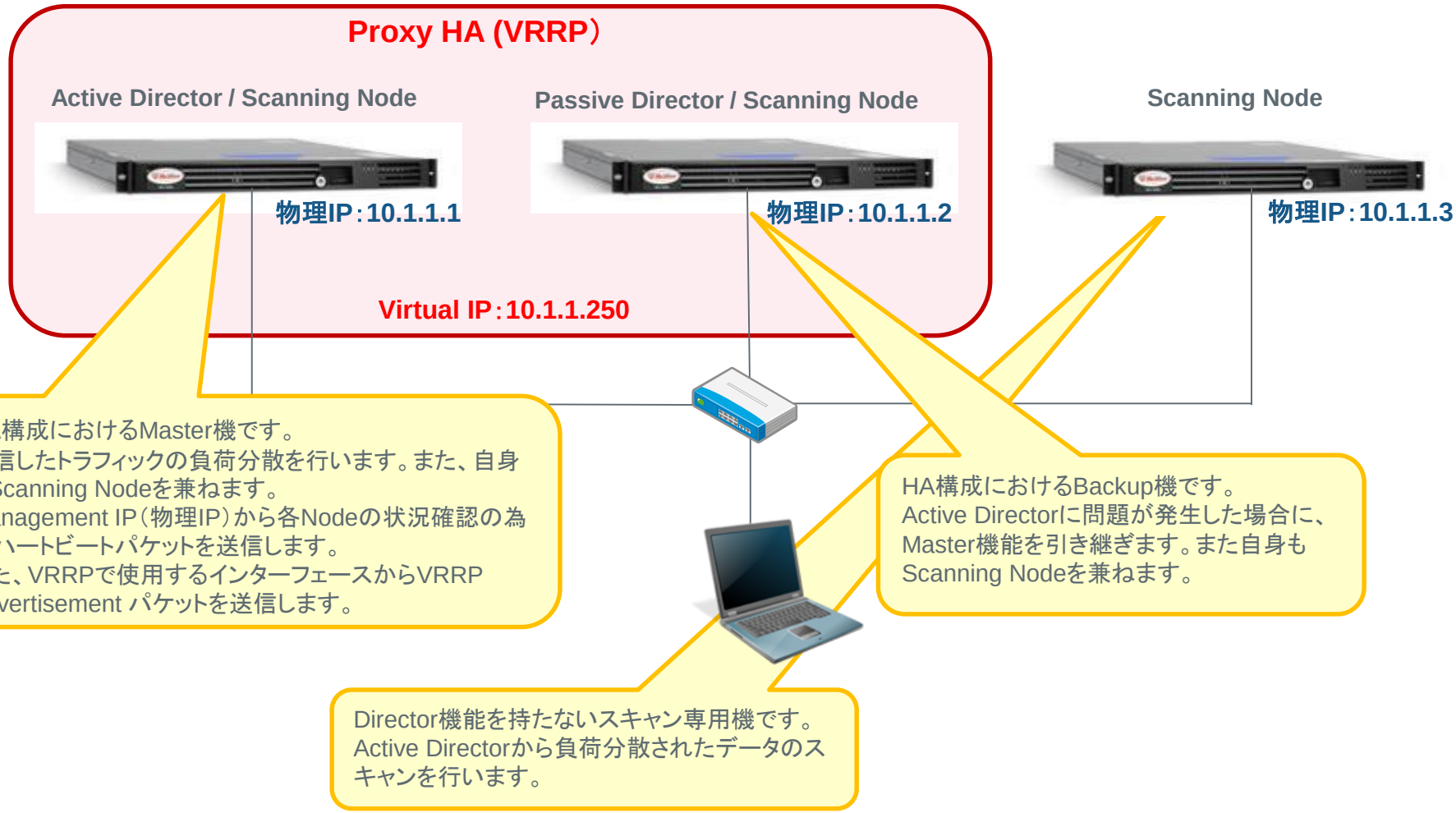
McAfee Web Gateway 7.x
Proxy HA 概要

Support & Service 統括本部
Contents Security Support

December 27, 2016

Proxy HA 構成概要



Proxy HA 構成について①

- McAfee Web Gatewayでは冗長機能を持ったProxy構成（Proxy HA）を組むことができます。

- 各Director ノード間でActive-Passive型のFailoverを行います。

- Directorノードは必ず一つだけがActive Directorとなり、同時に2つ以上のノードがActiveになることはありません。
  ※Active-Active型のHA構成は組めません。

- VRRPによりネットワークの冗長性を確保します。
  ※Transparent　Routerも同様です。

- ActiveなDirectorノードが停止した場合、他に使用可能なDirectorが存在する場合は、そのノードがVirtual　IPを引き継ぎ、トラフィックを処理するようになります。

Proxy HA 構成について②

- 停止したDirectorが復旧した場合は、そのDirectorが再びActive Directorとなります。

- 各ノードでPriorityを同じに設定している場合は、Network上に最初にあらわれたノードがActive Directorとなります。

- スキャン処理の負荷分散はScanning ノード間で行います。
  DirectorノードはScanningノードを兼ねます。

- Active DirectorはVirtual IPアドレスに送信されたトラフィックに対し、クライアントからのトラフィックを受け付けます。
  これを自身(Scanning node)とその他のMWG(Scanning node)にカーネルレベルでリダイレクトすることでロードバランスを実現しています。

