YAMAHA

感 動 を ・ と も に ・ 創 る

イーサアクセスVPNルーター RTXシリーズ ～開発コンセプト～

2002年12月3日

ヤマハ株式会社
AV・IT事業本部　マーケティング室
平野 尚志 (mya@comm.yamaha.co.jp)

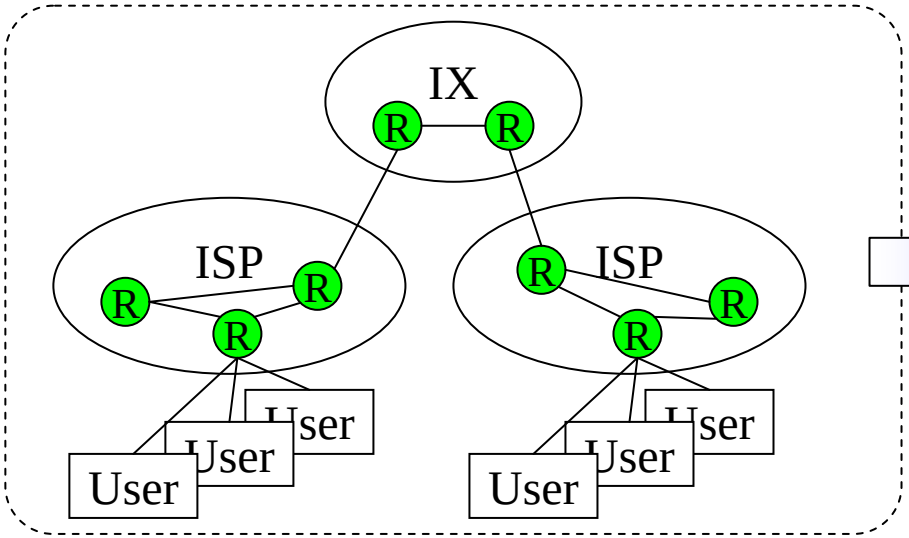
概要

○ルーターとは？
○ヤマハルーター
○RTXシリーズ～開発コンセプト～

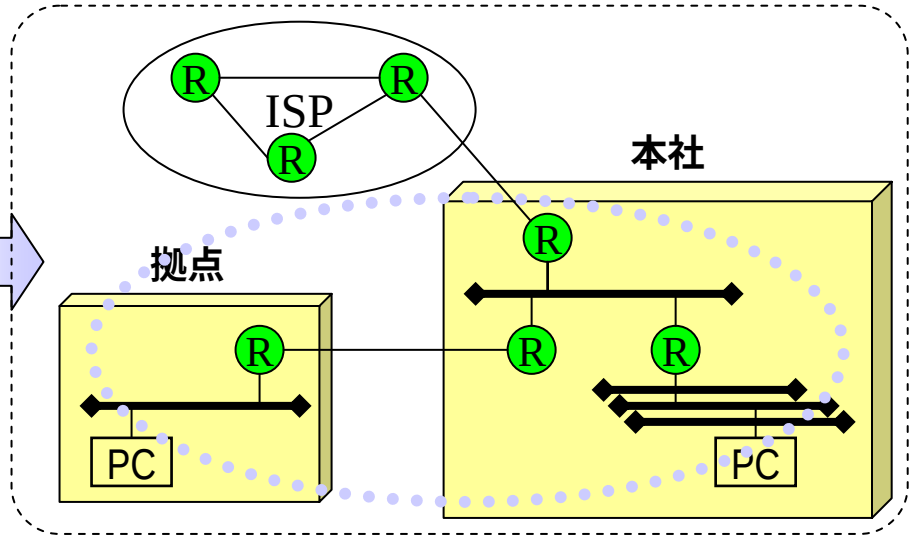
[付録資料]
・フィルタ型ルーティング
・VPN
・ネットボランチのトピックス
・ネットボランチの利用環境と実験環境
・ファイアウォール機能

ルーター？

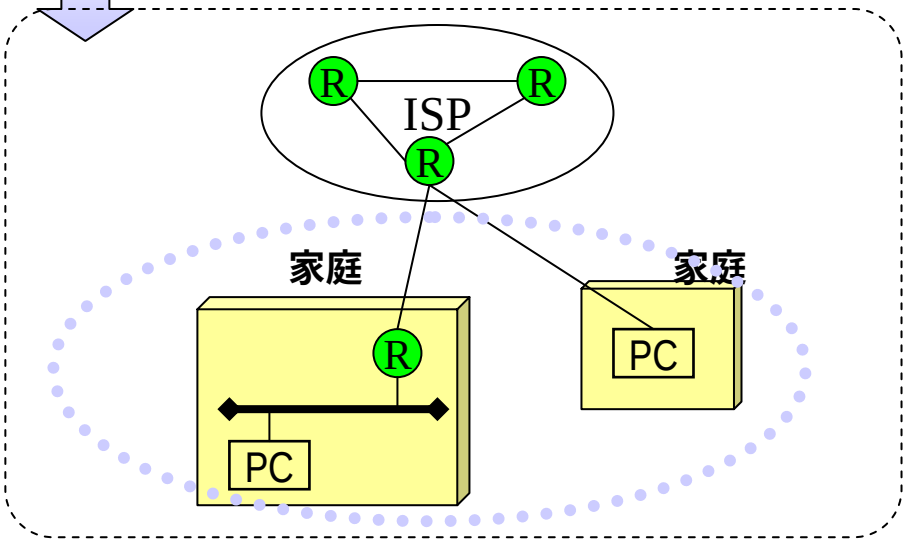
ルーターとは？



インターネットのIP通信の中継



企業の内外とのIP通信の中継



家庭などの内外とのIP通信の中継

[ルーターとは？]

・IP通信を中継する機器

・インターネット(IP網)は、ルーターを繋いで構成されている。

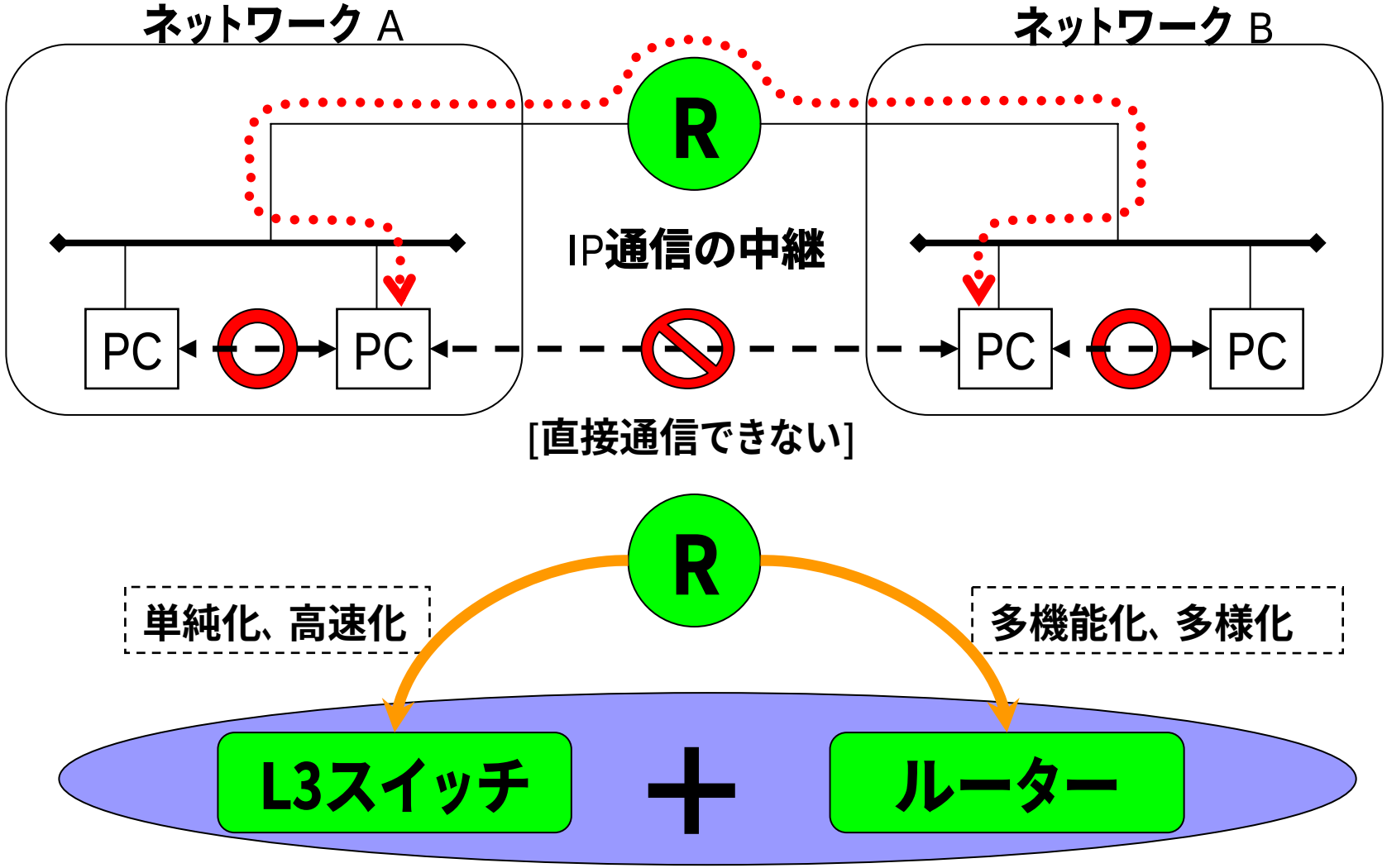
IX: Internet eXchange

JPIX→http://www.jpix.ad.jp/

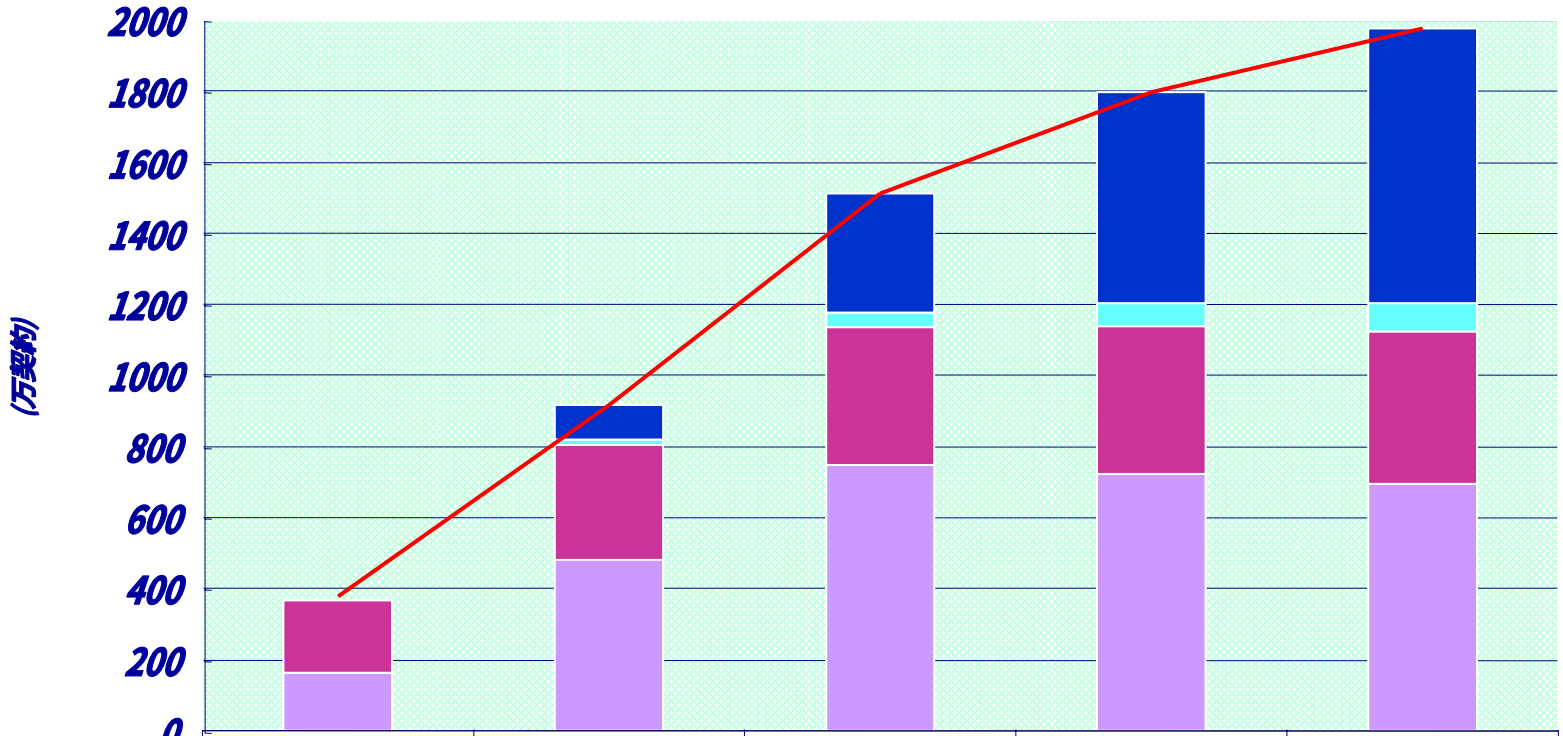
ISP: Internet Service Provider

®: Router

ルーターとは？



高速インターネット普及予測

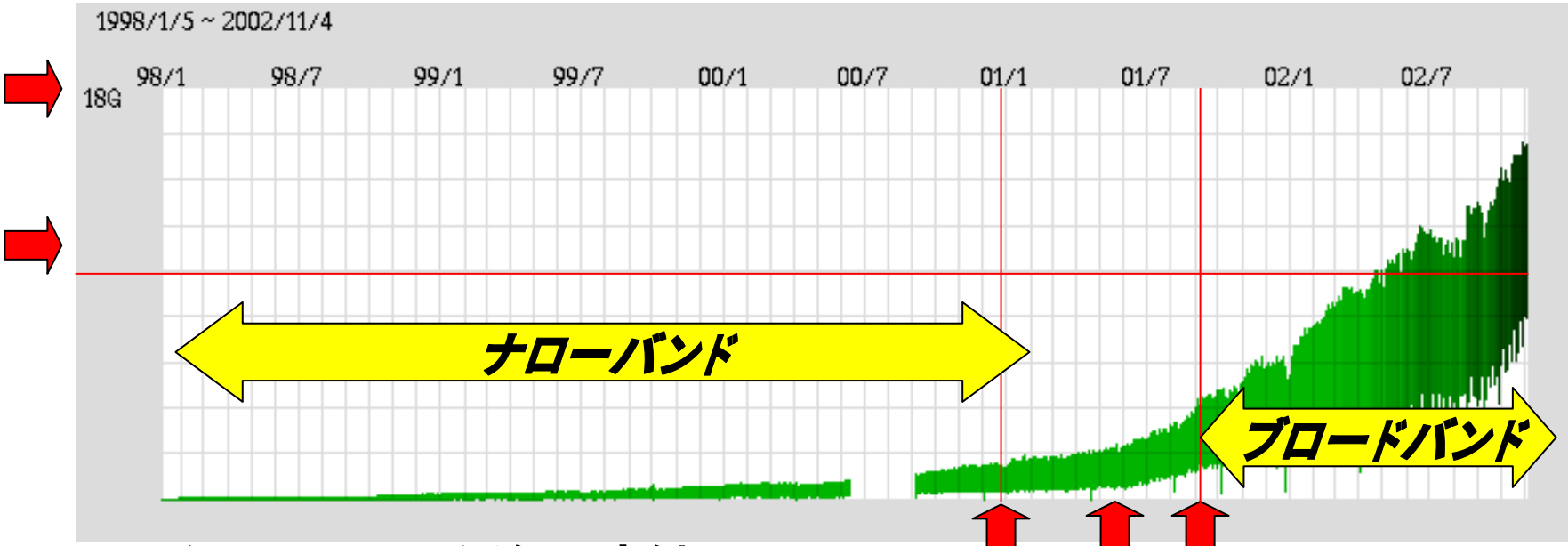


	2001年	2002年	2003年	2004年	2005年
FTTx	7	97	335	593	773
無線	2	16	41	65	80
CATV	205	323	388	417	429
DSL	164	481	749	722	695
TOTAL	378	917	1513	1797	1977

(総務省・ブロードバンド構想　2001/10/16)

IXの状況

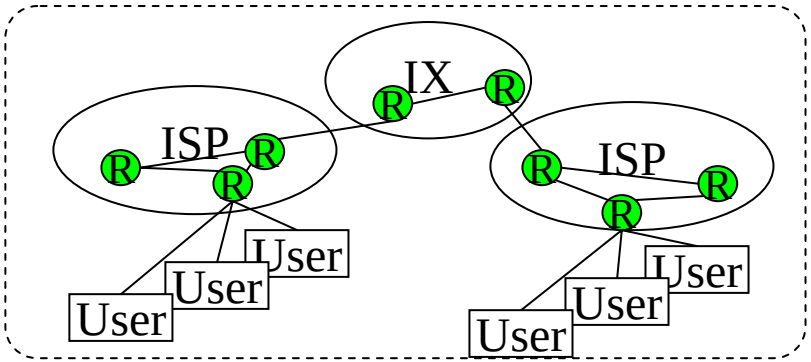
(JPIXのバックボーントラフィック→http://www.jpix.ad.jp/jp/techncal/traffic.html)