Proxy HA 構成について③

- 各Scanningノードの動作状態はActive DirectorのManagement IPから送信するハートビートにより確認します。
  ※Scanningノードは自動的に検出されます。

- ハートビートはプロトコル番号253を使用します。

- トラフィックの分散はハートビートによる動作状態や接続数をベースに独自のアルゴリズムで計算されます。

- Proxy HA構成および設定については下記Q&Aを参照ください。
  http://www.mcafee.com/japan/pqa/aMcAfeeMwg.asp?ancQno=WG12031901&ancProd=McAfeeMwg

Proxy HA 設定項目①

- **設定箇所:**

  [Configuration] - [Appliances] – [Proxies(HTTP(S), FTP,ICAP and IM)]

Network Setup:

Proxy HAを選択します。

Proxy HA:

- Port Redirects:

Proxy portと同じポート番号を以下の項目に設定します。

Original destination port: 9090

Destination proxy port: 9090

※上記はProxy portが9090（Default）の場合の例です。

Proxy HA 設定項目②

- Director Priority:

ノードのプライオリティを入力します。
0を設定した場合は、Scanning Nodeになります。
その場合のScanning Nodeは、Director機能を持ちません。
0より大きい数を設定した場合はDirector Nodeとなります。
複数のDirectorが存在する場合は、より数字の大きいNodeがActive Director として選出されます。
DirectorはScanning Nodeとしても動作します。

- Management IP:

ローカルノードのNICに設定されたIPアドレスを入力します。
このIPアドレスを持つインタフェースからハートビートが送受信されます。

- Virtual IPs:

Proxy HAとして構成する仮想IPアドレスを設定します。
Proxy HAに参加する全てのノードで同じIPにする必要があります。

Proxy HA 設定項目③

- Virtual router id:

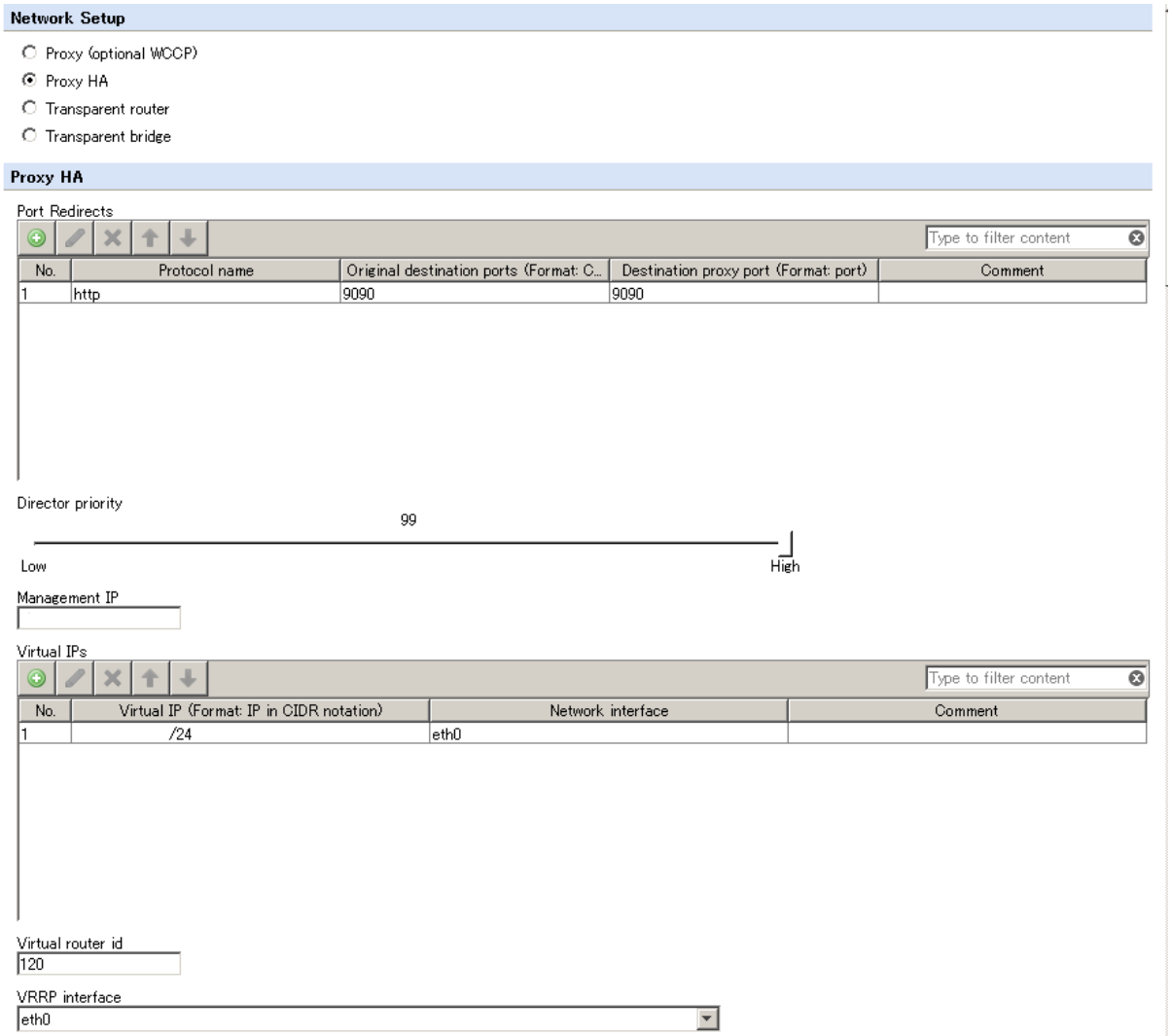
VRRPで利用するVRIDを入力します。全てのノードで同じIDにする必要があります。