フレッツADSL 1.5M

各社ADSL 8M

インターネットのIP通信の中継



IX: Internet eXchange

JPIX→http://www.jpix.ad.jp/

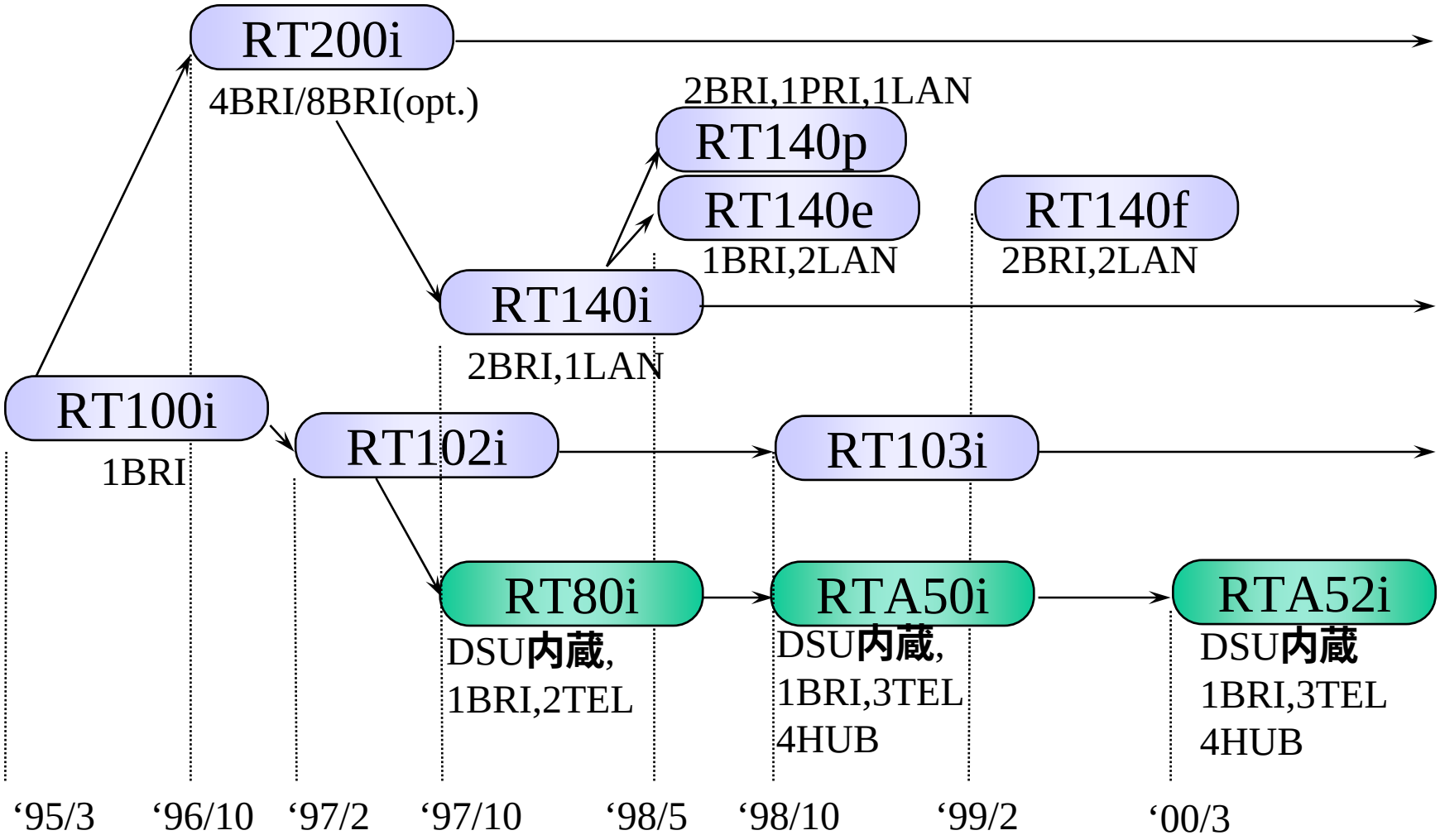
ISP: Internet Service Provider

®: Router

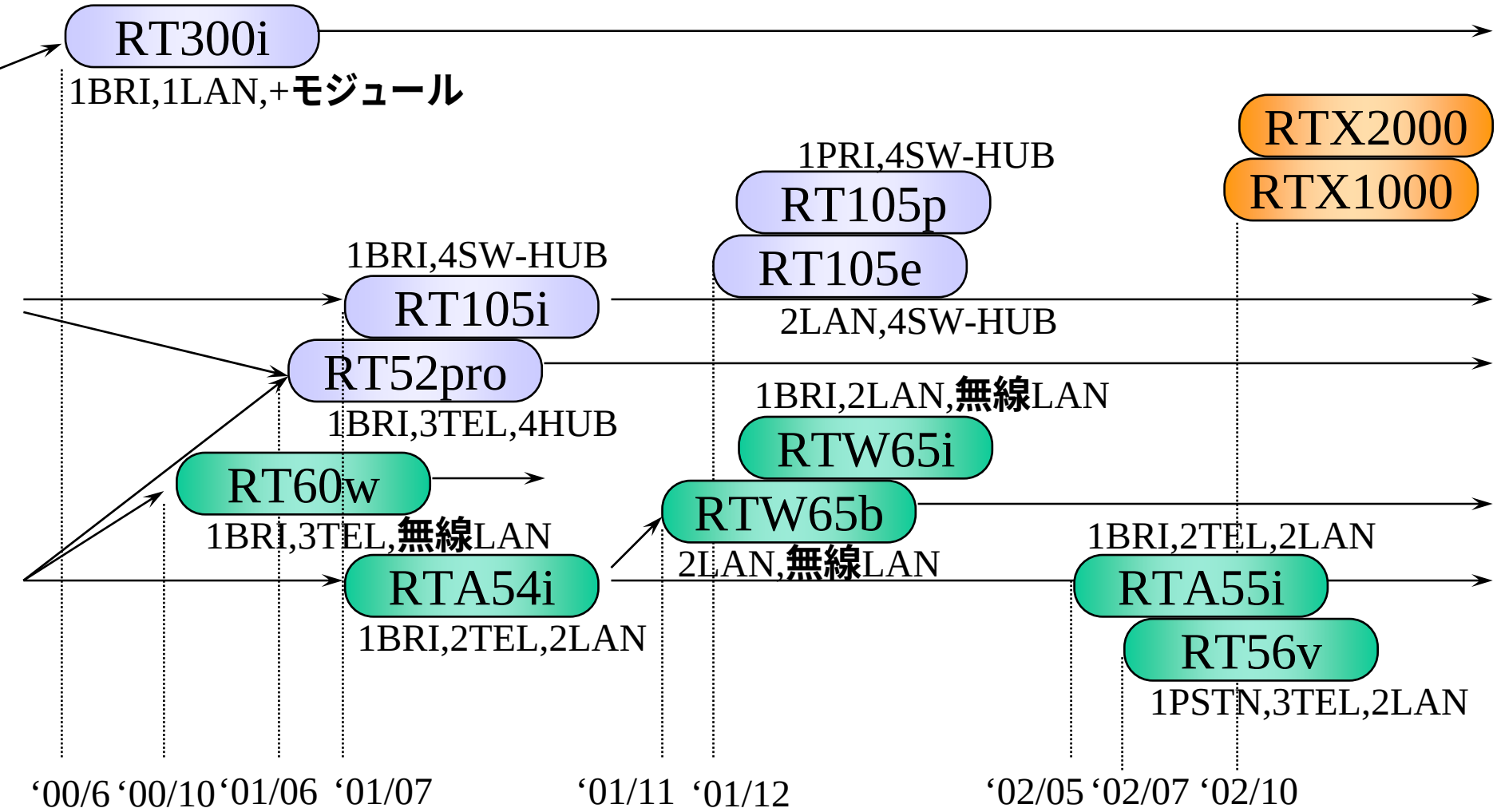
ヤマハルーター

- 歩み
- シリーズ構成

ヤマハルータの歩み#1



ヤマハルータの歩み#2



企業向けから個人、SOHO向けまで
信頼性と使い易さの実績

high-end

mid-range

1,000,000

Low-end

200,000

SOHO

個人

RT300 series

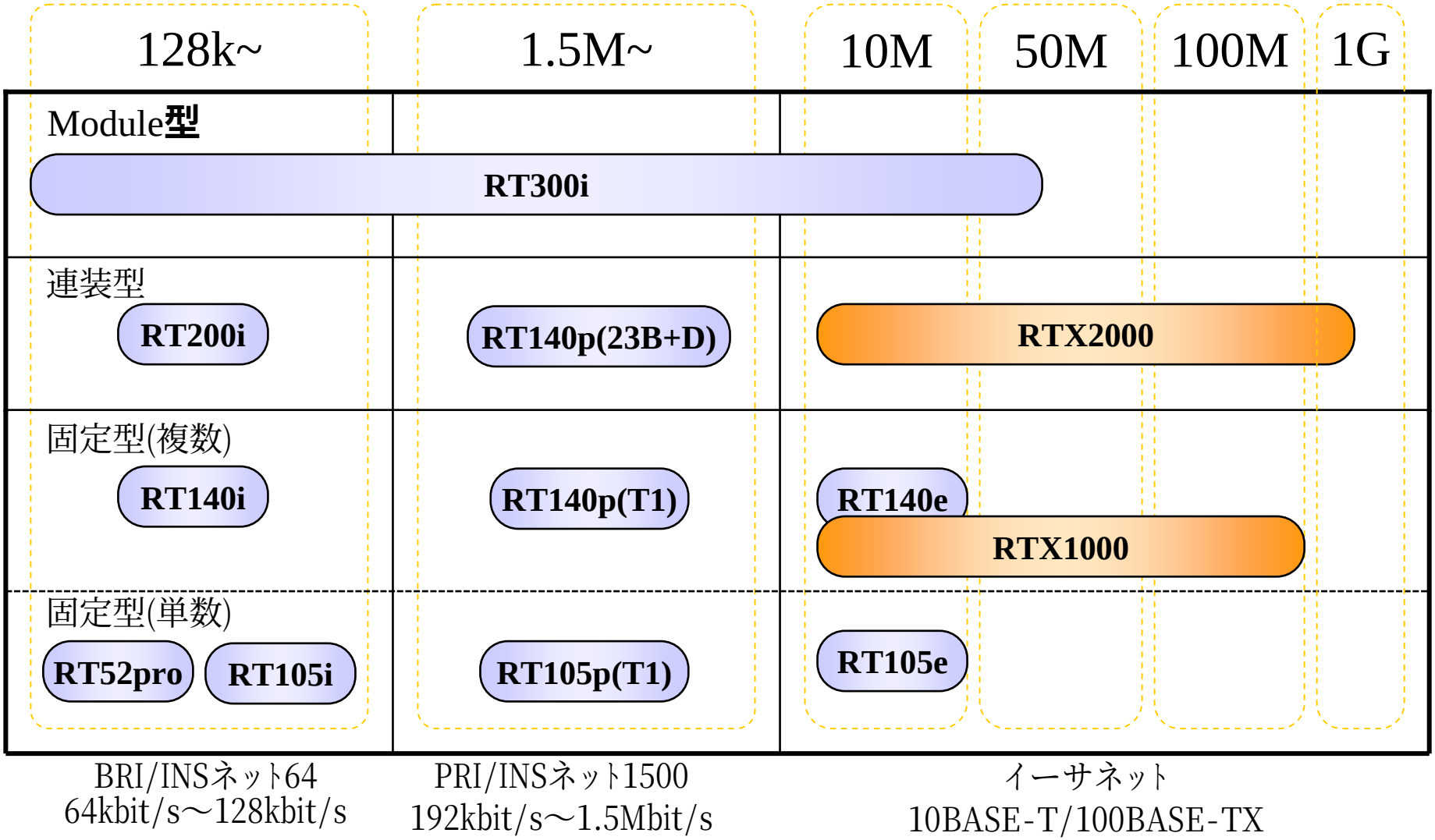
RT140 series

RT105 series

NetVolante series

YAMAHA

RTシリーズとRTXシリーズの製品構成



シリーズの位置付け

[RT100iの特徴]
※技術者が気軽に扱える手頃なルータ
(現場の要望がダイレクトに反映)

[RT100iの2つの顔]
a) プロバイダ接続用ルータ
b) 拠点側ルータ

主な区分	ネットボランチ	RT/RTXシリーズ
用途	プロバイダ接続	拠点
利用形態	スタンドアローン	ネットワーク
ユーザ層	初心者から技術者	企業など
設定機能	WWW設定	コンソール設定

RT/RTXのシリーズ･コンセプト

「多拠点ネットワーク構築のキーユニット」

ヤマハルーターで実現される多拠点ネットワーク･ソリューション

多拠点･遠隔地に設置される機器の性能

1. **信頼性**
2. **低価格**
3. **相互接続性**

ネットボランチのシリーズ・コンセプト

「オールインワン・ソリューション」

個人でも、ビジネスでも、

インターネットを「簡単」、「快適」に楽しむためのツール

1) **オール・イン・ワン**

標準的に必要とされる機能を1台にパッケージ

~~つながるだけ?~~

2) **多機能でもかんたんな設定**

標準機能に絞込まれたWeb設定

高度な利用もコンソールコマンドで自由自在

3) **初心者でも安心のセキュリティ**

高いデフォルトのセキュリティ・ポリシー

ヤマハ ルーターの特徴

・信頼性
・相互接続性
・一般化

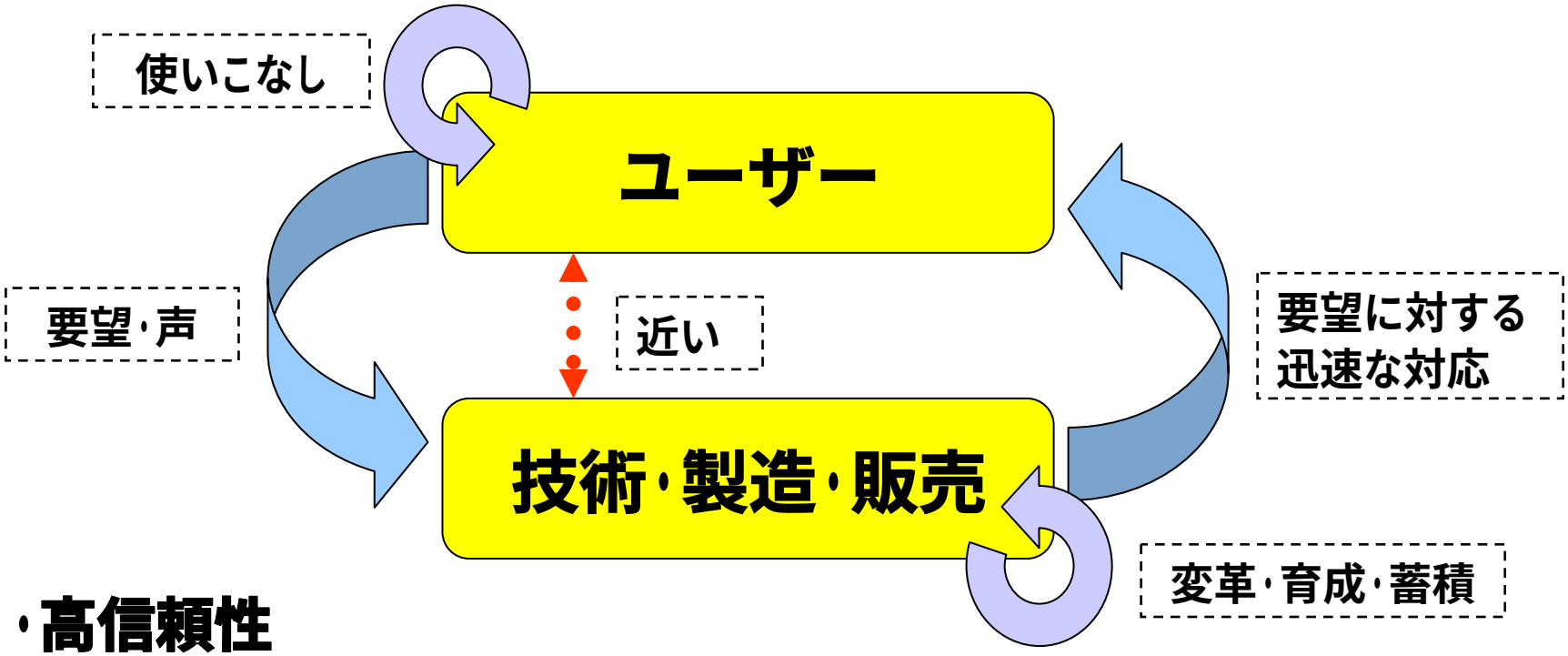
RTシリーズ
RTXシリーズ

RT100i

ネットボランチ
シリーズ

・ユーザー拡大

ヤマハのルーターは、国産



- **高信頼性**
  高信頼性部品の採用、部品点数の削減、自社工場で生産
- **自社製LSI (外販用を含む) の多用**
  →低レイヤ層から把握
- **ファームウェア(ドライバソフトなど)の自社開発**
  →迅速対応、ユーザサポートの充実
- **使いやすい設定機能と豊富な設定例**

RTXシリーズ
開発コンセプト

・RTX1000
・RTX2000

RTXシリーズ

進化

RTシリーズ

次世代イーサアクセスVPNルーター

RTX series

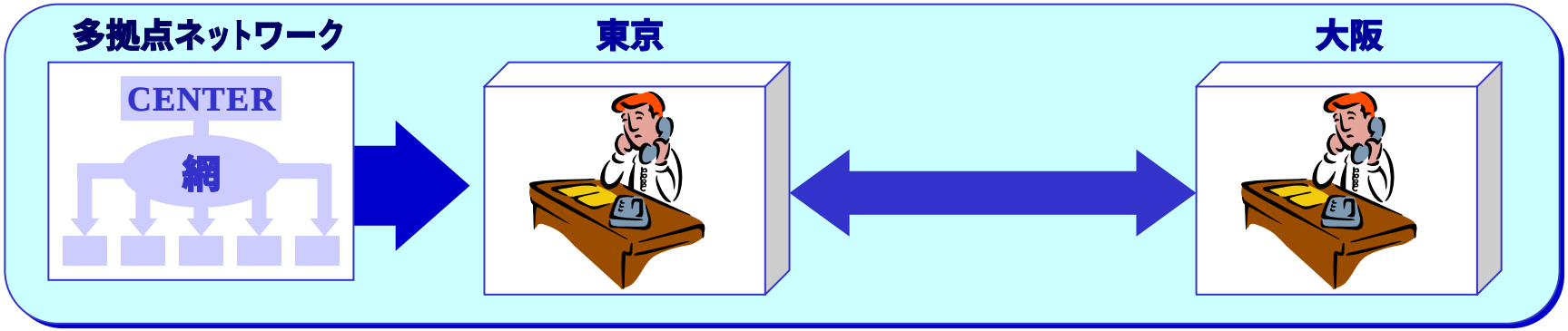
RTX2000

(2002年11月5日発売)

RTX1000

(2002年10月22日発売)

企業の多拠点ネットワークの動向



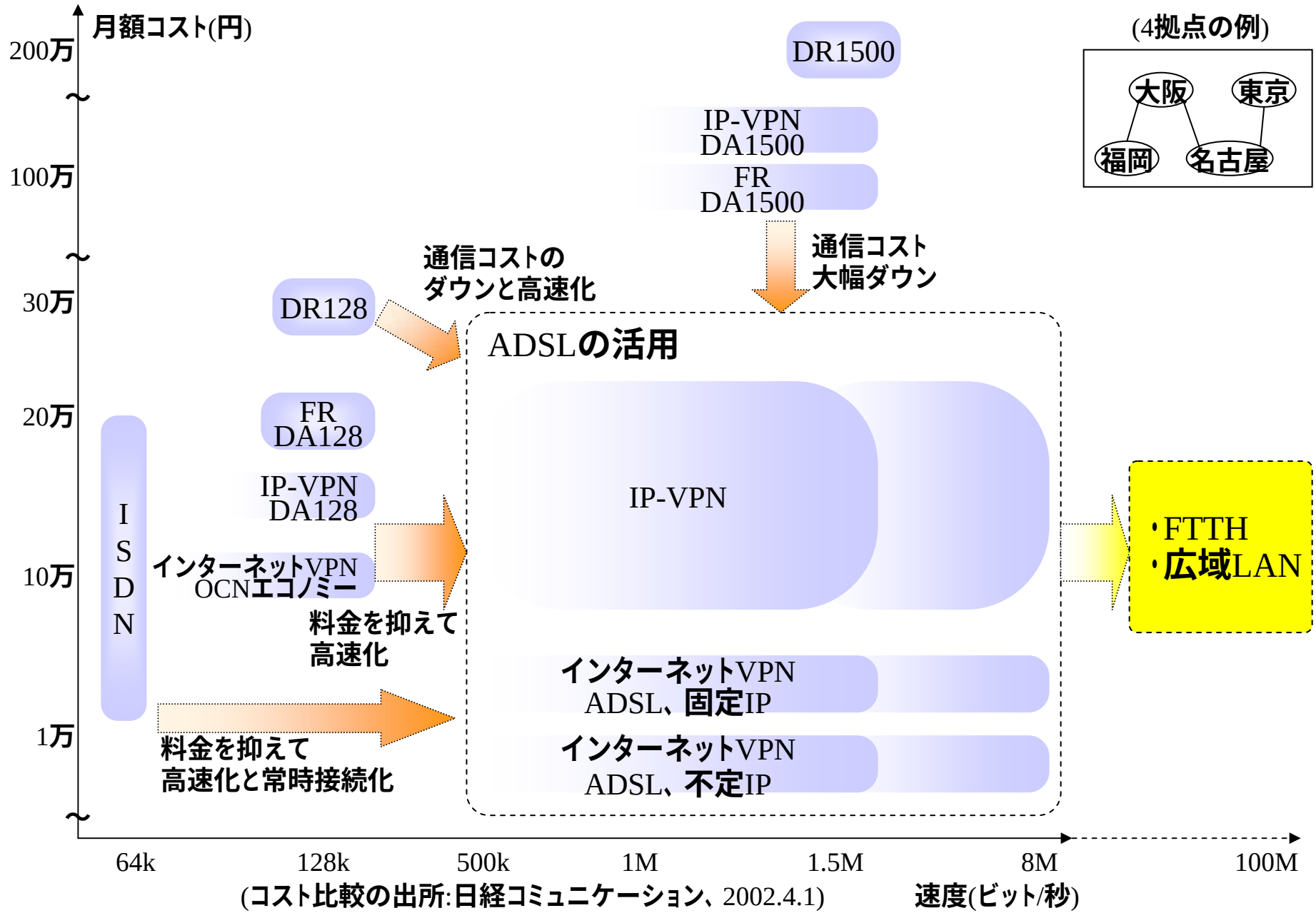
【既存のアクセス回線の選択肢】
- ISDN(64k)
- OCNエコノミー(128k) + インターネットVPN
- フレームリレー網(64k/128k)
- IP-VPN網(64k/128k)
- 専用線(デジタルリーチ: 64k～1.5M)

2001年のブロードバンドは
個人ユーザー先行

【ビジネス使用の条件】
- 信頼性の保持
- コストダウンの要請
- 高速化の要請

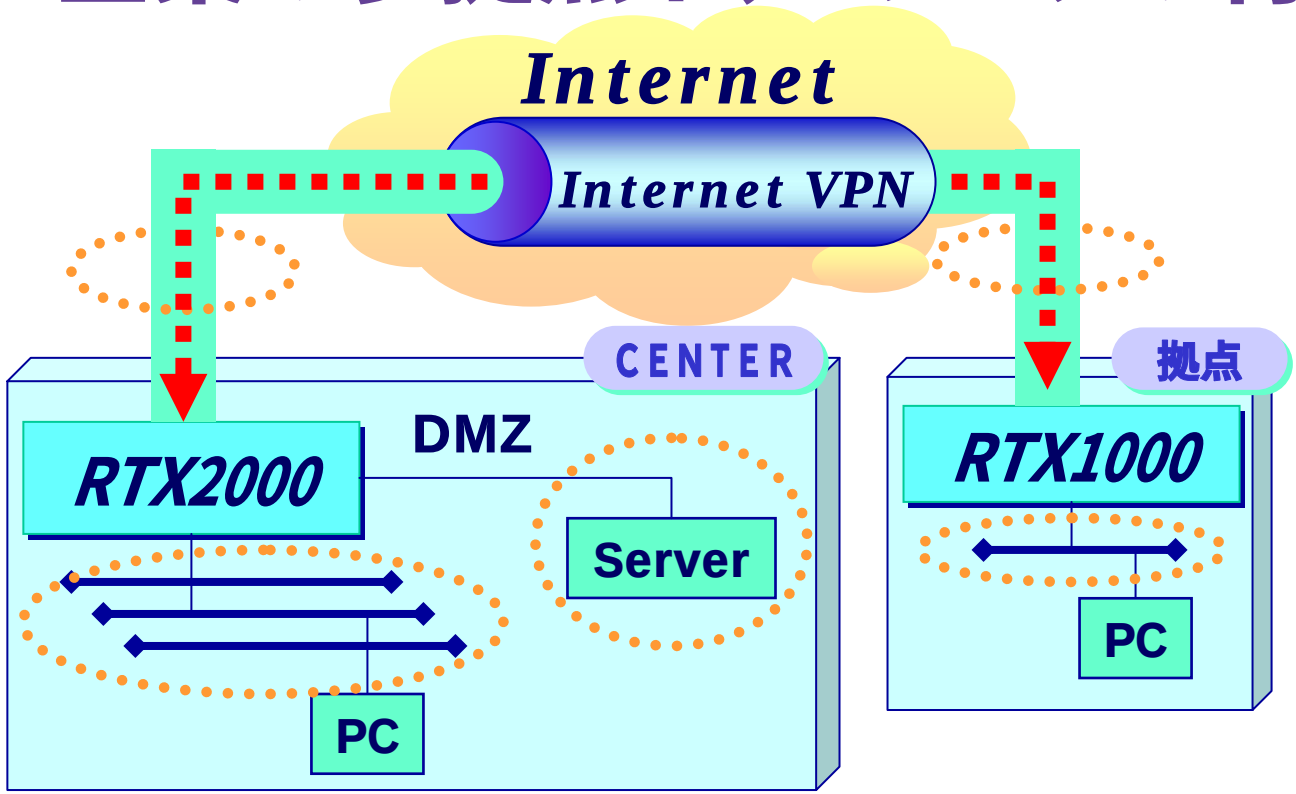
【ビジネスのブロードバンド化】
前提：低価格、高速、大容量
a) ギャランティ型アクセス回線
b) ベストエフォートアクセス回線+ 冗長性

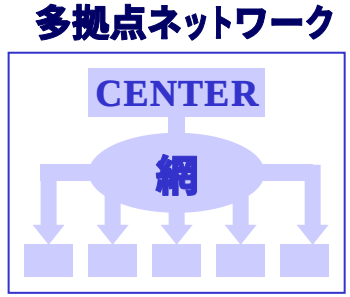
企業の多拠点ネットワークの通信コスト比較



(コスト比較の出所:日経コミュニケーション、2002.4.1)

企業の多拠点ネットワークの利用形態(VPN)





[ルーターに求められる要素]
- スループット
- LANの規模
- VPN(スループット)
- コスト(多拠点)

[ルーターに求められる要素]
- スループット
- 公開サーバの有無→DMZ
- LANの規模
- VPN(スループット,拠点数)

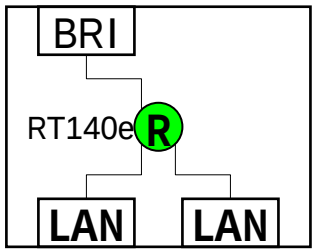
[ユーザーの選択条件]

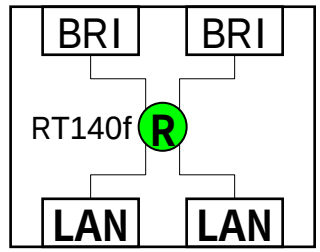
1) 処理能力、ポート数、価格

2) 信頼性、安全性、機能性、相互接続性

3) 実績、設定や管理のしやすさ

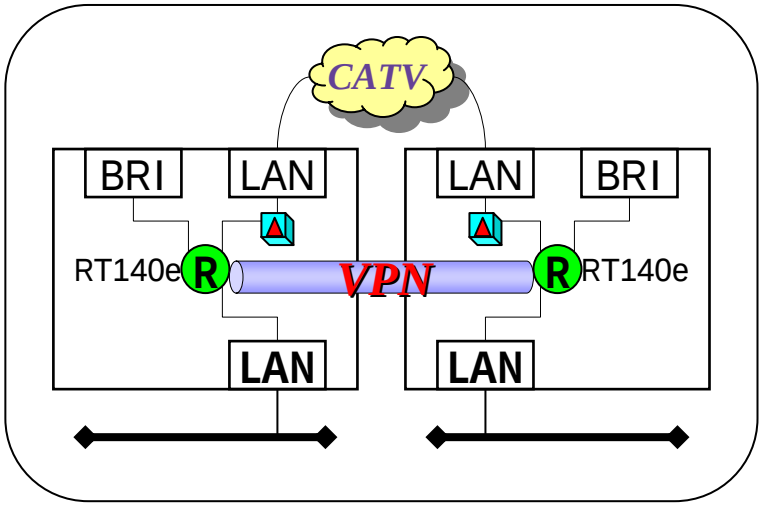
信頼と実績のブロードバンドVPNルーター
YAMAHA RT140e/RT140f





[RT140e]
- 1998年5月発売
- LAN: 2ポート
- BRI: 1ポート

[RT140f]
- 1999年2月発売(完売)
- LAN: 2ポート
- BRI: 2ポート



[ソフトウェア]
- 1998年5月: IPsec搭載 (セキュリティ・ゲートウェイ機能)
- 1999年1月: LAN間NAT搭載 (NATディスクリプタ機能)
- 2001年4月: PPPoE搭載～IPv6搭載
- 2001年12月: DHCPクライアント機能

ブロードバンドへの取り組み

日付	Revision	内容
1998年 5月	Rev.3.00.09	・RT140e発売
1999年 1月	Rev.4.00.02	・NATディスクリプタ機能
1999年 2月	Rev.4.00.05	・RT140f発売
2000年 5月	Rev.6.00.10	・RT300i+オプションモジュール発売
2000年 9月	Rev.4.01.06	○ネットボランチ(RTA52i)にNATディスクリプタ機能
2000年11月	Rev.5.00.10	○RT60w発売 (NATディスクリプタ機能、DHCPクライアント機能)
2001年 4月	Rev.5.01.12	○RT60wでブロードバンド接続設定対応(PPPoE機能)
2001年 4月	Rev.6.01.06	・PPPoE機能
2001年 5月		・IPv6正式対応発表 (2001年8月に対応完了)
2001年 7月	Rev.4.03.10	○RTA54i発売
2001年 7月	Rev.4.04.05	○常時接続保持機能(RTA54i)
2001年11月	Rev.5.03.07	○RTW65b発売
2001年12月	Rev.6.02.14	・RT105e発売 ・DHCPクライアント機能

Internet VPNへの取り組み

日付	Revision	内容
1998年5月	Rev.3.00.09	・セキュリティ・ゲートウェイ機能リリース1 (IPsec Version 2 I-Draft対応)
1998年9月	Rev.3.00.23	・TUNNELインタフェースへの静的フィルタ適用
1998年12月	Rev.3.01.11	・セキュリティ・ゲートウェイ機能リリース2 (IPsec Version 2 I-Draft対応)
1999年4月	Rev.4.00.07	・TUNNELインタフェースへのNATディスクリプタ適用
1999年7月	Rev.4.00.18	・セキュリティ・ゲートウェイ機能リリース3 (IPsec Version 2 RFC対応)
2000年2月	Rev.4.00.33	・ダイヤルアップVPN ・IPComp
2000年7月	Rev.4.00.39	・VPNパススルー(静的IPマスカレードの制限緩和)
2001年4月	Rev.6.01.06	・RT300i用VPNモジュール ・各種サービスの停止機能…IPsec用サービスの停止機能
2001年5月	Rev.6.02.03	・IPv6 ・TUNNELインタフェースへのファイアウォール適用
2001年9月	Rev.6.02.07	・TUNNELインタフェースのISDNによるバックアップ
2002年6月	Rev.6.03.08	・VPNプロトコル: PPTP対応

IPsec Version 2 RFC:RFC2401〜RFC2409、RFC2451

製品概要

- RTX1000
- RTX2000

RTXシリーズ

継承?
進化?

RTシリーズ

企業内の多拠点ネットワーク構築を実現
イーサアクセスVPNルーター

イーサアクセスVPNルーター

RTX1000

希望小売価格

118,000円 (税別)

次世代イーサアクセスVPNルーター

RTX 1000

高速性

- 100 Mbit/sの高スループット
- 3DES時スループット23Mbit/sを実現

冗長性

- VRRP
- ISDN,イーサネット,VPNにバックアップ

高機能性

- 高度なルーティング
  OSPF,BGP4,フィルタ型ルーティング,
  マルチホーミング
- 高度なIPv4/IPv6ファイアウォール機能
- IPv6標準搭載
  トンネル、ネイティブ、デュアルスタック、VPN

広域イーサネットに
インターネットVPNに
IP-VPNに

インターネット経由で、
企業内の多拠点ネットワーク構築を実現する

イーサアクセスVPNルーター

RTX2000

希望小売価格

398,000円 (税別)

次世代イーサアクセスVPNルーター

RTX 2000

高速性

◆最大ルーティング能力500Mbit/s
◆100Mbit/sワイヤスピードの高スループット
◆VPNスループット50Mbit/s(3DES)

冗長性

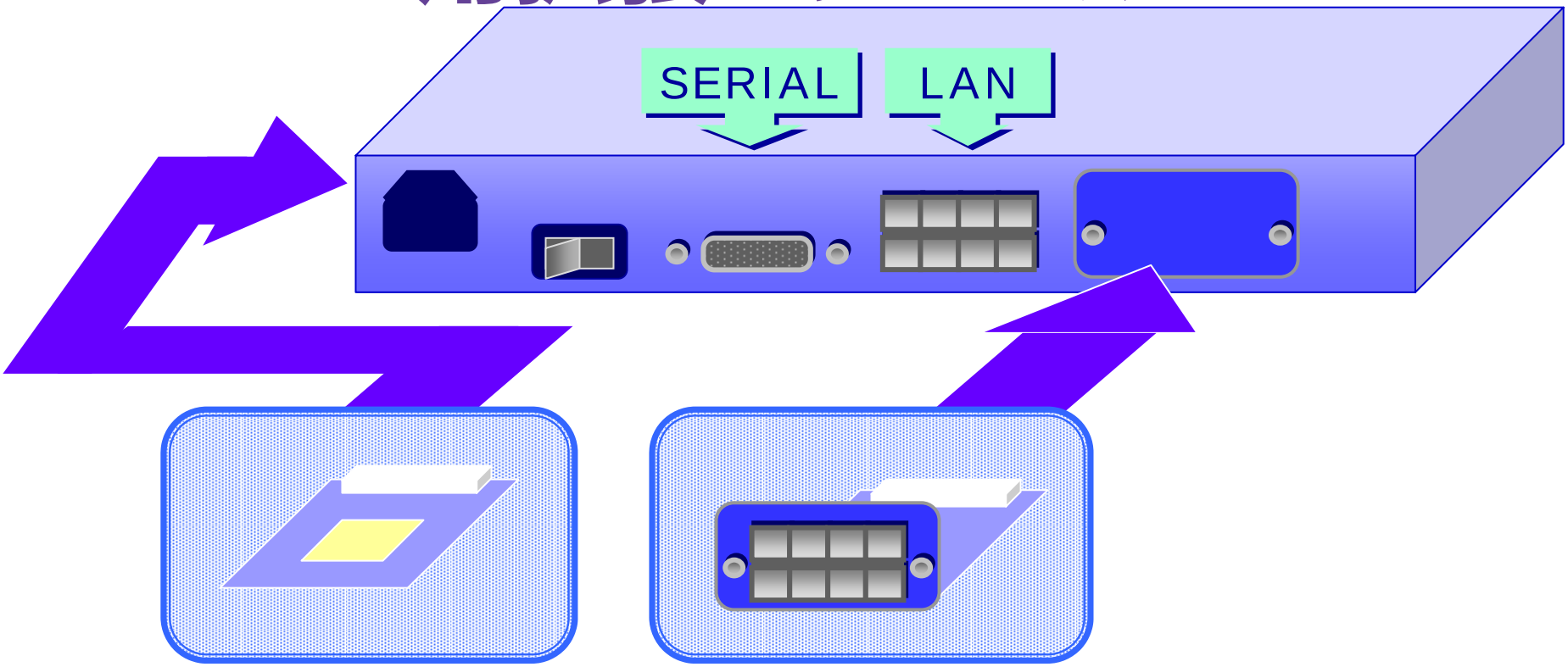
◆ VRRP
◆ イーサネット,VPNにバックアップ

高機能性

◆LANポート毎の独立ルーティング(最大16)
◆拡張モジュールで柔軟なネットワーク構築
(VPNモジュールとLANモジュール)
◆高度なフィルタリングによる
IPv4/IPv6ファイアウォール機能搭載。
◆ IPv6標準搭載で、将来の二重投資を回避。

広域イーサネットに
インターネットVPNに
IP-VPNに

RTX2000用拡張モジュール



VPNモジュール

YBB-VPN-A

希望小売価格
98,000円 (税別)

LANモジュール
(10BASE-T/100BASE-TX 8ポート)

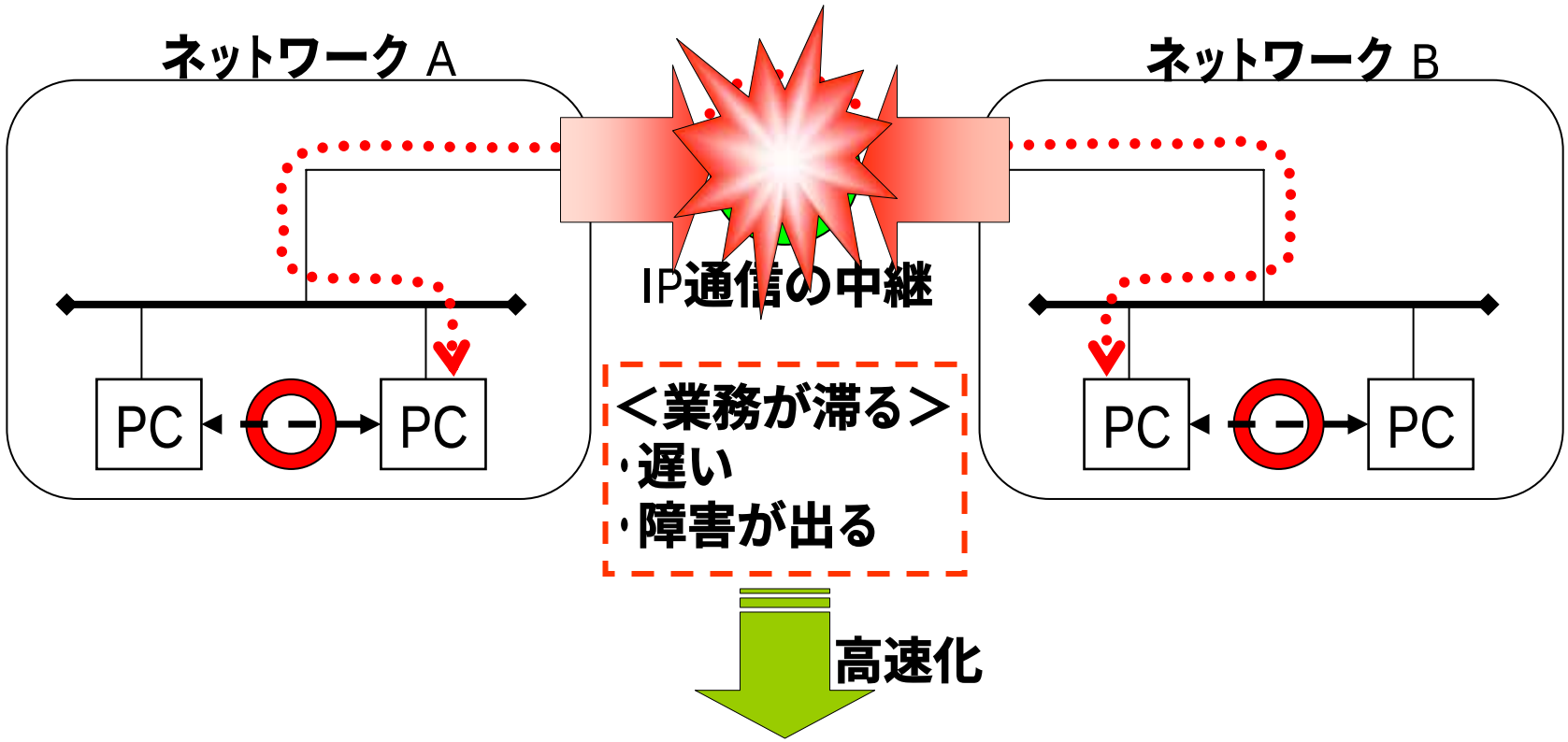
YBB-8FE-TX

希望小売価格
98,000円 (税別)