- VRRP interface:

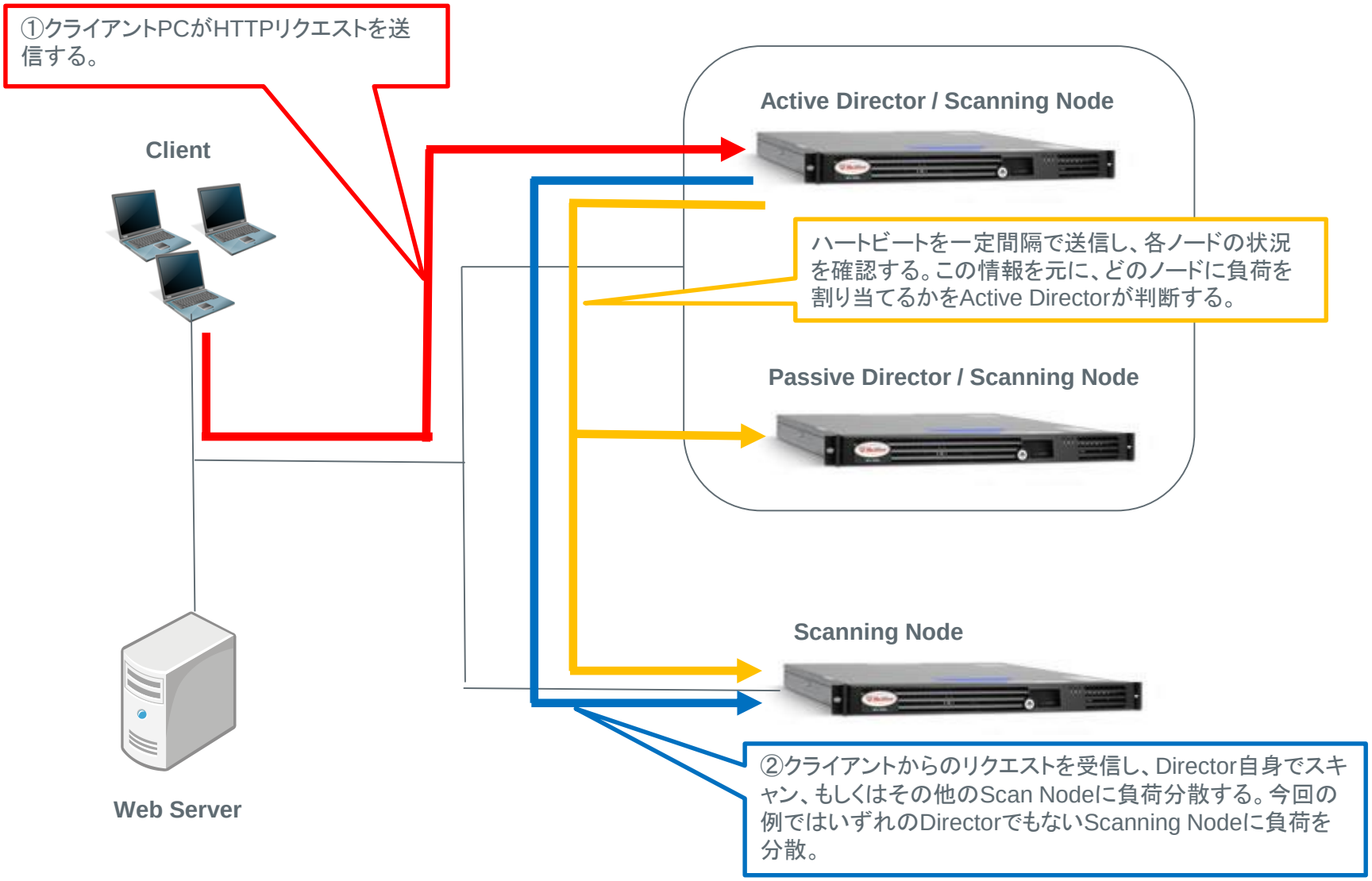
VRRPで利用するインターフェースを設定します。設定されたインターフェースからVRRP Advertisementパケットが送信されます。