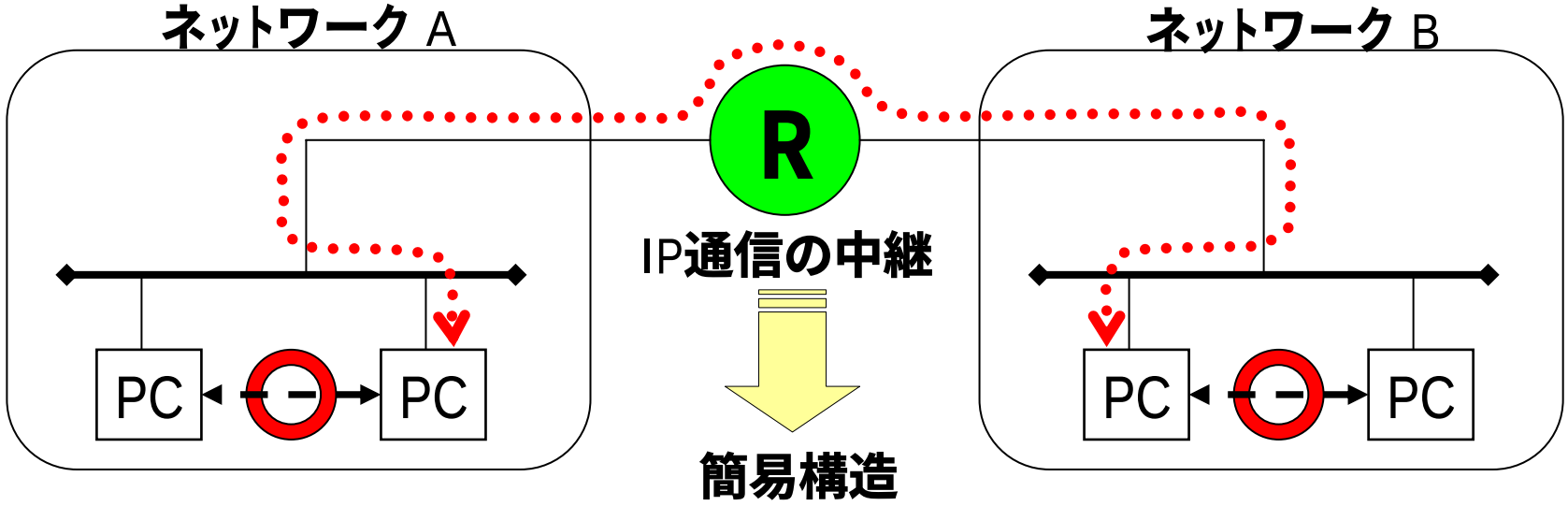
速いルーターとは？

- RT105e
- RTX1000
- RTX2000

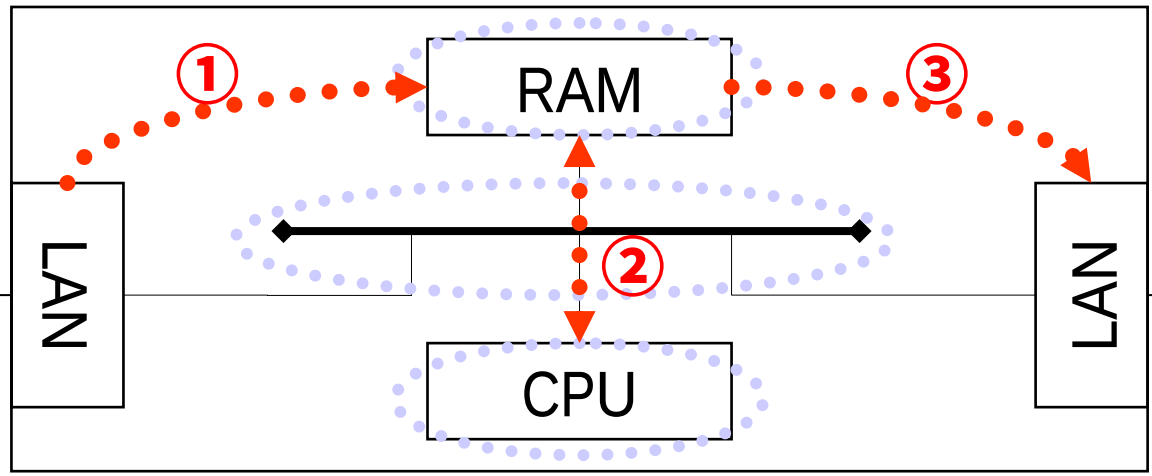
「速い」ルーターでできること



「速い」ルーターとは？

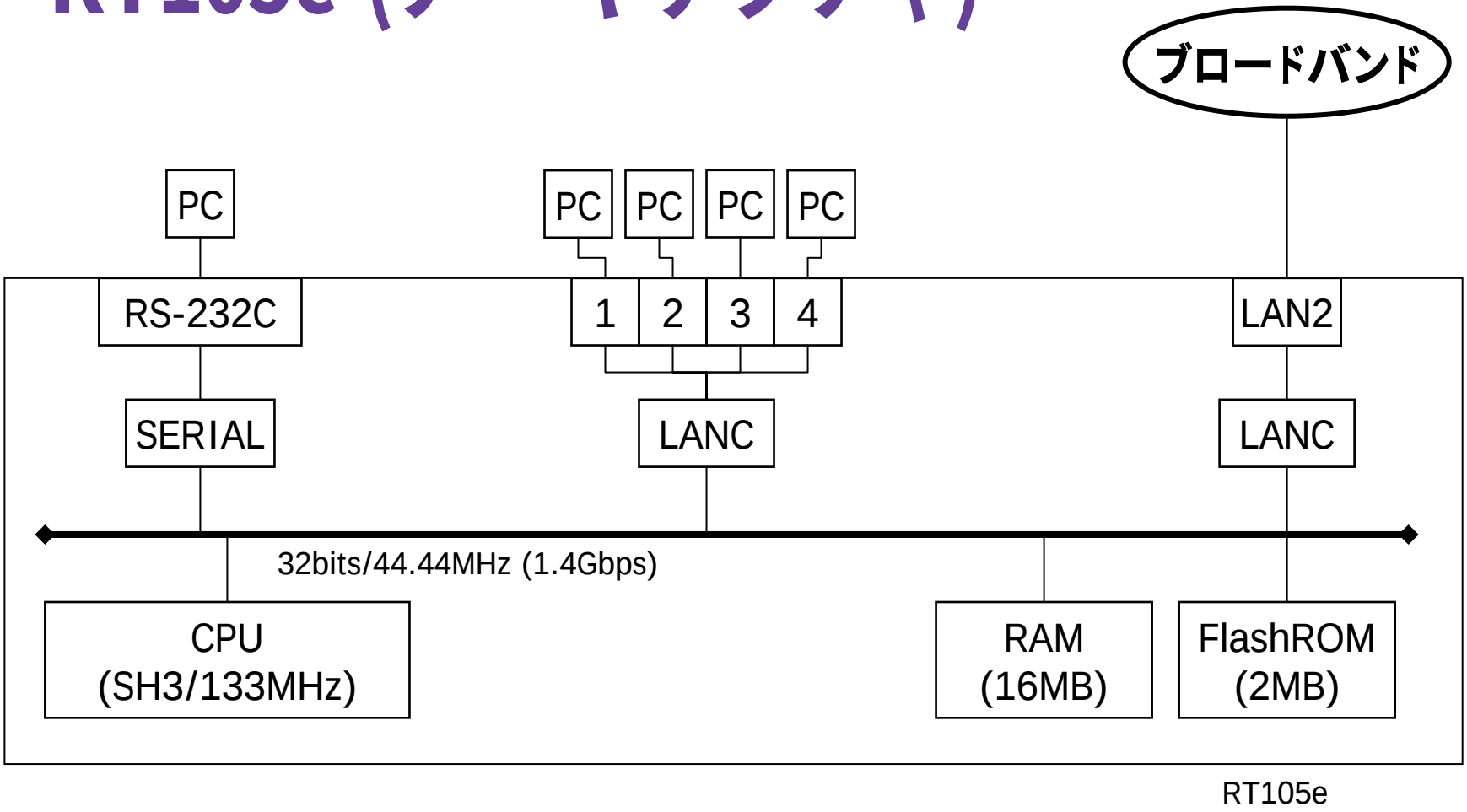


①パケット入力
②ルーティング
③パケット出力



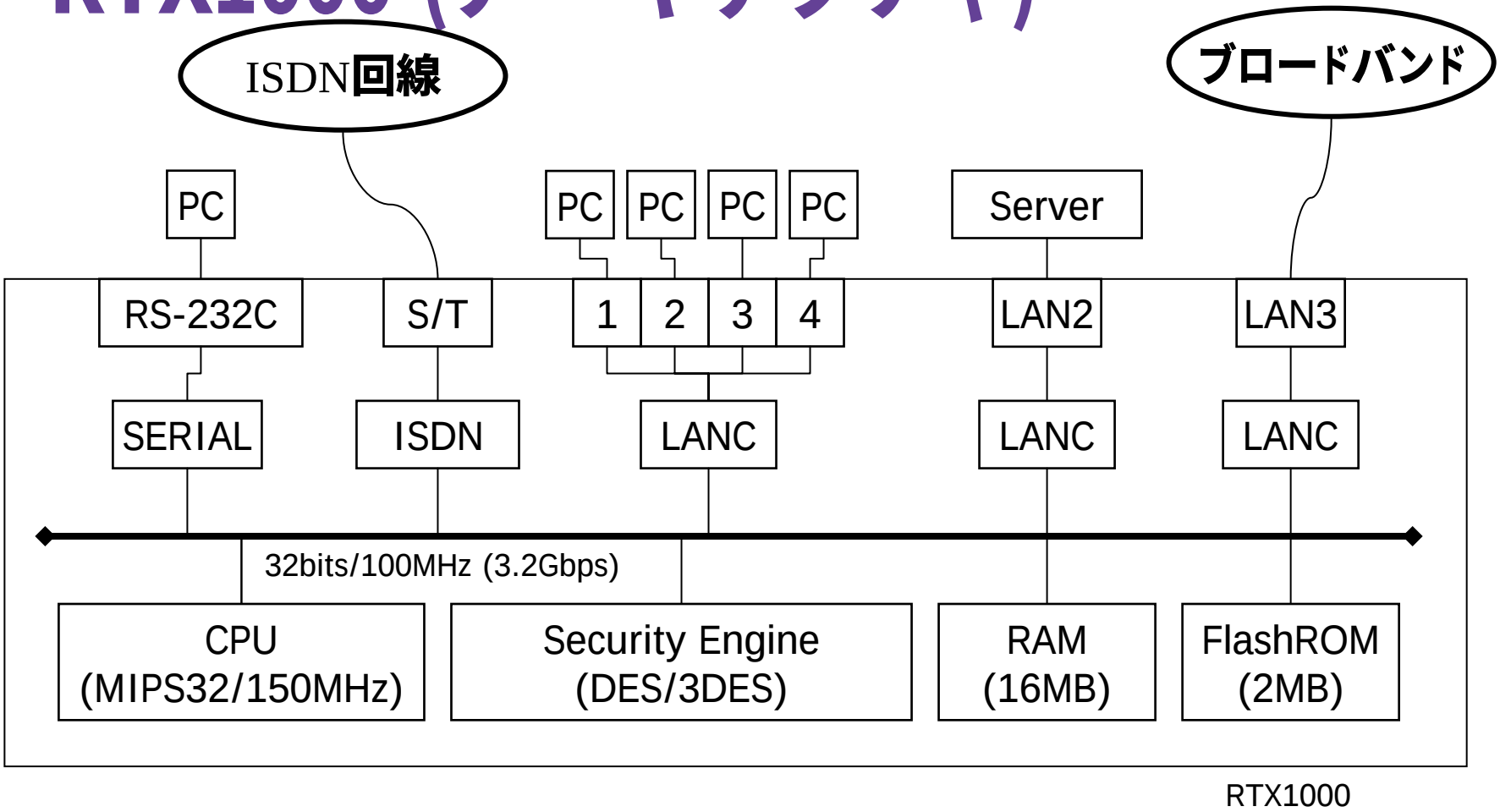
[ポイント]
ボトルネックの解消

RT105e (アーキテクチャ)



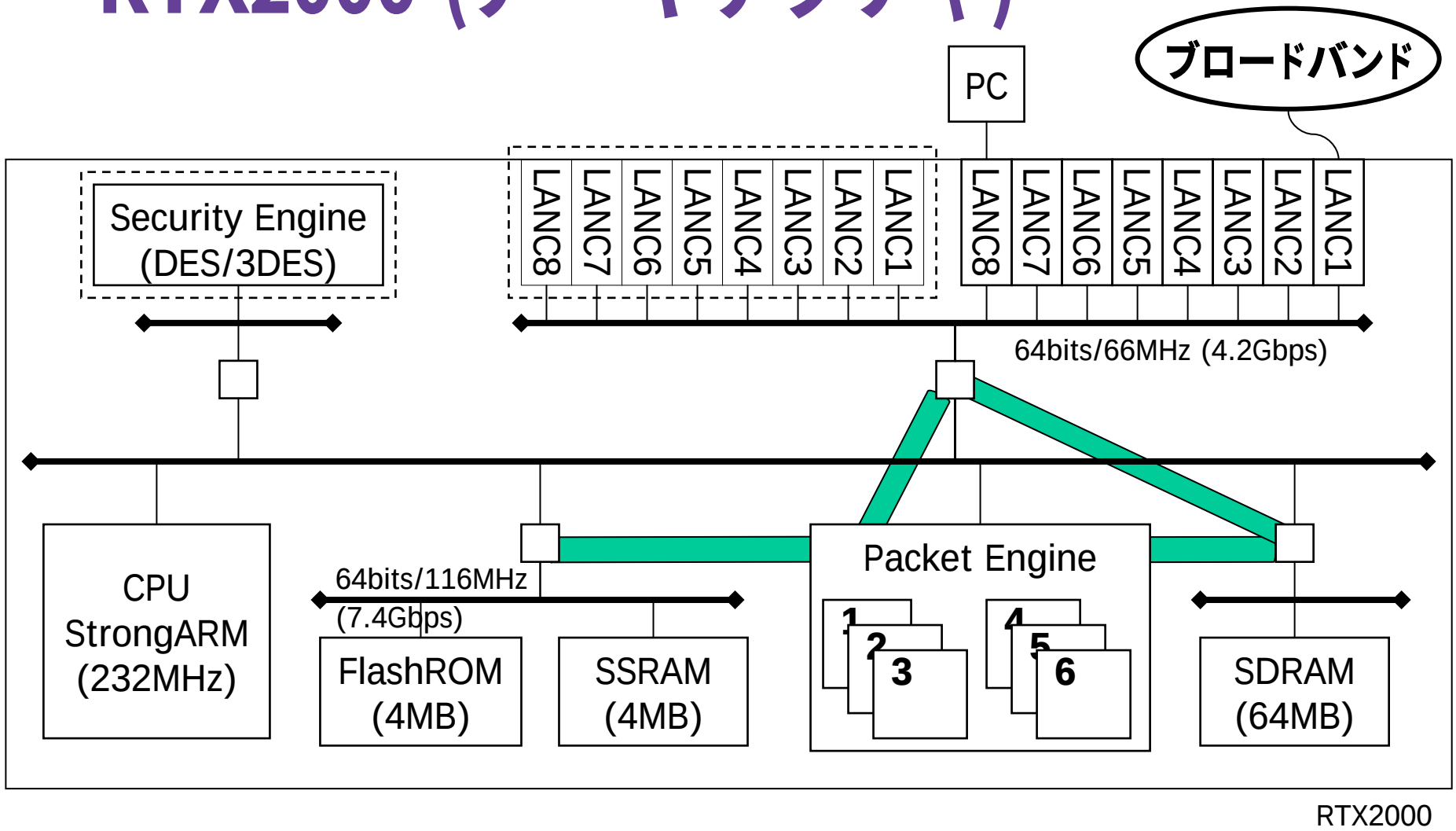
※概念を説明するためのイメージ図です。

RTX1000 (アーキテクチャ)



※概念を説明するためのイメージ図です。

RTX2000 (アーキテクチャ)



RTX2000

※概念を説明するためのイメージ図です。

スループット/処理能力

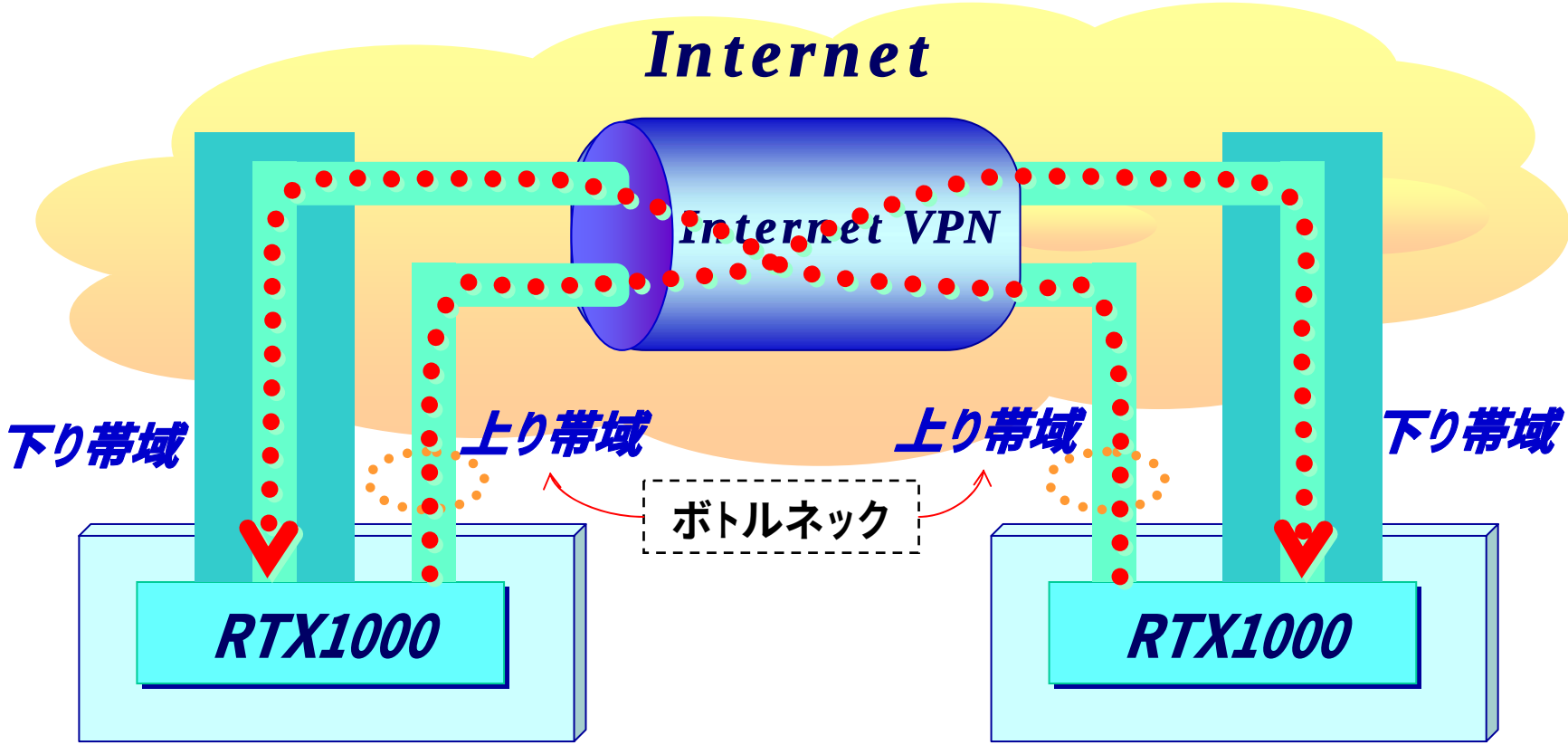
・RTX1000
・RTX2000

RTXシリーズ

高速化

RTシリーズ

(参考) ADSL環境でのVPNスループット



	1.5M ADSL	8M ADSL	12M ADSL
下り帯域	最大 1.5 Mbps	最大 8 Mbps	最大 12 Mbps
上り帯域	最大 512 Kbps	最大 1 Mbps	最大 1 Mbps

(参考) データリンクによってMTUが違う

MTUが異なる場合には、ルーターでパケットの分割と再構築が必要になる。

データリンク	MTU	Total Length
IPv4最大MTU(RFC791)	65535	—
IPv4最小PTMU(RFC1191)	576	—
IPv4最小MTU(RFC791)	68	—
IP over ATM	9180	—
FDDI	4352	4500
Ethernet	1500	1518
PPP (標準)	1500	—
IEEE 802.3 Ethernet	1492	1518
PPPoE(RFC2516)	1492	
PPPoE(フレッツ)	1454	
IPv6最小MTU(RFC2460)	1280	—

Ethernet

MAC (14)	IPパケット (46〜1500)	FCS (4)

PPPoE

MAC (14)	PPPoE (6)	PPP (2)	IPパケット (38〜1492)	FCS (4)

元パケット

MAC (14)	IPパケット (1500)	FCS (4)

PPPoEに流すとき、分割

フラグメントパケット#1

MAC (14)	PPPoE (6)	PPP (2)	IPパケット (1492)	FCS (4)

フラグメントパケット#2

MAC (14)	PPPoE (6)	PPP (2)	IPパケット (8+30)	FCS (4)

http://rfc.netvolante.jp/rfc/rfc1191.txt (Path MTU Discovery)

(参考)パケット処理能力

回線速度	最大値	
64k bit/s (half)	95 pps	
128k bit/s (half)	190 pps	
10M bit/s(half)	14,881 pps	15k pps
100M bit/s (half)	148,810 pps	150k pps

Q.「パケット処理能力」とは、何か？

一般的にRFC2544(RFC1944)に従ったベンチマークテストのうち

「パケットサイズが64バイトのスループット(Throughput)」のことを指します。

この数値はpps(packets/sec)で表され、正確な測定のためには、専用の測定装置が利用されます。

Q.RFC1242で定義される「スループット(Throughput)」とは、何か？

「パケットロスが発生しない最大パケット転送能力」です。

"The maximum rate at which none of the offered frames are dropped by the device."

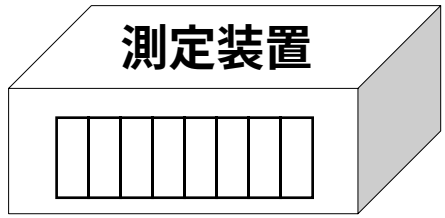
Q.RFC1242とRFC1944とは、どう違うのですか？

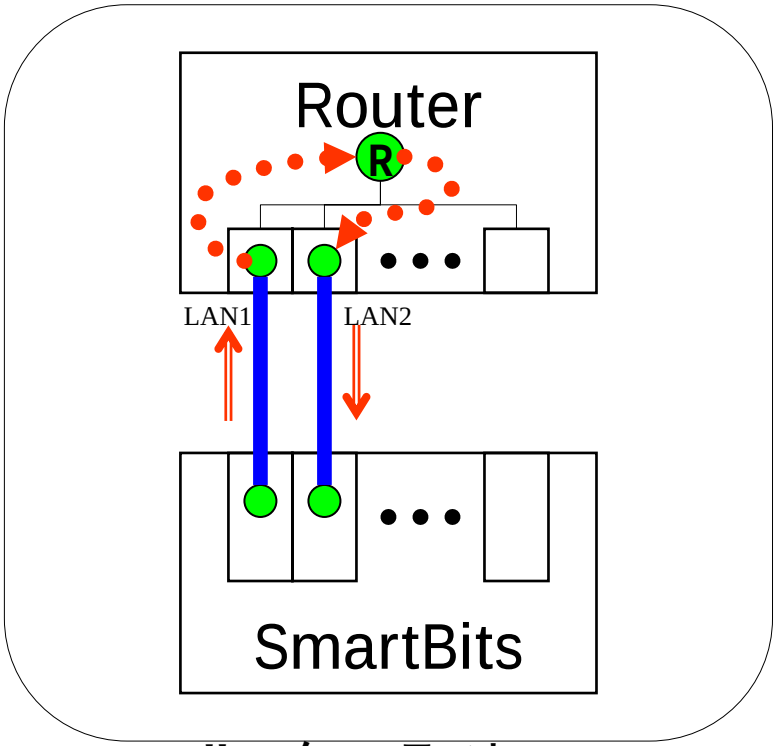
RFC1242:「ベンチマーク用語」

RFC1944(RFC2544):「ベンチマーク方法」

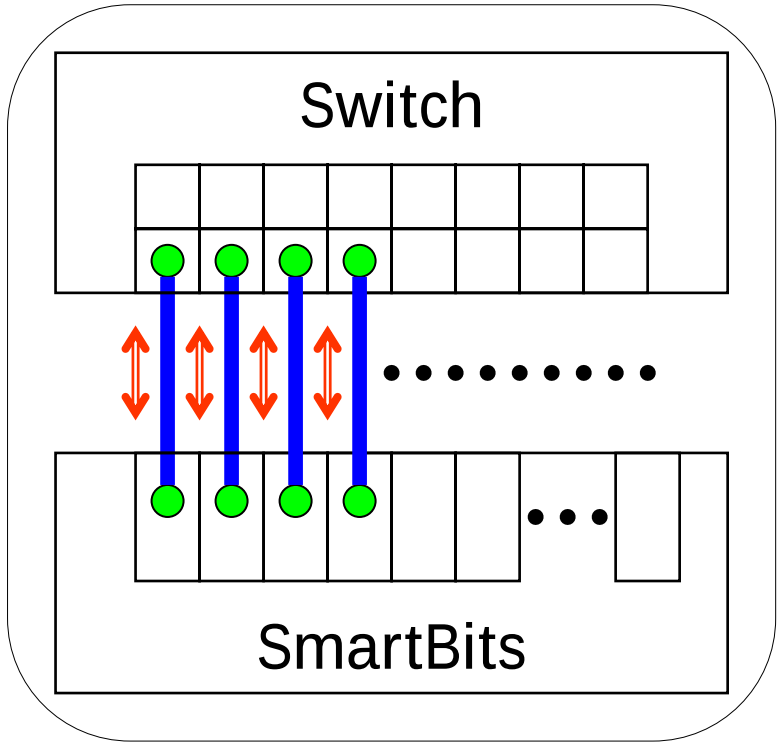
http://www.rtpro.yamaha.co.jp/RT/FAQ/TCPIP/routing-performance.html
http://rfc.netvolante.jp/rfc/rfc1242.txt (Benchmarking ***Terminology*** for Network Interconnection Devices)
http://rfc.netvolante.jp/rfc/rfc2544.txt (Benchmarking ***Methodology*** for Network Interconnect Devices)
http://rfc.netvolante.jp/rfc/rfc2285.txt (Benchmarking Terminology for ***LAN Switching Devices***)
http://rfc.netvolante.jp/rfc/rfc2889.txt (Benchmarking Methodology for ***LAN Switching Devices***)

SmartBitsによる測定(L2/L3)