Proxy HA 設定項目③

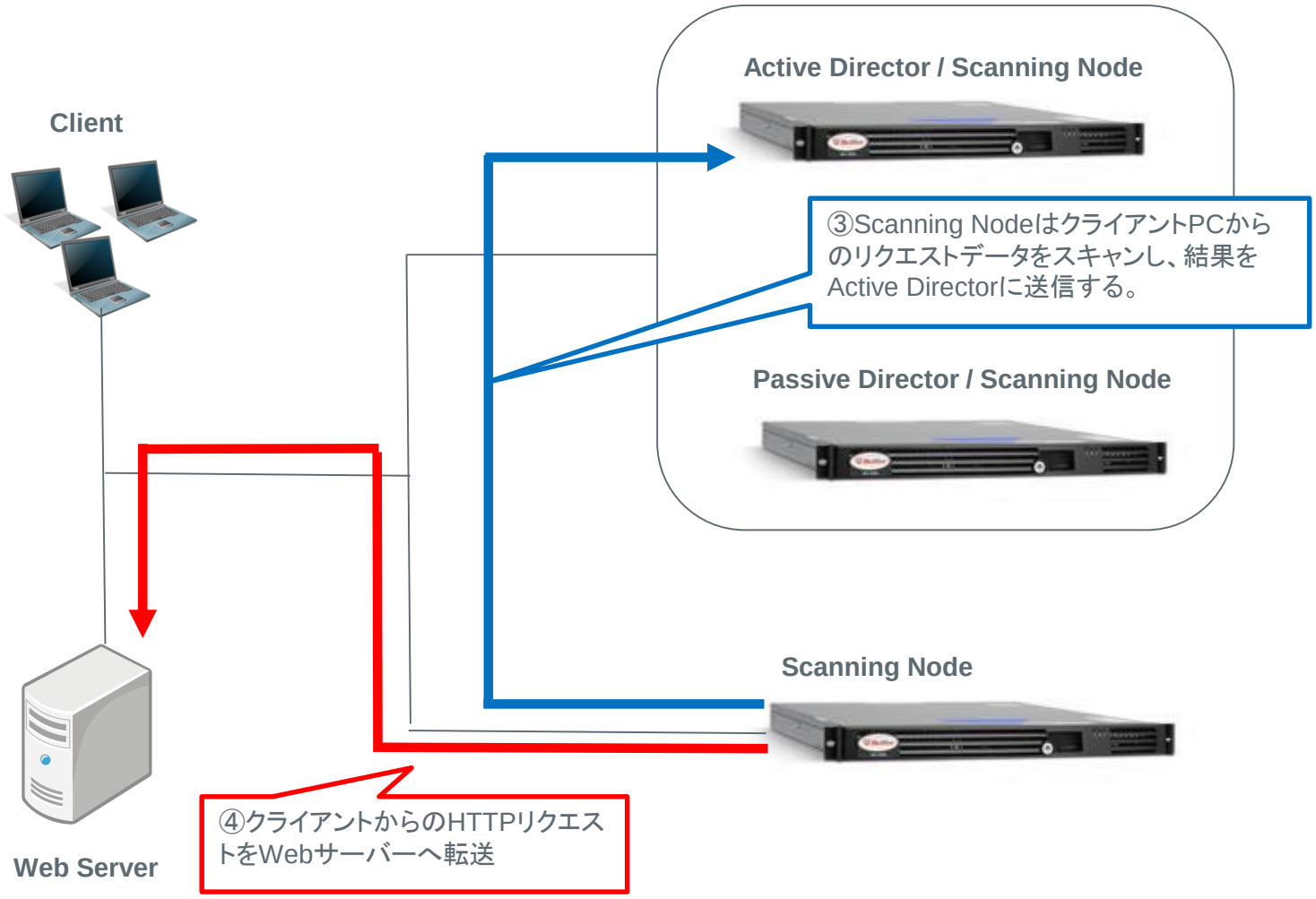
- 設定画面



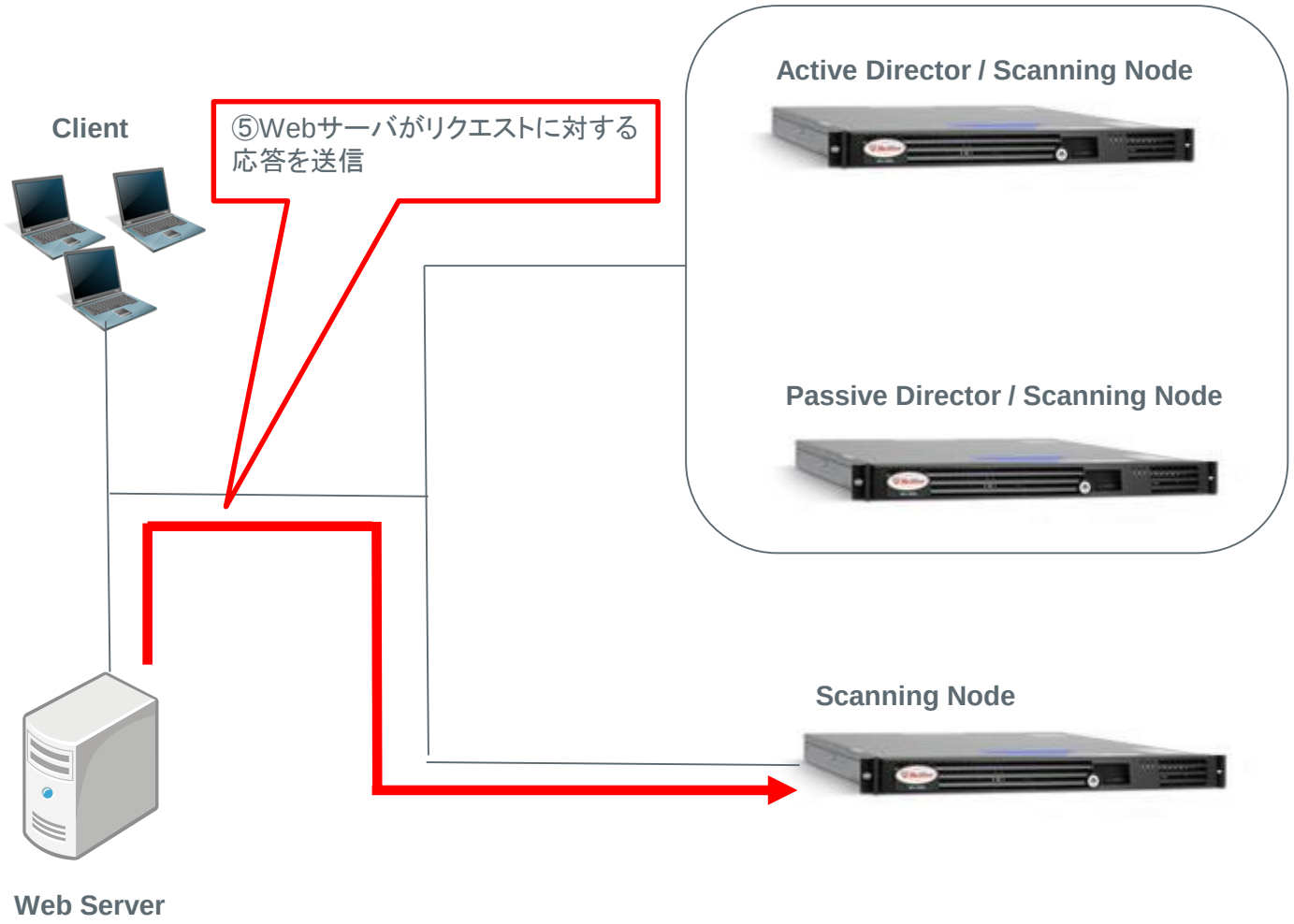
トラフィックフロー① （Request Cycle）



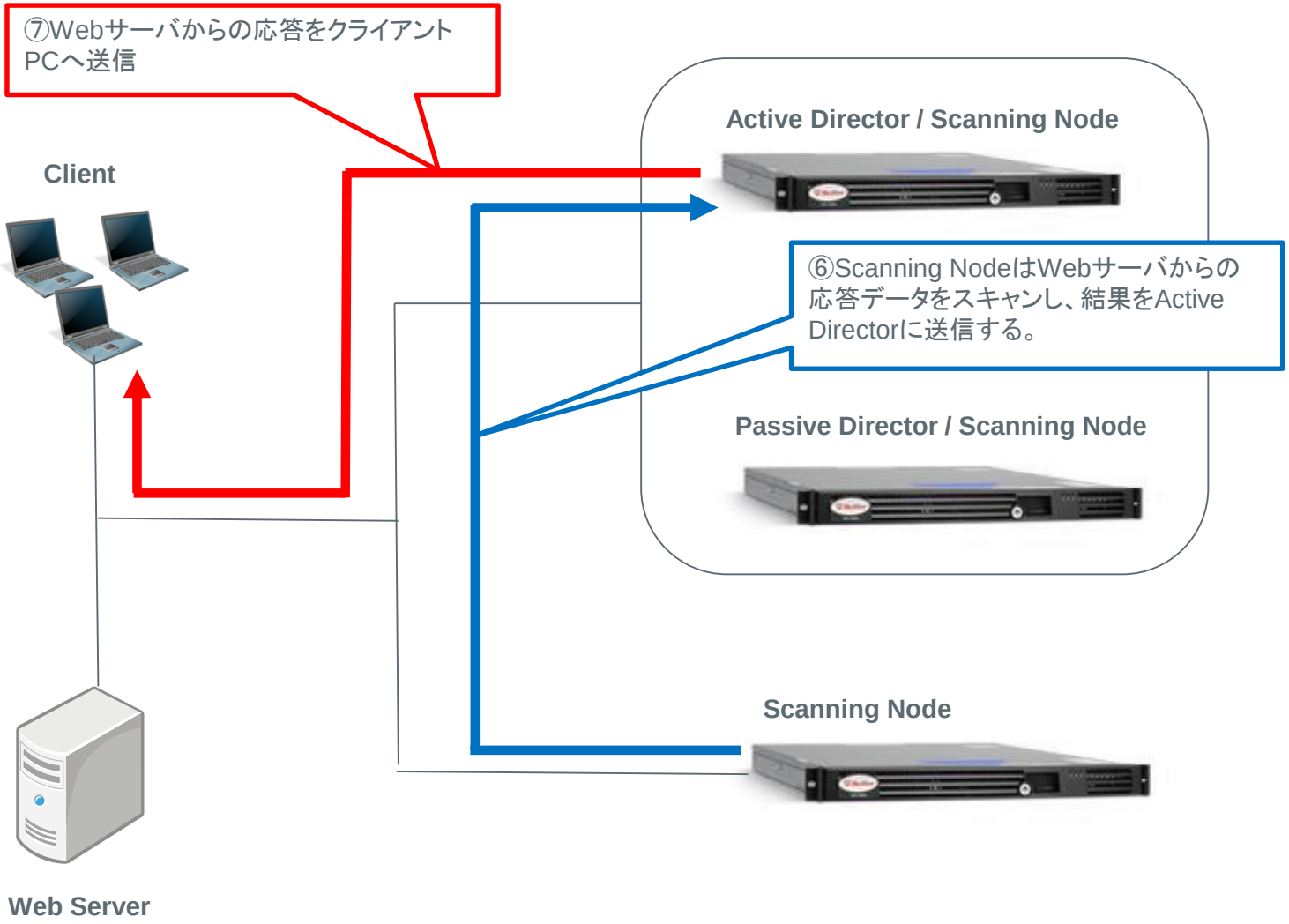
トラフィックフロー② （Request Cycle）



トラフィックフロー③ （Response Cycle）



トラフィックフロー④ （Response Cycle）



VRRPによる冗長　動作①

Virtual Router ID：51
Director Priority：99
物理IPアドレス：10.1.1.1
Virtual IPアドレス：10.1.1.250
Virtual MACアドレス：00:00:5e:00:01:01

①VRRPを設定した2台の機器を起動すると、まず「Initialize」ステータスになる。

Virtual Router ID：51
Director Priority：89
物理IPアドレス：10.1.1.2
Virtual IPアドレス：10.1.1.250
Virtual MACアドレス：00:00:5e:00:01:01

Master (Active Director)

Backup（Passive　Director）

②それぞれの機器がお互いに「VRRP Advertisement」パケットをVRRP用に割り当てられた以下のマルチキャストアドレス宛に送信する。

宛先MACアドレス：01:00:5e:00:00:12
宛先IPアドレス：224.0.0.18

③「VRRP Advertisement」パケットを受信すると、パケットに含まれているPriorityと自身のPriorityを比較する。

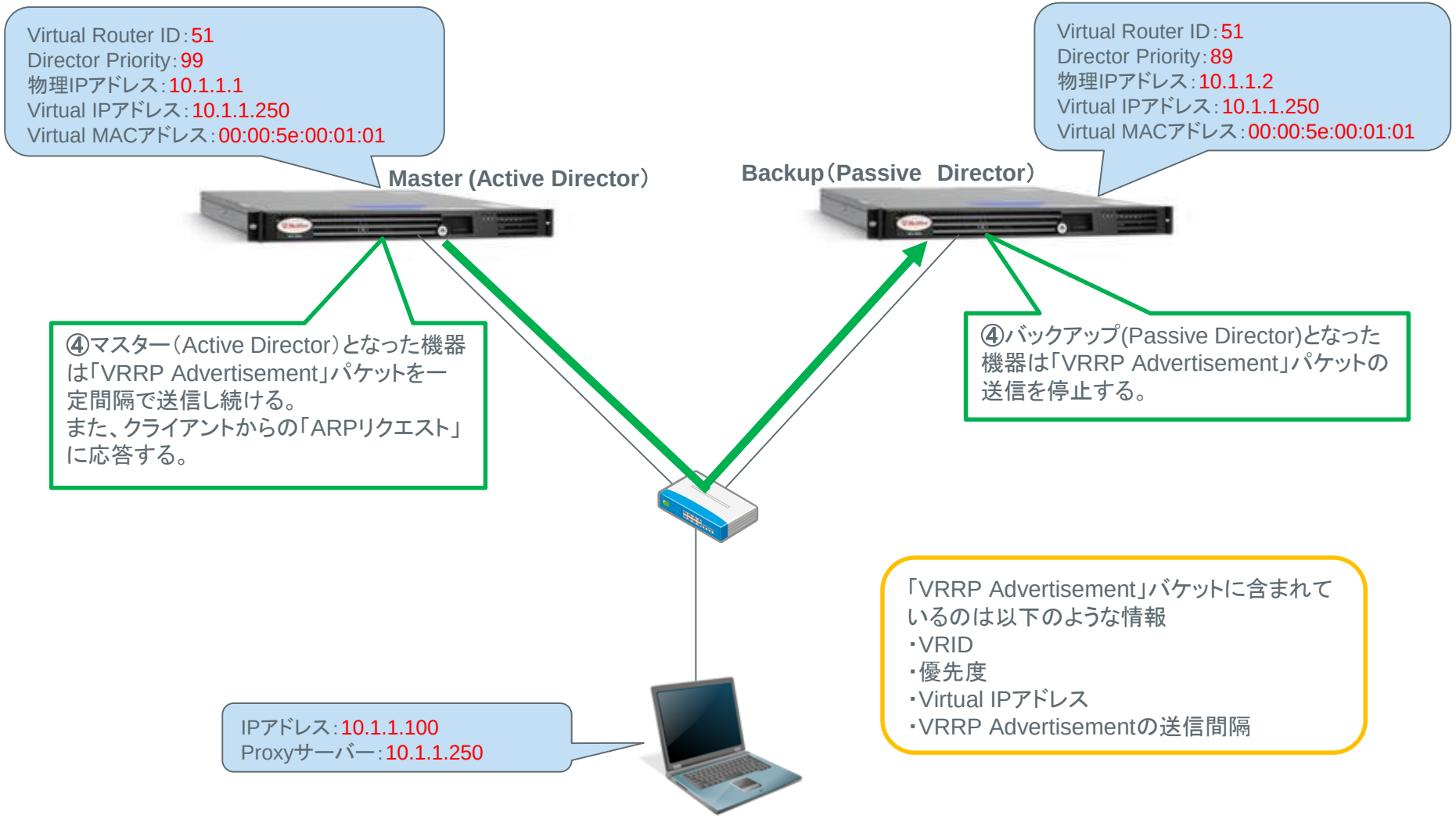
自身のPriorityが小さければバックアップ（Passive Director）となり、「Initialize」から「Backup」に遷移する。