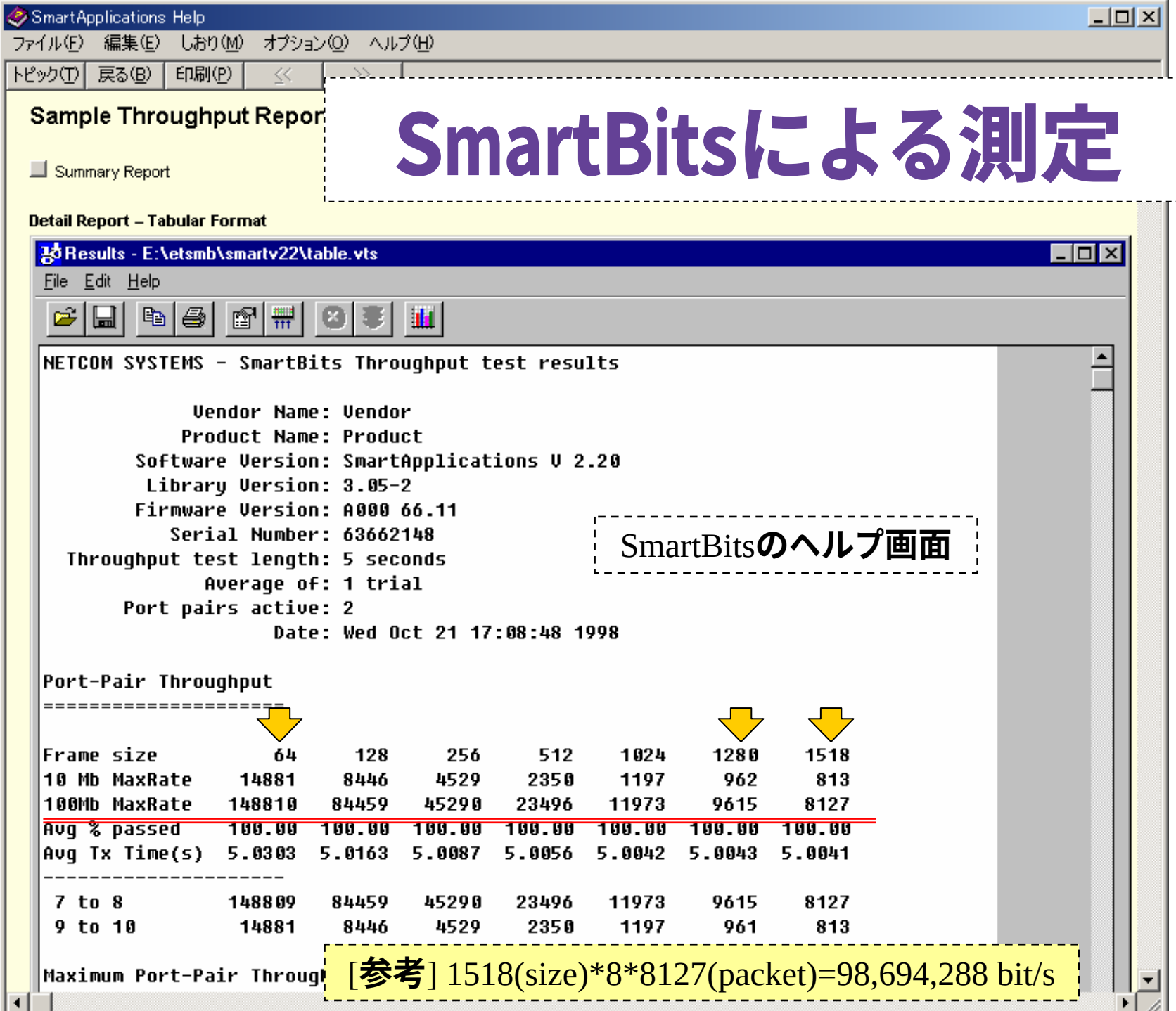
ルーター・テスト(L3)



スイッチ・テスト(L2)

SmartBits
- SmartWindow →パケット生成、耐久試験など
- ***SmartApplications*** →RFC1242&RFC2544準拠の性能測定

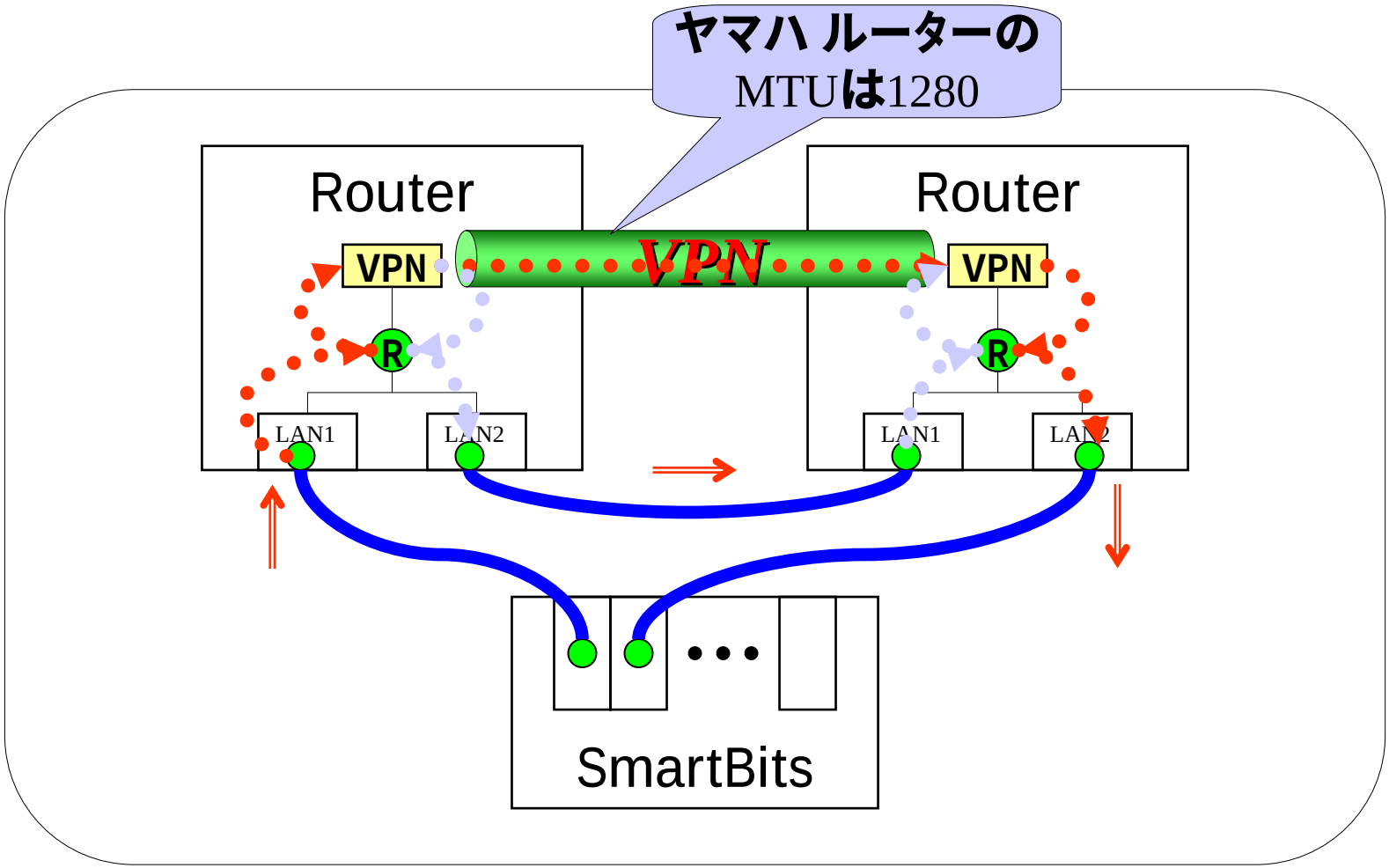
SmartBitsによる測定



SmartBitsのヘルプ画面

[参考] 1518(size)*8*8127(packet)=98,694,288 bit/s

SmartBitsによる測定(VPN)



ルーター・テスト(L3)

スループット比較

速度比較	ポート数	速度	3DES	VPN数	価格
RT300i	(10/100)*2	39.8M bit/s	3.0M bit/s	100	800,000円
RT300i+VPN	(10/100)*2		10.2M bit/s	500	1,000,000円
RT140e	(10/100)*2	14.2M bit/s	1.1M bit/s	20	320,000円
RT105e	(10/100)*2	15.5M bit/s	1.2M bit/s	30	68,000円
他社製品	**ポート数**	**速度**	3DES	VPN数	**価格**
CISCO 3640 (IOS 12.0.5T)		F: 100M bit/s P: 21.2M bit/s			約160万円～
CISCO 2621 (IOS 12.1.7)		F: 66.9M bit/s P: 15.0M bit/s			約60万円～
FITELnet-F40	(10/100)*2	9.8M bit/s	4.6M bit/s	32	118,000円
SonicWall TELE3	(10/100)*2	75M bit/s	20M bit/s	5	(5u) 148,000円
SonicWall PRO 200	(10/100)*3	190M bit/s	25M bit/s	500	745,000円
NetScreen-5XP	(10)*2	20M bit/s	13M bit/s	10	(10u) 98,000円
NetScreen-5XT	(10/100)*2	70M bit/s	20M bit/s	10	(10u)138,000円
NetScreen-25	(10/100)*4	100M bit/s	25M bit/s	25	680,000円
AR740	(10/100)*2	66M bit/s	ー	ー	312,900円
AR740+VPN	(10/100)*2	66M bit/s	DESのみ	(?)	364,400円
RTXシリーズ	**ポート数**	**速度**	3DES	VPN数	**価格**
RTX2000	(10/100)*8	500M bit/s	ー	ー	398,000円
RTX2000 + VPN	(10/100)*8	500M bit/s	50M bit/s	500	496,000円
RTX1000	(10/100)*3	100M bit/s	23M bit/s	30	118,000円

※ヤマハ調べ(カタログ値、または、RFC1242/RFC2544に従った測定値,2002年10月)

製品比較

出所:
日経コミュニケーション、2002.11.4、P.52〜P.53
新型WANを狙い撃つ拠点ルーター
「ブロードバンド2回線に接続切れても自動迂回で障害回避」

	古河電気工業	NEC	アライドレテシス	センチュリー	ヤマハ	富士通
製品名	FITELnet-F40	IX2010	AR410V2	XR-360/Pro	RTX1000	Si-R170
発売	2001年11月	2002年6月	2002年10月	2002年10月	2002年10月	2002年11月
価格	118,000円	198,000円	69,800円	118,800円	118,000円	128,000円
インターフェイス	10M/100M*4(SW) 10M/100M*1	10M/100M*1 10M/100M*1 拡張*1	10M/100M*4(SW) 10M/100M*1 拡張*1	10M/100M*4(SW) 10M/100M*1 BRI*1	10M/100M*4(SW) 10M/100M*1 10M/100M*1 BRI*1	10M/100M*1 10M/100M*1
(LAN*2+VPN)	○	○(★、208,000円)	○(★、121,300円)	○	○	○
(同上+BRI)	×	?	○(★、159,100円)	○	○	×
(LAN*3+VPN)	×	○(★、244,000円)	○(★、159,100円)	×	○	×
(同上+BRI)	×	×	×	×	○	×
最大VPN (3DES)	7.2M bit/s	約15M bit/s (★?)	約5M bit/s (★,DESのみ)	9.1M bit/s	23M bit/s	20M bit/s
ルーティングプロトコル	RIP1/2、BGP4	RIP1/2、OSPF	RIP1/2、OSPF	RIP1/2、OSPF	RIP1/2、OSPF、BGP4	RIP1/2、OSPF、BGP4
(IPv6)	×(予定)	RIPng	×(予定)	×	RIPng	RIPng
VPN機能	IPsec	IPsec	IPsec(★)、L2TP	IPsec	IPsec、PPTP	IPsec
備考	・バックアップ機能 ・VRRP相当(独自)	・QoS ・VLANタグ	・VRRP ・マルチホーミング ・マルチキャスト	・攻撃検知機能 ・VRRP	・QoS(予定) ・バックアップ機能 ・VRRP ・攻撃検知機能 ・マルチホーミング	・QoS ・バックアップ機能 ・VRRP
オプション (★)		・VRRP: 3万円 ・IPsec高速:1万円 ・10M/100M*4(SW): 36,000円	・BRI*1: 37,800円 ・10M*1: 37,800円 ・PRI*1: 102,900円 ・暗号: 51,500円			

RTX1000性能評価 (ルーティング)

Rev.7.00.04の場合 (スループットのチューンは、継続中)

パケット処理能力(pps: paket/second)

最大スループット (bit/s)

Port-Pair Throughput

Frame size	64	128	256	512	1024	1280	1518
100Mb MaxRate	148810	84459	45290	23496	11973	9615	8127
Avg % passed							100.00
Avg Tx Time(s)	10.002	10.002	10.002	10.002	10.002	10.002	10.002
(01,01,01) to (01,02,01)							8127

パケットサイズ(bit換算)*1秒間の転送パケット数

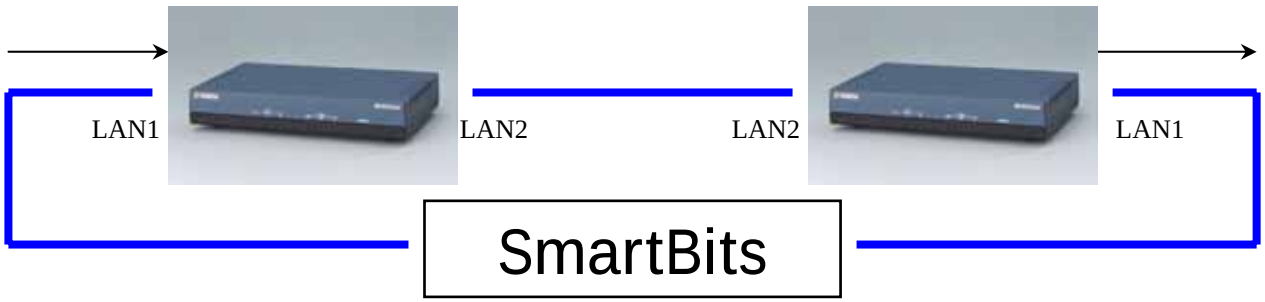
→(1280*8)*(9107)=93255680 bit/s→93.26Mbit/s

※KやMの換算において1024ではなく1000で割る(通信界)

※スループットのチューンは継続作業中です。

RTX1000性能評価 (ルーティング*2)

Rev.7.00.04の場合 (スループットのチューンは、継続中)



パケット処理能力(pps: paket/second)

最大スループット (bit/s)

Port-Pair Throughput

Frame size	64	128	256	512	1024	1280	1518
100Mb MaxRate	148810	84459	45290	23496	11973	9615	8127
Avg % passed							100.00
Avg Tx Time(s)	10.002	10.002	10.002	10.002	10.002	10.002	10.002
(01,01,01) to (01,02,01)							8127

パケットサイズ(bit**換算**)*1**秒間の転送パケット数**

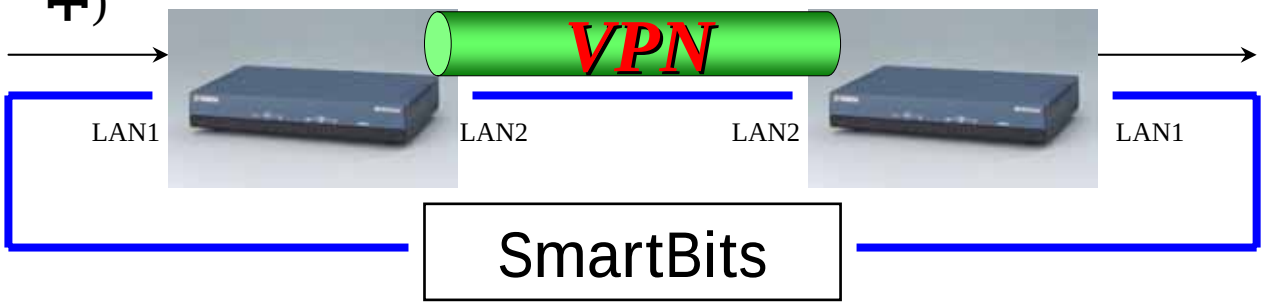
→(1280*8)*(8744)=89538560 bit/s→89.54Mbit/s

※K**や**M**の換算において**1024**ではなく**1000**で割る(通信界)**

※**スループットのチューンは継続作業中です。**

RTX1000性能評価 (VPN:3DES)

Rev.7.00.04のケース (スループットのチューンは、継続中)



最大VPNスループット(bit/s)

3DES
Port-Pair Throughput

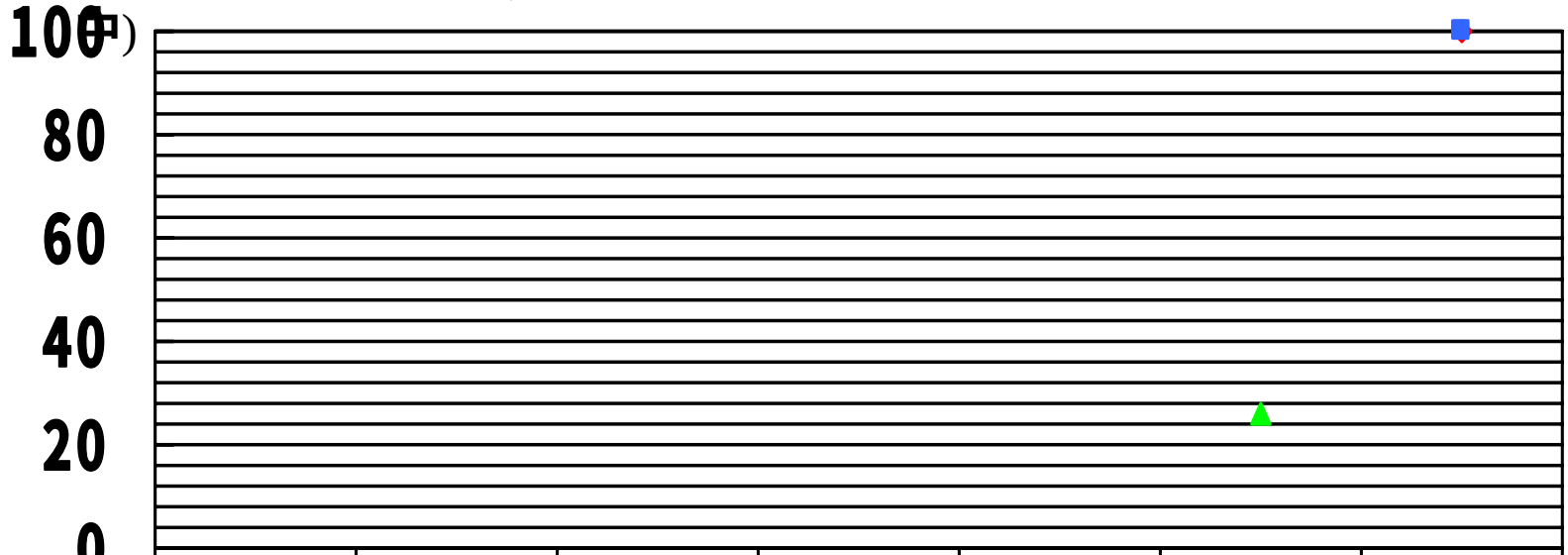
Frame size	64	128	256	512	1024	1280	1492	1518
100Mb MaxRate	148810	84459	45290	23496	11973	9615	8267	8127
Avg % passed						25.70		
Avg Tx Time(s)	9.9997	9.9996	9.9996	9.9997	9.9995	9.9993	9.9992	9.9987
(01,01,01) to (01,02,01)						2471		

パケットサイズ(bit**換算**)*1**秒間の転送パケット数**
→(1280*8)*(2471)=25303040 bit/s**→**25.30Mbit/s
※K**や**M**の換算において**1024**ではなく**1000**で割る(通信界)**

※スループットのチューンは継続作業中です。

RTX1000性能評価 (グラフ)

Rev.7.00.04のケース (スループットのチューンは、継続中)

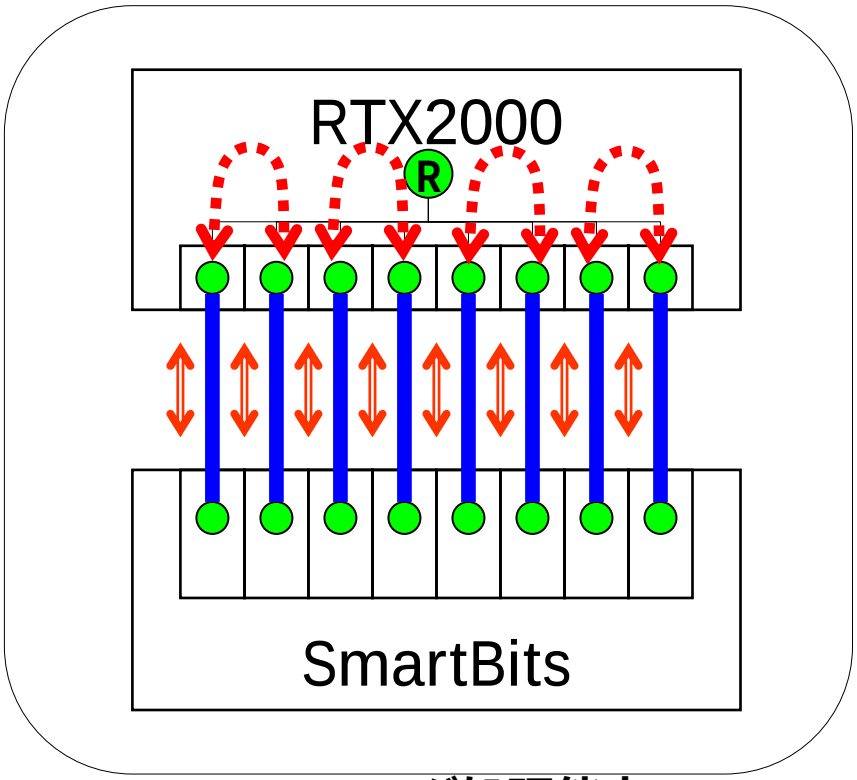


	64	128	256	512	1024	1280	1518
RTX							100.00
RTX-RTX							100.00
VPN(3DES)						25.70	

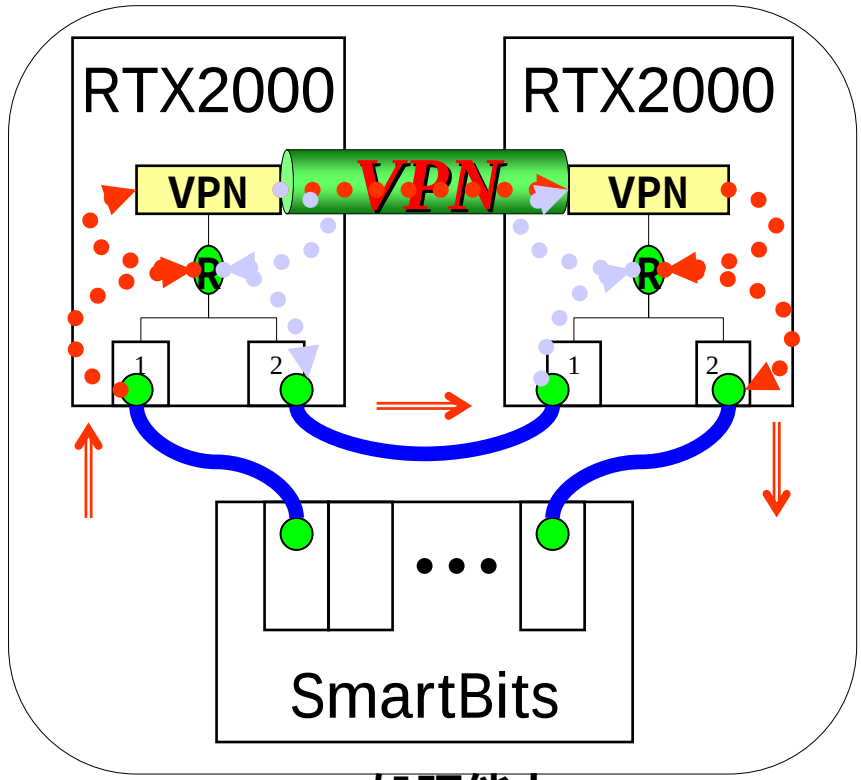
フレームサイズ

※スループットのチューンは継続作業中です。

RTX2000性能評価



ルーティング処理能力



VPN処理能力

[Rev.7.00.10]

・2ポート間: 64～1518で、100% (1対、方方向)
・8ポート間: 64で、280k pps (4対、双方向)
・8ポート間: 1518で、800M bps(4対、双方向)

[Rev.7.00.10]

・VPN(DES/3DES): 1280で、70%以上

※スループットのチューンは継続作業中です。

CISCO製品のカタログ値

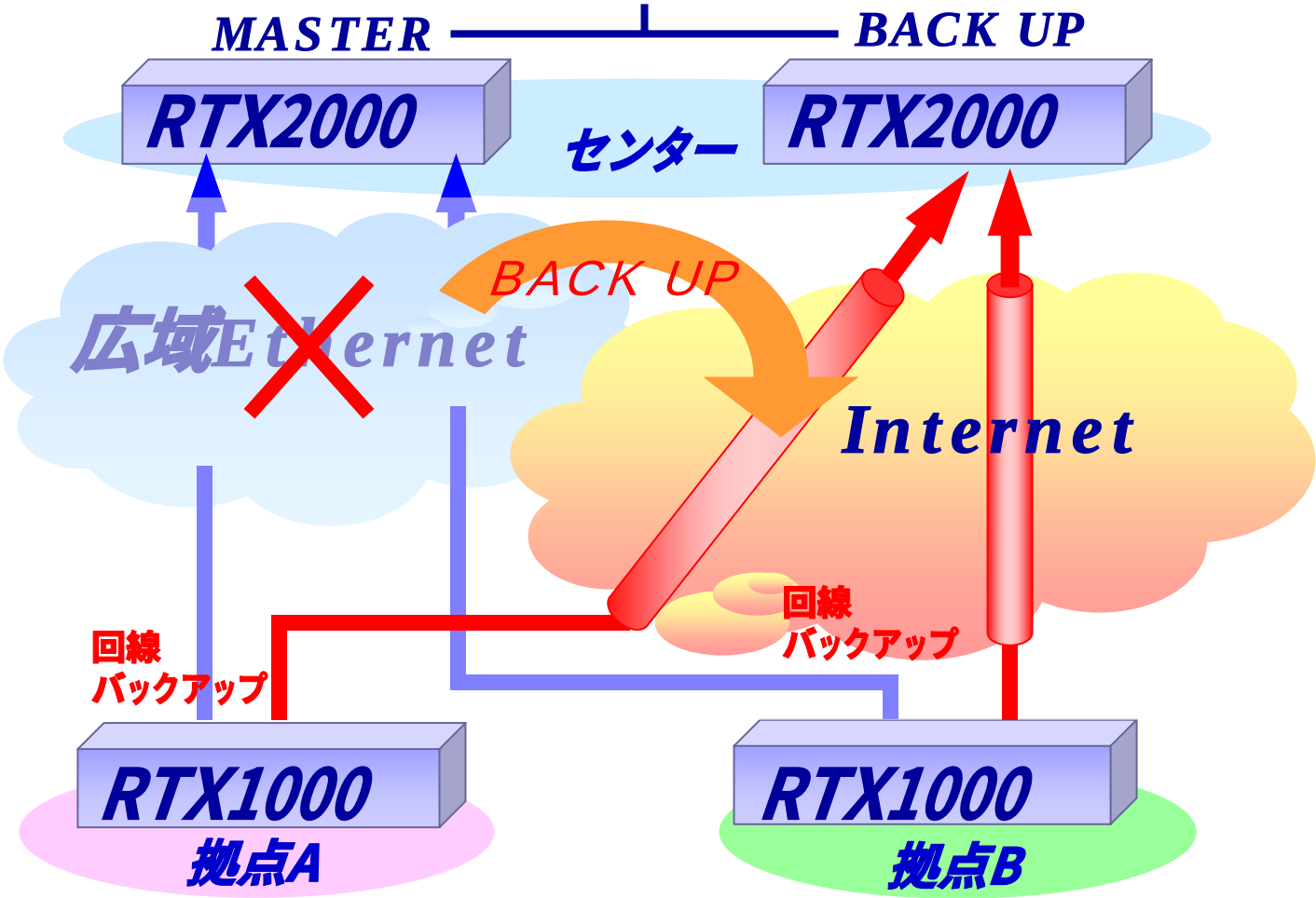
	fast switching (max)	process switching (max)	**圧縮** performance (software)	**暗号化** performance (software)
1720/1750	8.4k pps			
1721	12k pps			
2610-2612	15k pps		256k bps	512k bps
2620/2621	25k pps		384k bps	768k bps
2650/2651	37k pps		384k bps	768k bps
2610/2611XM	20k pps			
2620/2621XM	30k pps			
2650/2651XM	40k pps			
2691	70k pps			
3620	30〜40k pps	2k pps	512k bps	1024k bps
3640	50〜70k pps	4k pps	1024k bps	2048k bps
3660	100〜120k pps	10〜12k pps	1554k bps	3072k bps
4000	14k pps	1.8k pps		
4500	45k pps	3.5k pps		
4700	75k pps	4.6k pps		
720x (NPE100)	100k pps			
720x (NPE150)	150k pps	5k pps		
7500/RSP2	220〜250k pps	8k pps		
7500/RSP4	320〜350k pps	18k pps		

※インターネット検索による調査 (2002年10月)

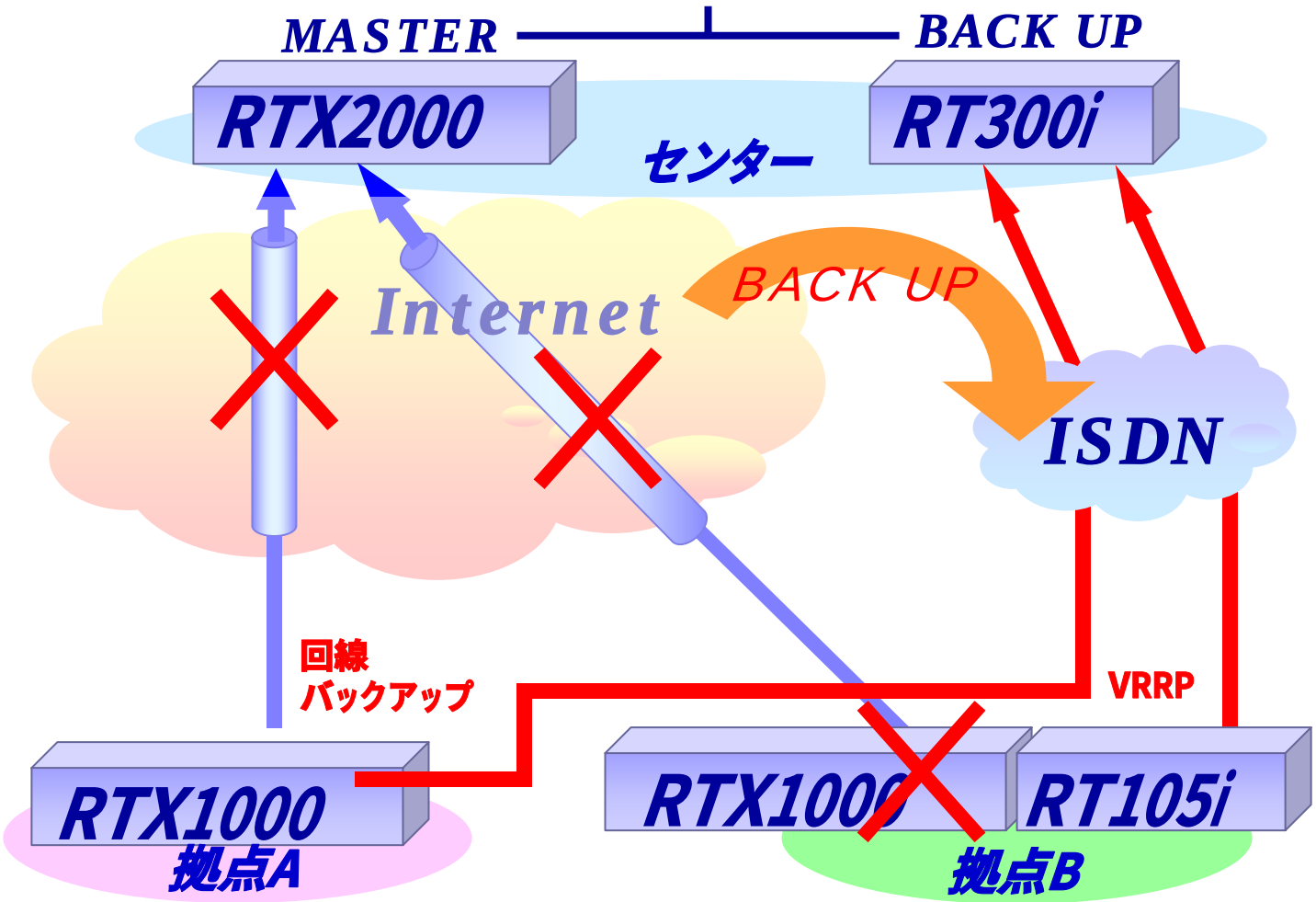
バックアップ・ソリューション

・広域Ethernet
・インターネットVPN
・IP-VPN

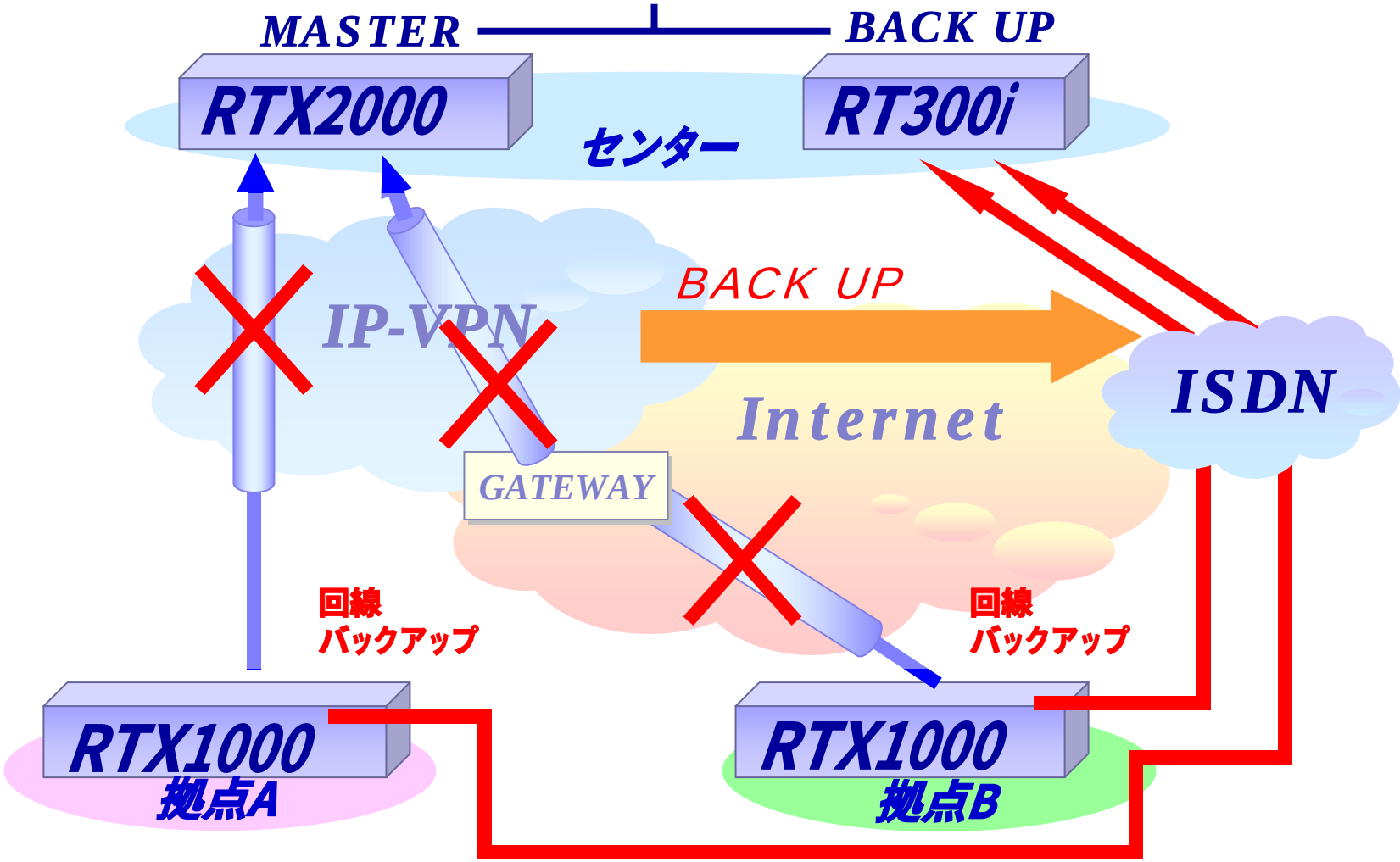
広域Ethernet 構築図



Internet VPN 構築図



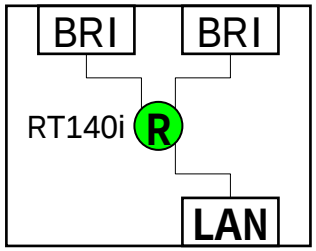
IP-VPN 構築図



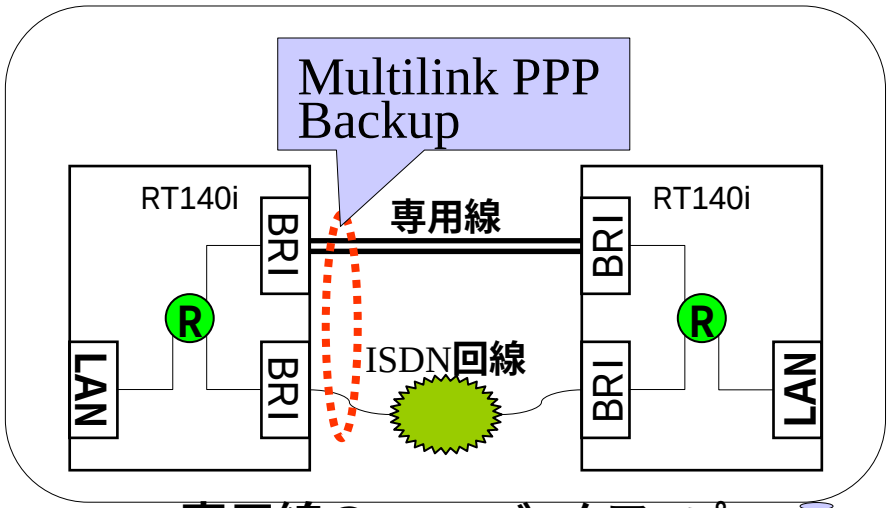
企業は 切れないネットワーク を望んでいる

切れたら大騒ぎ

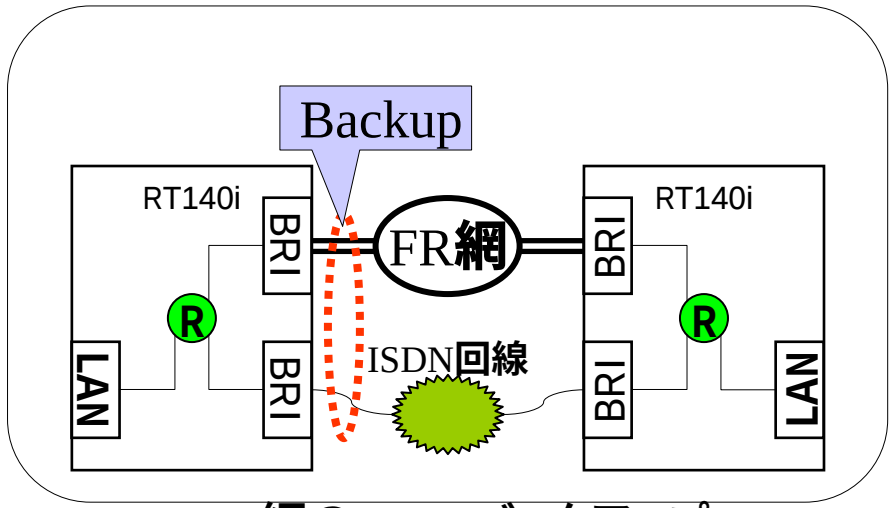
信頼と実績のRT140i(ISDNバックアップの定番)