③「VRRP Advertisement」パケットを受信すると、パケットに含まれているPriorityと自身のPriorityを比較する。

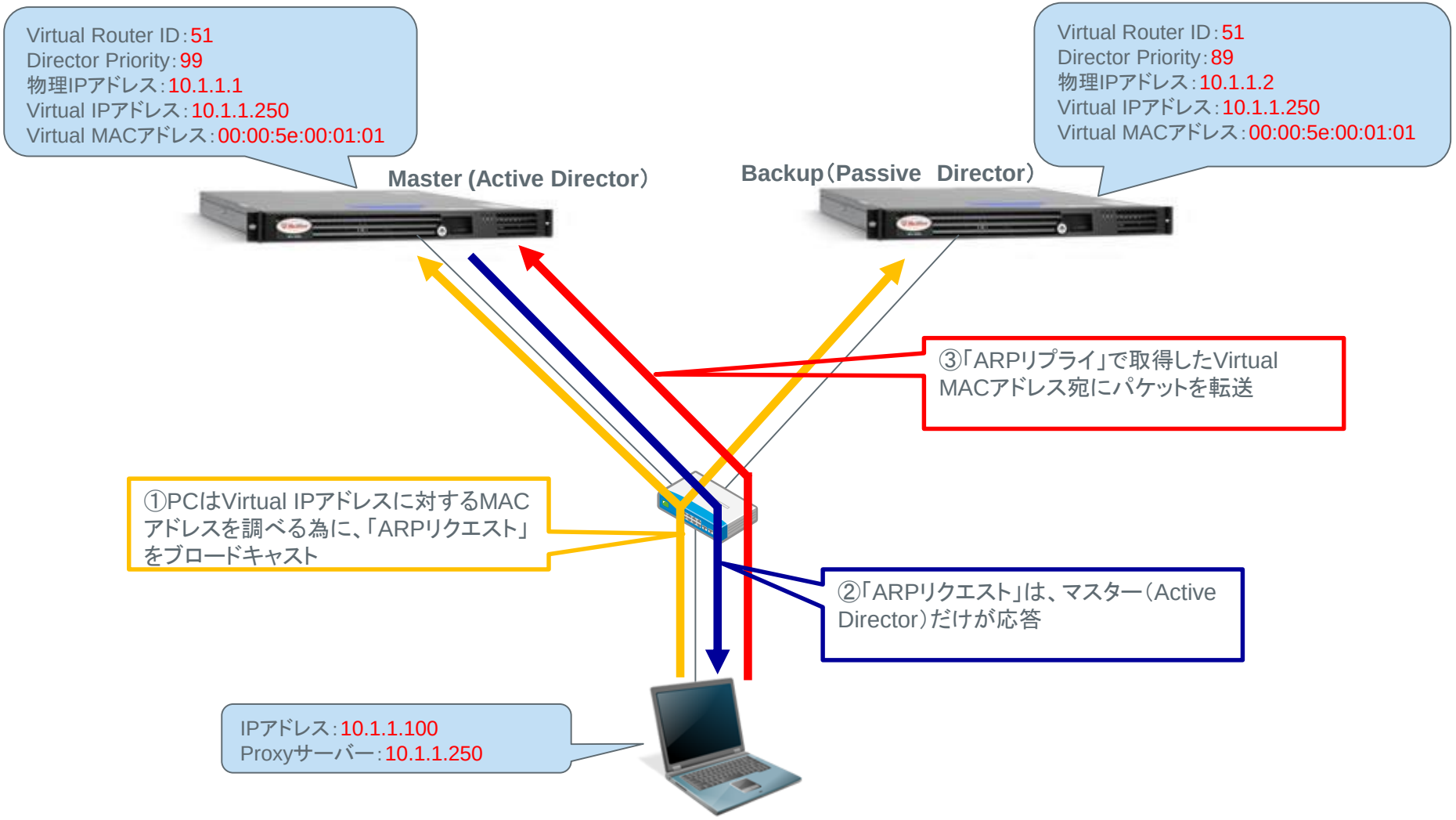
自身のPriorityが大きい場合にはマスター（Active Director）となり、ステータスは「Initialize」から「Master」に遷移する。