[RT140i]
・1997年10月発売
・LAN: 1ポート(10BASE-T/100BASE-TX)
・BRI: 2ポート



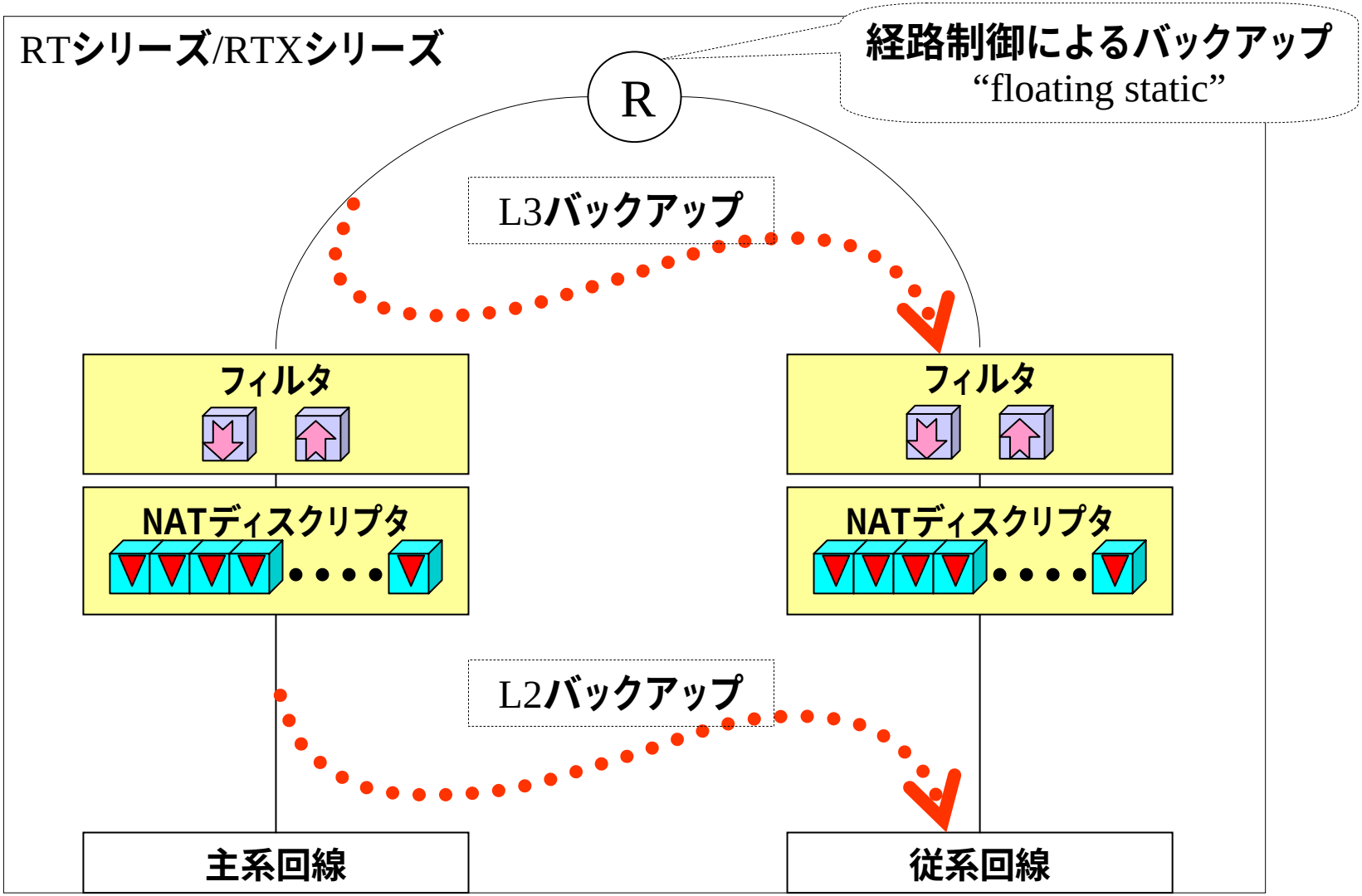
専用線のISDNバックアップ



FR網のISDNバックアップ

異常課金も大騒ぎ

「floating static」と「L2/L3バックアップ」



※概念を説明するためのイメージ図です。

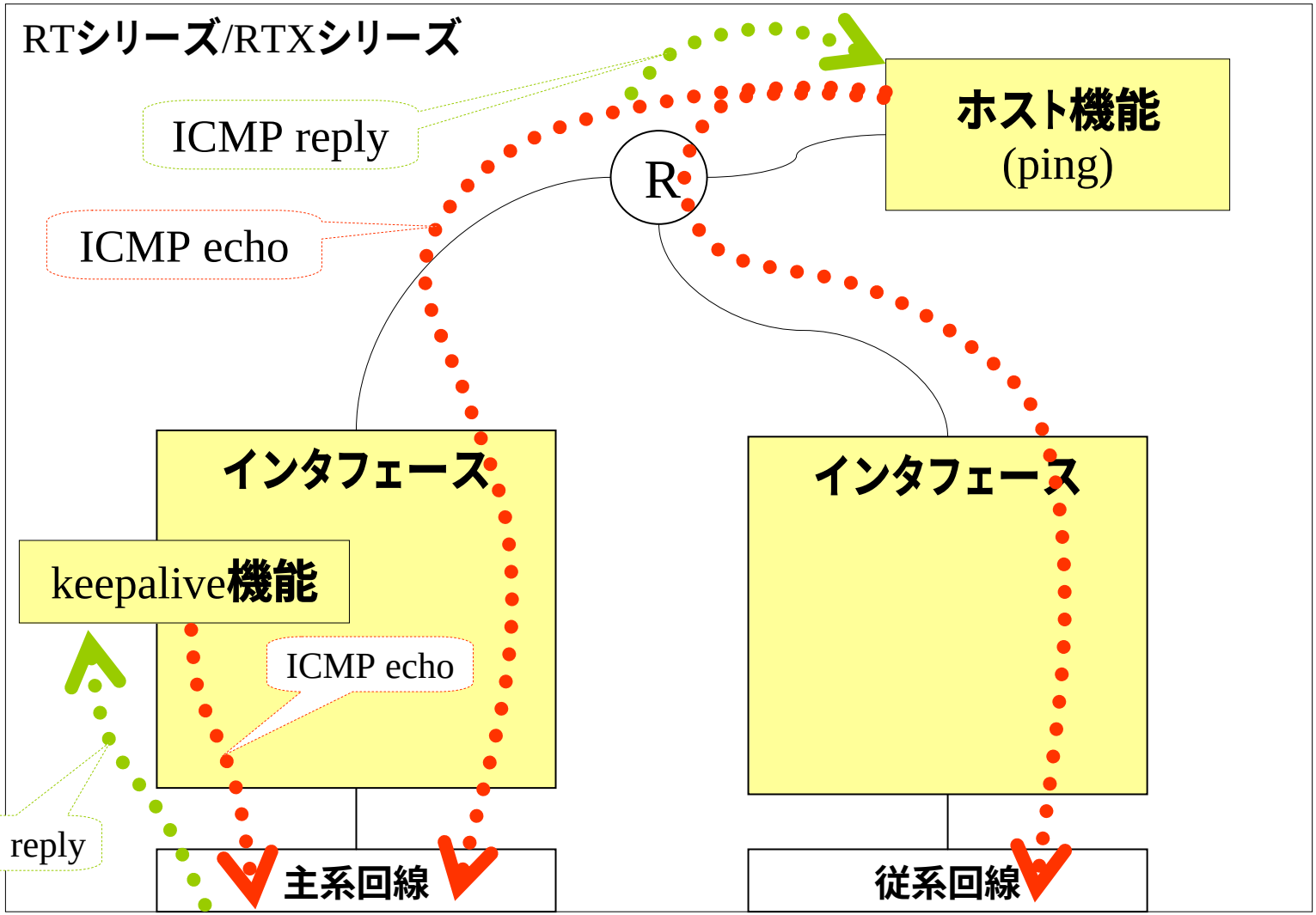
回線バックアップ方式の一覧

Layer	機能	主系回線	検出方法	従系回線
経路制御	floating static	・**動的経路情報**	・**経路情報の交換～消滅**	○**静的経路情報**
L3 (**独自**)	pp backup	・PPP ・PPPoE	・LCP keepalive ・ICMP keepalive	○PP ○LAN ●tunnel
	lan backup	・ethernet	・ARP keepalive ・ICMP keepalive	○PP ○LAN ●tunnel
	tunnel backup	・IPsec	・IKE keepalive(heartbeat) ・ICMP keepalive	●PP ●LAN ●tunnel
L2 (**独自**)	leased backup	・**専用線**	・LCP keepalive	○ISDN
	fr backup	・FR**網**	・PVC**状態確認手順**	○ISDN
	tunnel backup	・IPsec	・IKE keepalive(heartbeat)	○ISDN (**廃止**)

※VRRP**は機器をバックアップする仕組みです。**

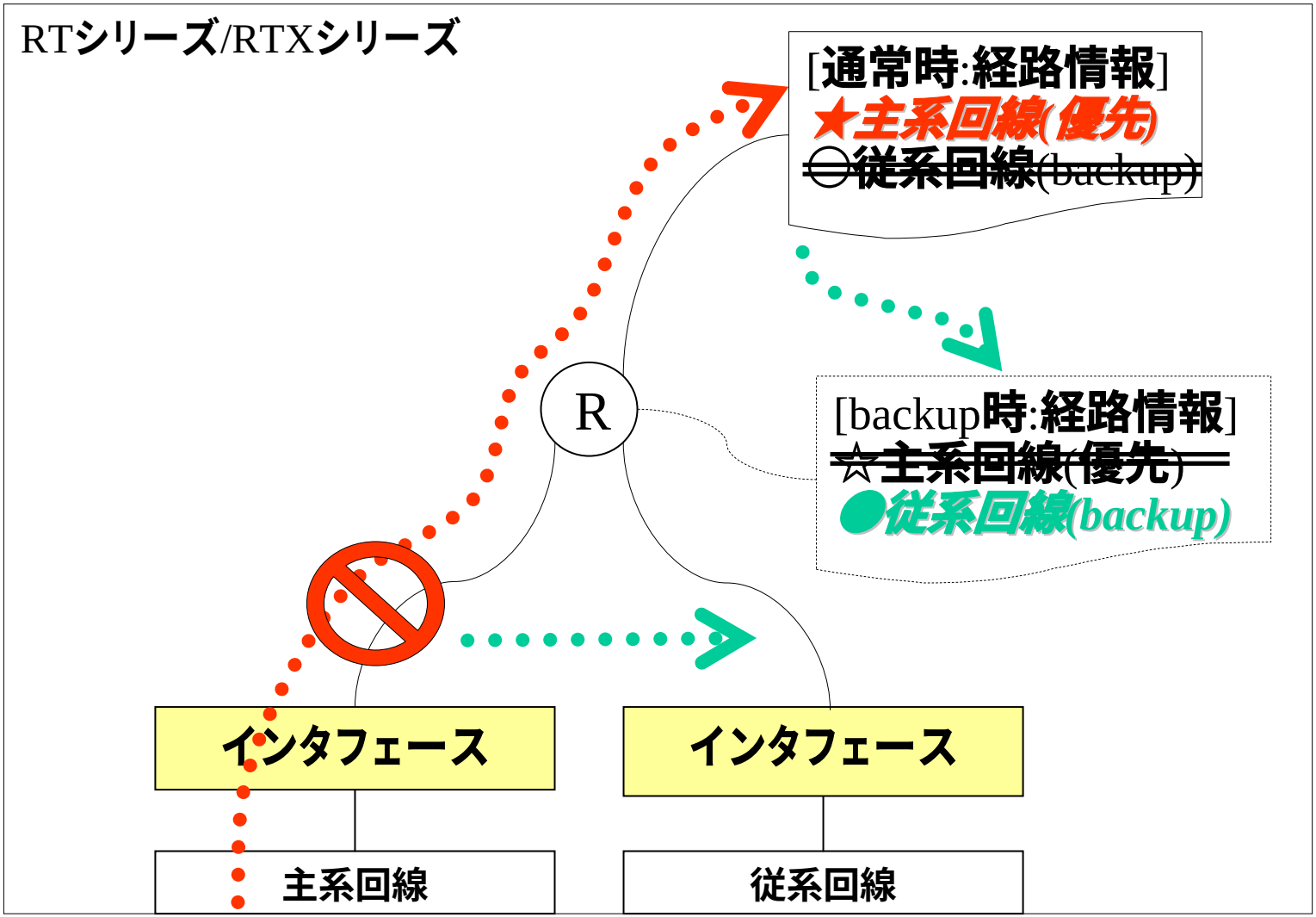
○: **機能提供済み**
●: **機能提供予定** (Rev.6.03.15**以降**)

“ICMP echo/reply”によるpingとkeepalive機能



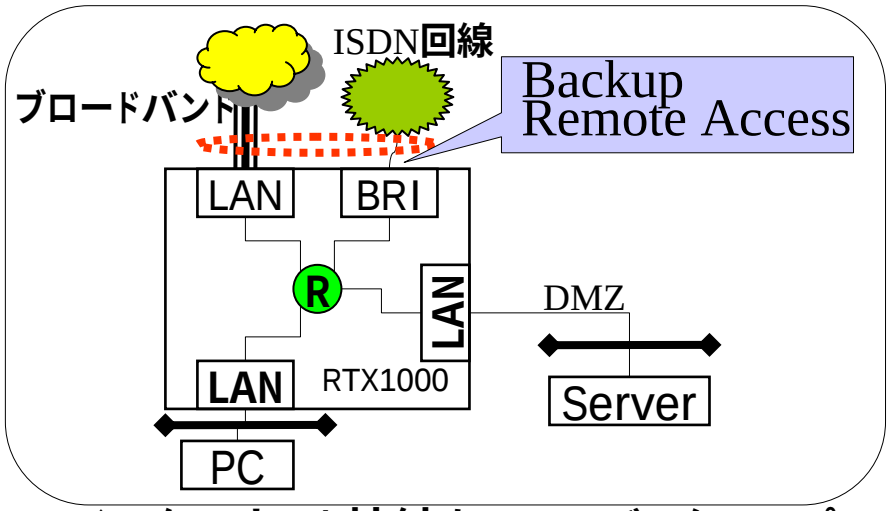
※概念を説明するためのイメージ図です。

floating static (動的経路→静的経路)

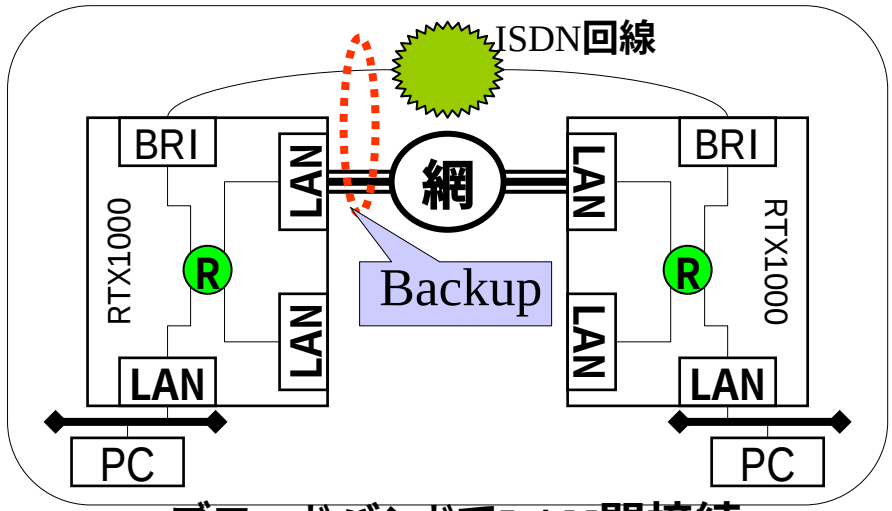


※概念を説明するためのイメージ図です。

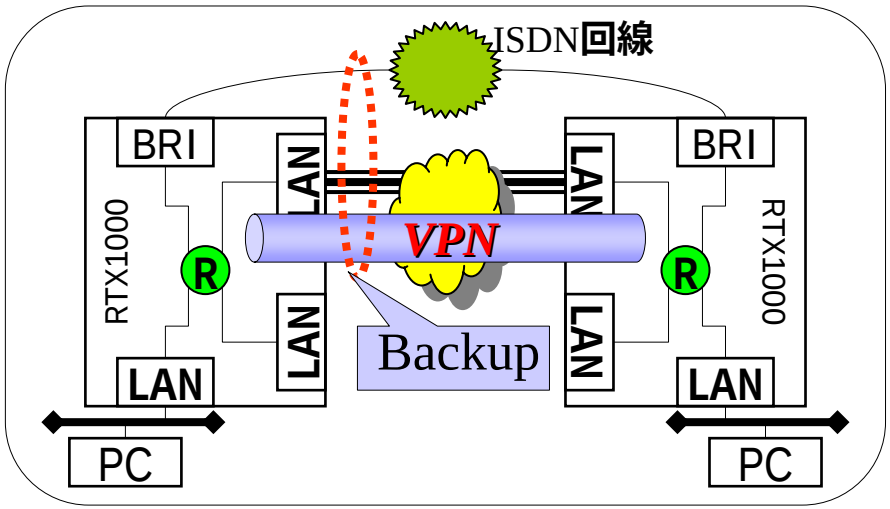
ISDNバックアップ



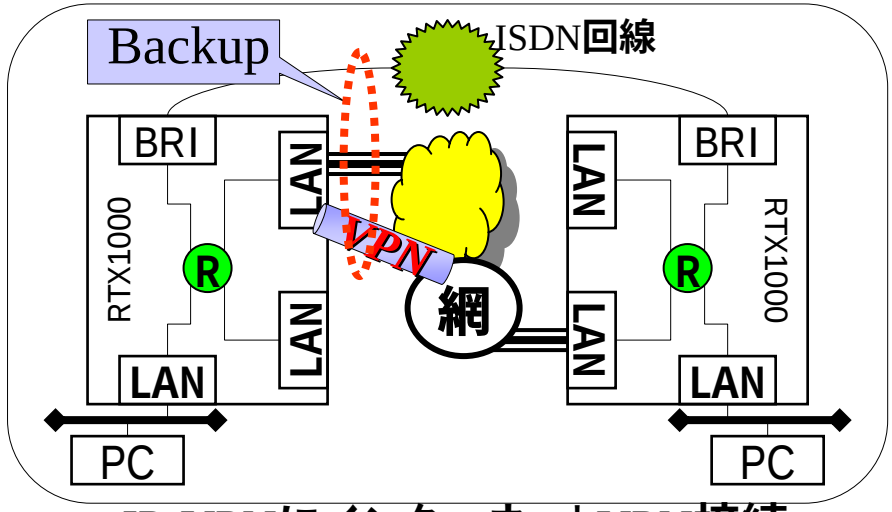
インターネット接続をISDNバックアップ



ブロードバンドでLAN間接続

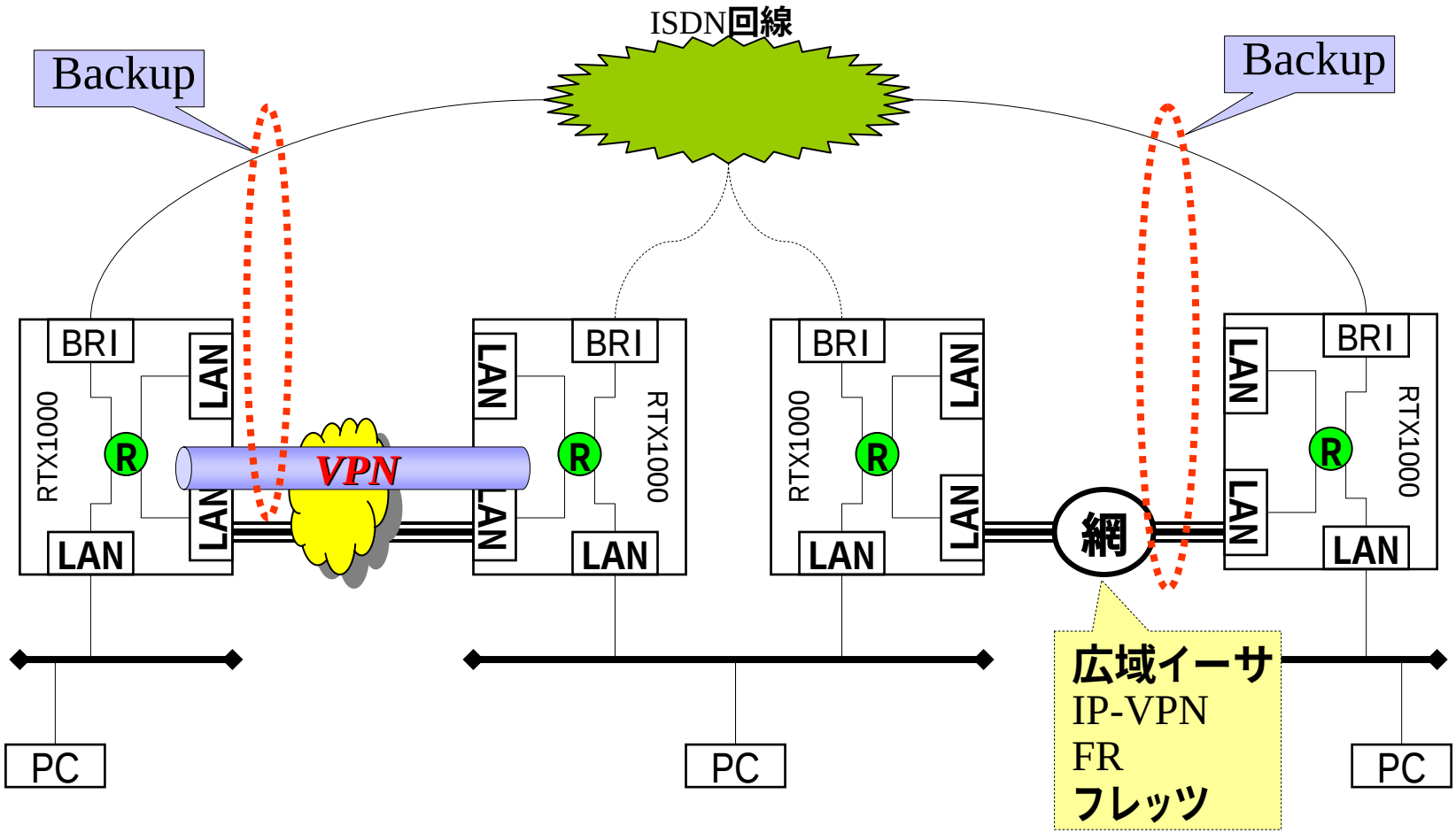


ブロードバンドでLAN間接続VPN



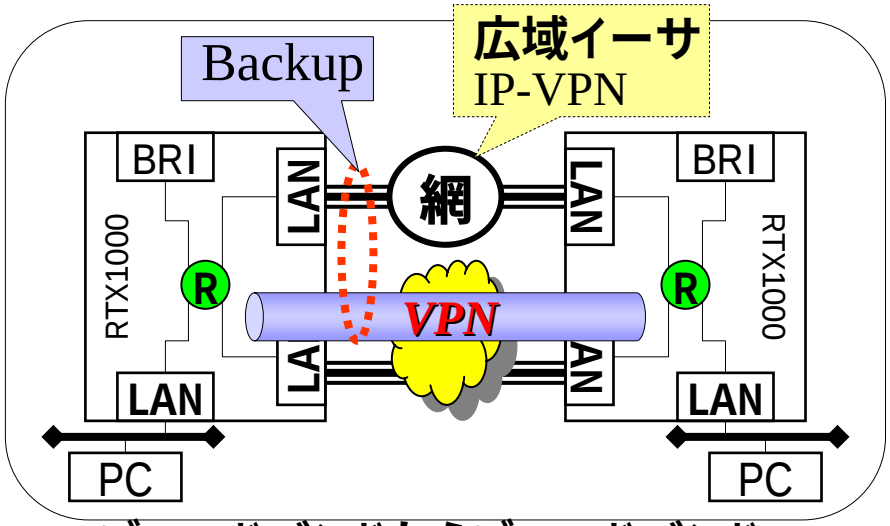
IP-VPNにインターネットVPN接続

ISDNバックアップ(複合)