IPアドレス：10.1.1.100
Proxyサーバー：10.1.1.250

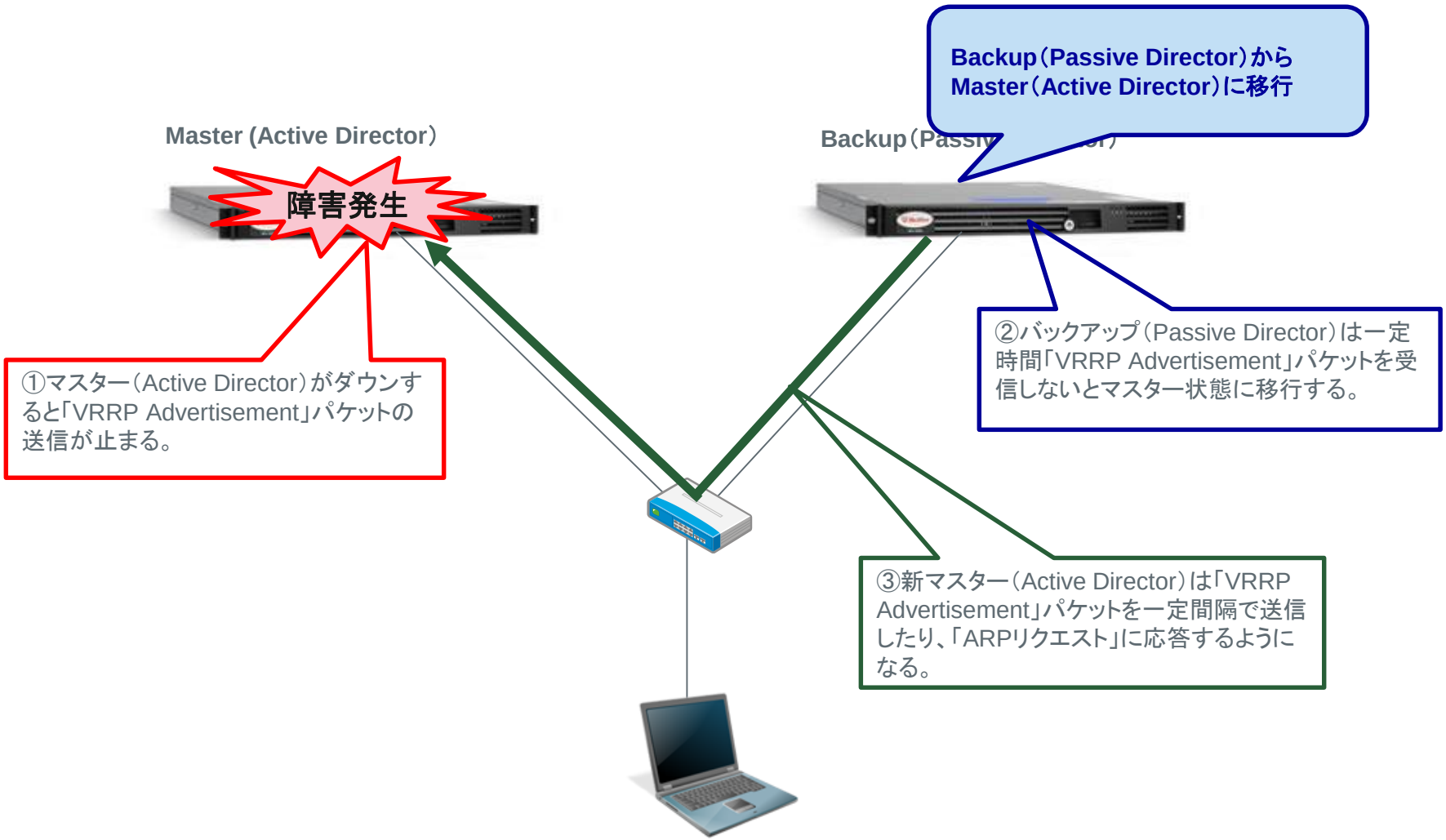
VRRPによる冗長　動作②



VRRPによる冗長　トラフィックフロー



VRRPによる冗長　切り替え



HAステータス確認コマンド①

- **HA状態の確認**

  コマンド：　mfend-lb –s

出力例 （Active Director情報）

```
device: mwgappl01
statechange:
        ip: 10.1.1.1
       ip6: ::
 protocols: 00000001
       mac: b8ac6f1298ff
     state: NETWORK
     stats: 0 0 0 0 0
statusvalid: 1
      type: director
    device: __SELF__
statechange:
        ip: 0.0.0.0
       ip6: ::
 protocols: 00000001
       mac: b8ac6f1298ff
     state: OK
     stats: 0 0 0 0 0
statusvalid: 1
      type: scanning
```

（Passive Director情報）

```
 device: mwgappl02
statechange: 1298958338 (Tue Mar  1 05:45:38 2011)
        ip: 172.16.247.114
       ip6: ::
 protocols: 00000001
       mac: a4badb46efd8
     state: REDUNDANT
     stats: 0 0 0 0 0
statusvalid: 1
      type: redundant
    device: mwgappl02
statechange: 1298958338 (Tue Mar  1 05:45:38 2011)
        ip: 172.16.247.114
       ip6: ::
 protocols: 00000001
       mac: a4badb46efd8
     state: OK
     stats: 0 0 0 0 0
statusvalid: 1
      type: scanning
```

HAステータス確認コマンド②

- **scanning動作の確認**

  コマンド： mwg-mon -c

出力例

current state: ok
port 9090 reachable

- **VRRPの到達確認**

  コマンド： tcpdump -np vrrp

出力例

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
05:50:39.119772 IP 172.16.247.113 > 224.0.0.18: VRRPv2, Advertisement, vrid 40, prio 60, authtype none, intvl 1s, length 20

注意点

- 同一セグメント上に、複数の異なる Proxy HA構成を設定する場合には、ロードバランスの重複が発生するため **/etc/sysconfig/mfend** ファイルに、それぞれのロードバランスのID（MFE_LBID）をユニークな値で設定し、それぞれが異なるグループであることを明確に設定してください。

  例: 同一セグメントに 4台のアプライアンスでA, B 二つのProxy HAグループを構築したい場合
  <サーバー1/2（グループA）のetc/sysconfig/mfend 末尾に以下を追加する>
  ### END AUTO GENERATED CONFIG
  MFEND_LBID=10

  <サーバー3/4（グループB）のetc/sysconfig/mfend 末尾に以下を追加する>
  ### END AUTO GENERATED CONFIG
  MFEND_LBID=20

  上記を設定後、各アプライアンスを再起動します。
  ※値はバックアップ/リストアによる保存、復元が行われません。
  　機器交換、アップグレードの後には必ずご確認ください。
- VRRPの重複が発生するため VRID をグループごとにそれぞれ異なるユニークな値に設定してください。


McAfee®
An Intel Company