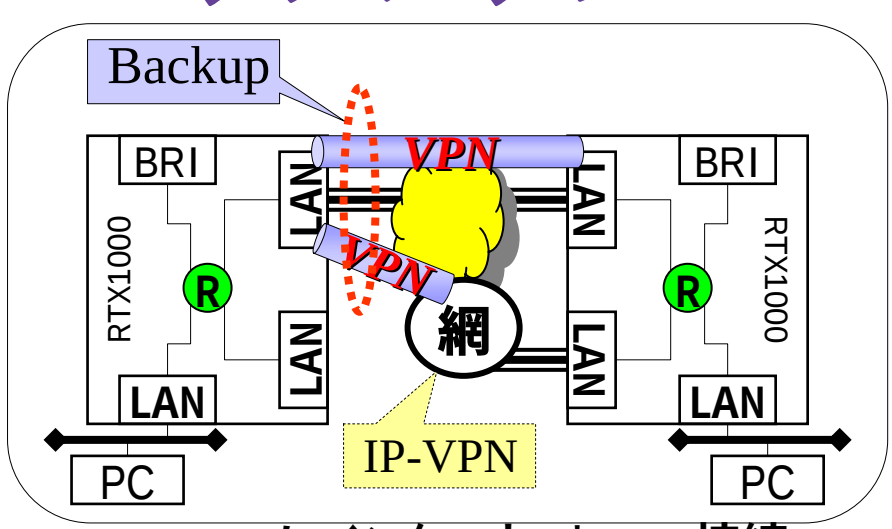


飛び越えてISDNバックアップ

ブロードバンド・バックアップ

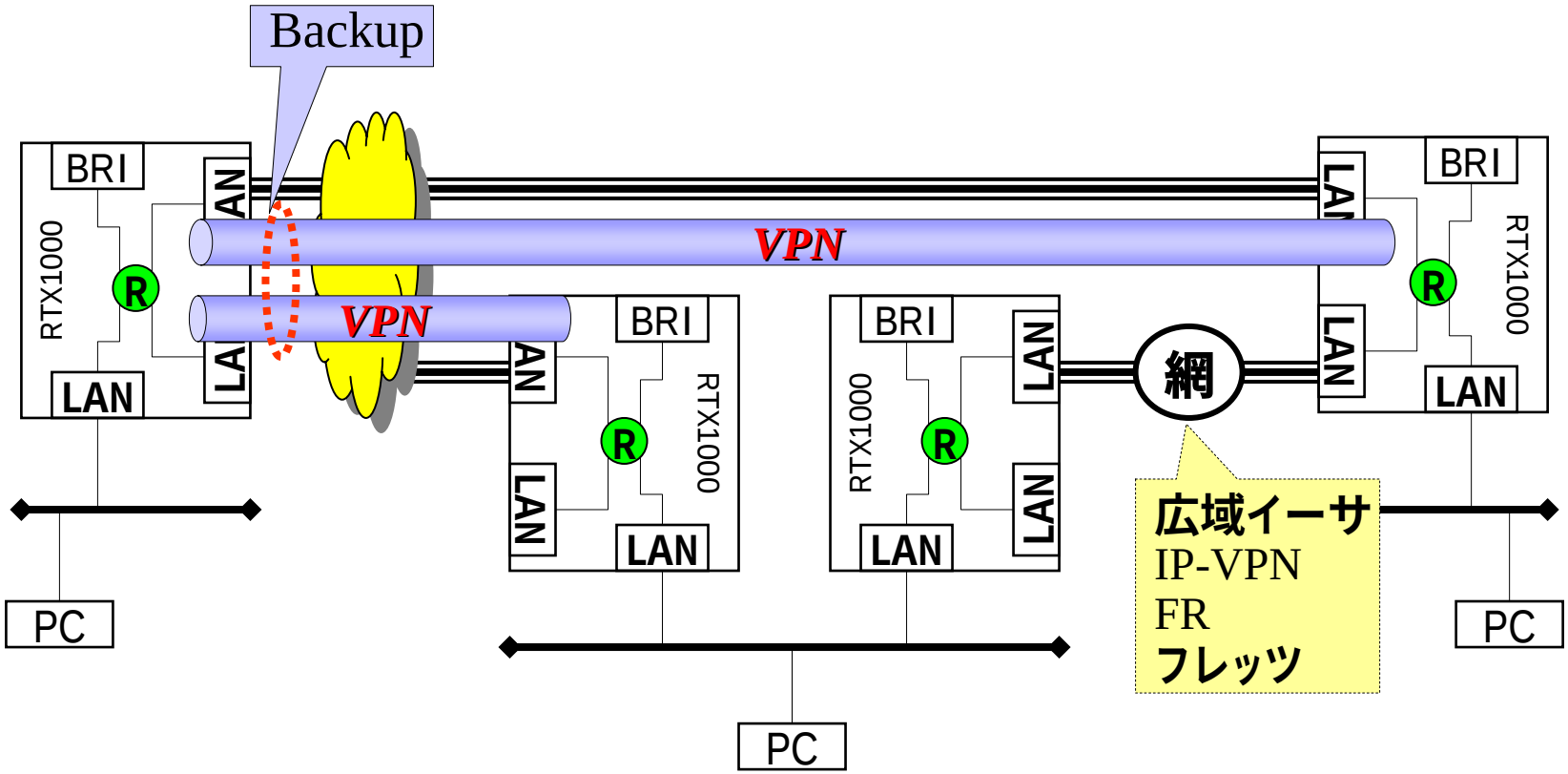


ブロードバンドからブロードバンドへ



IP-VPNにインターネットVPN接続

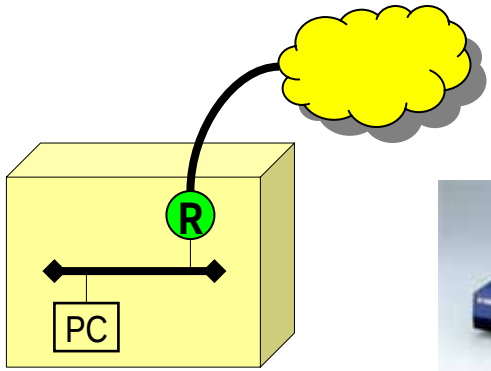
ブロードバンドバックアップ(複合)



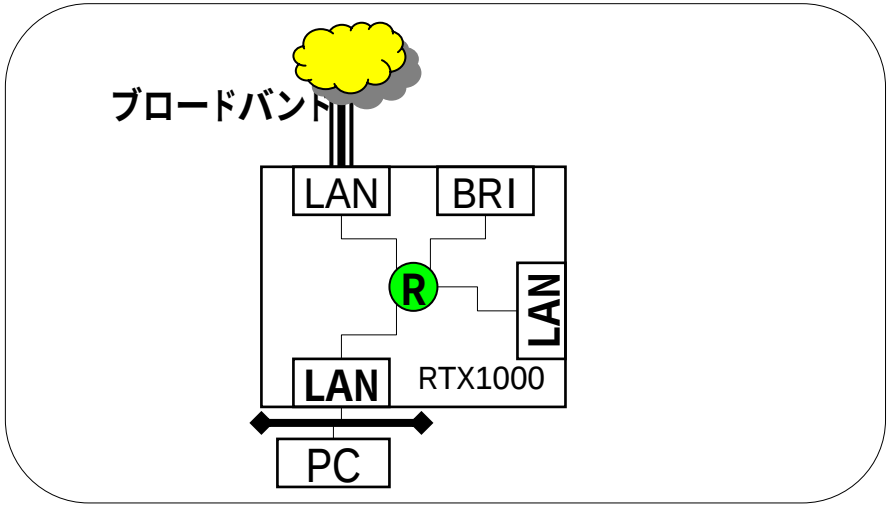
飛び越えてVPNバックアップ

いろいろな使い方

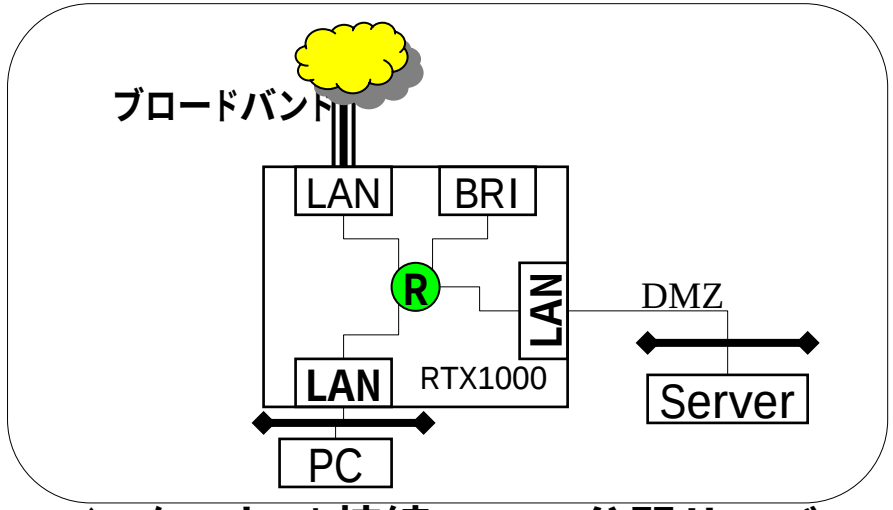
- インターネット接続
- 拠点間接続



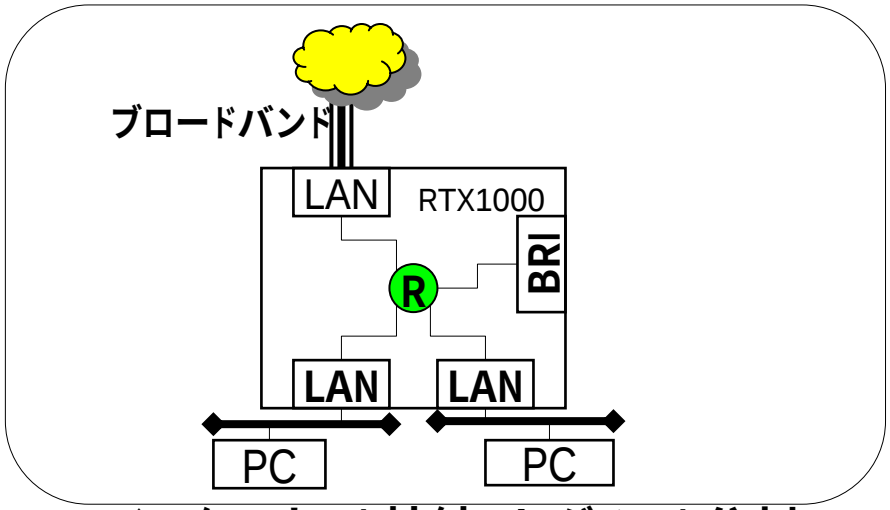
LANポートの使い方



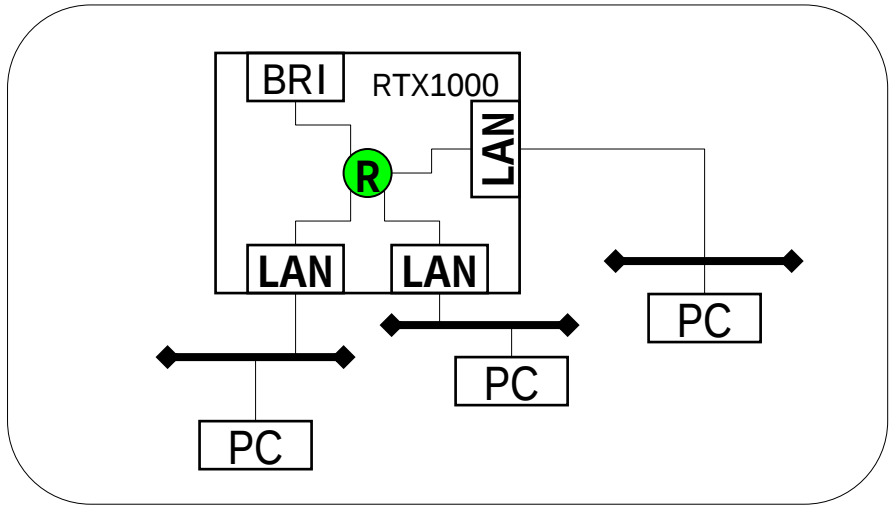
インターネット接続



インターネット接続+DMZ(公開サーバ)

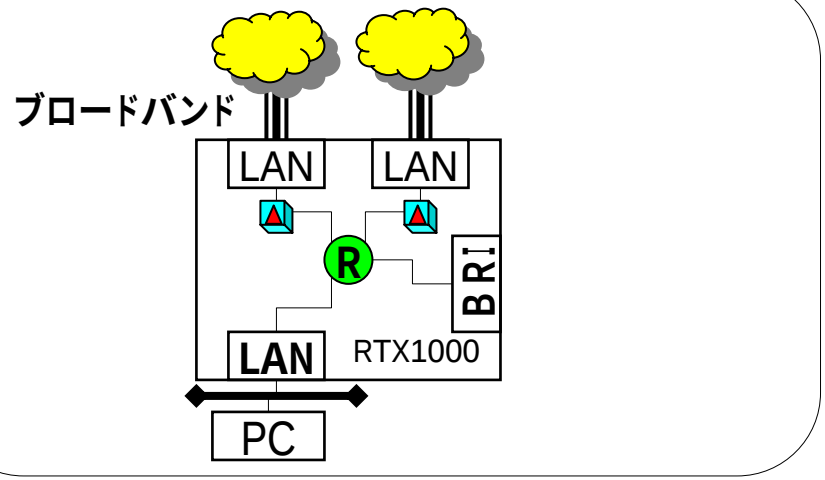


インターネット接続+セグメント分割

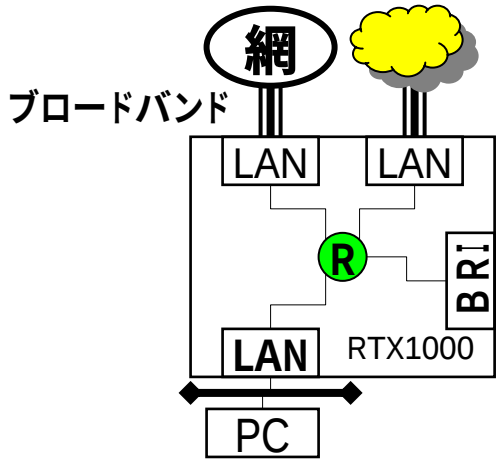


内部のセグメント分割

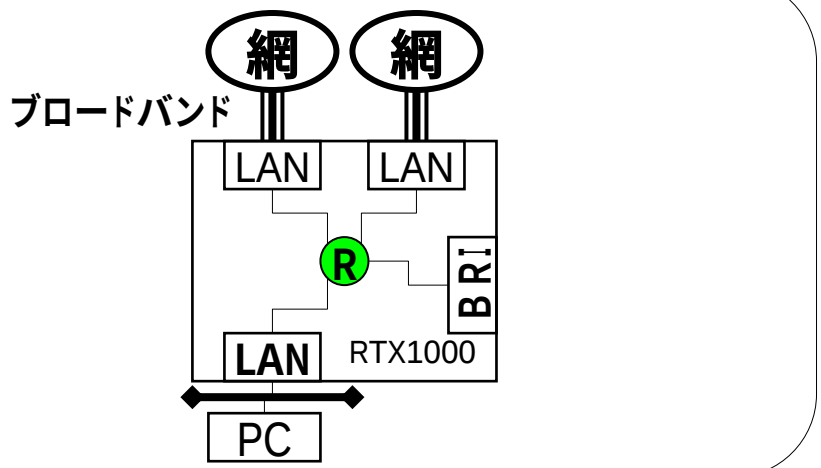
LANポートの使い方(WAN接続)



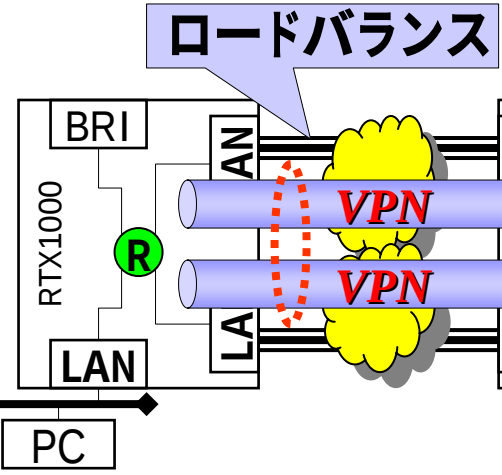
インターネット接続のマルチホーミング



ブロードバンド回線の複数収容

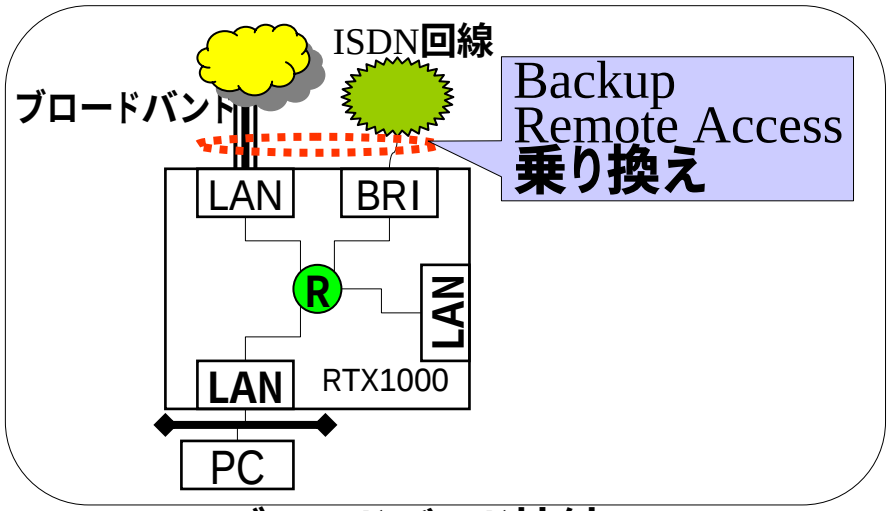


ブロードバンド回線の複数収容

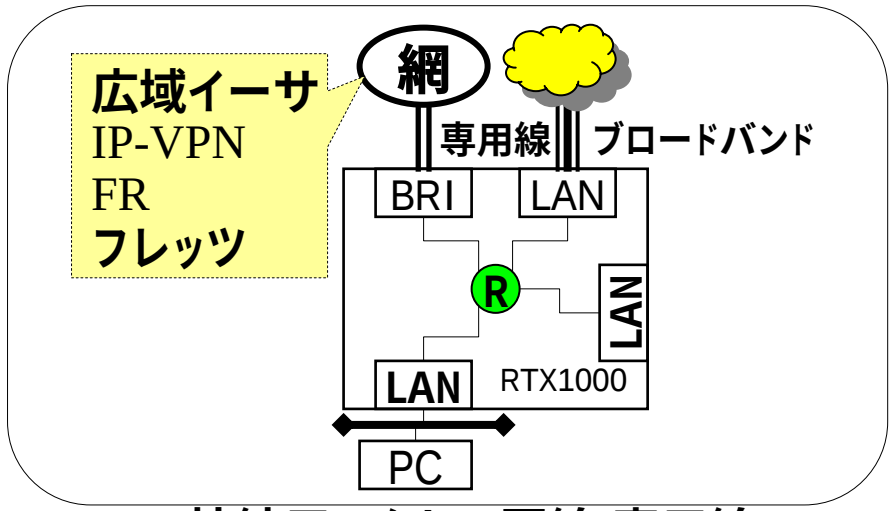


インターネットVPNのマルチホーミング

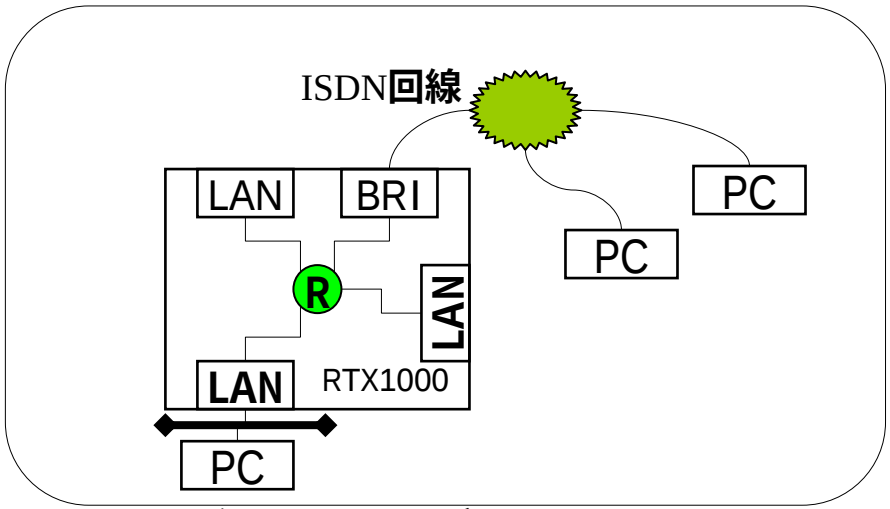
ISDNポートの使い方



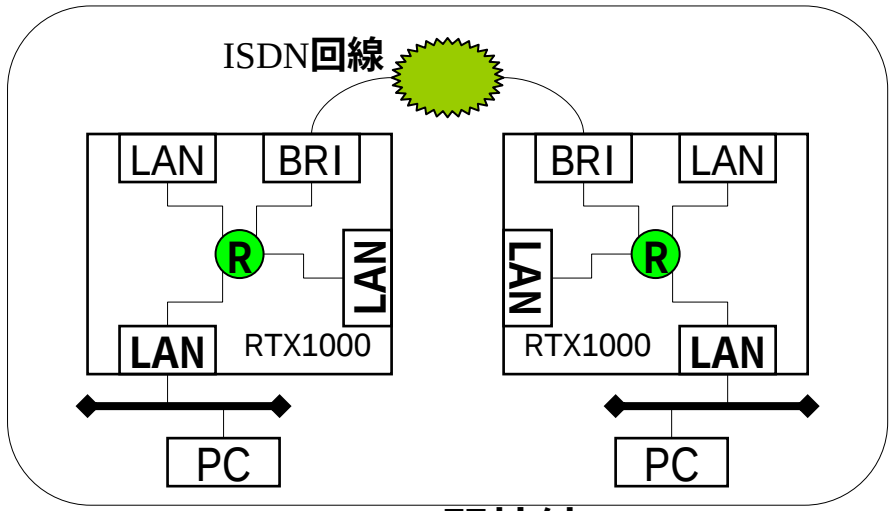
ブロードバンド接続+ α



～接続用アクセス回線(専用線)



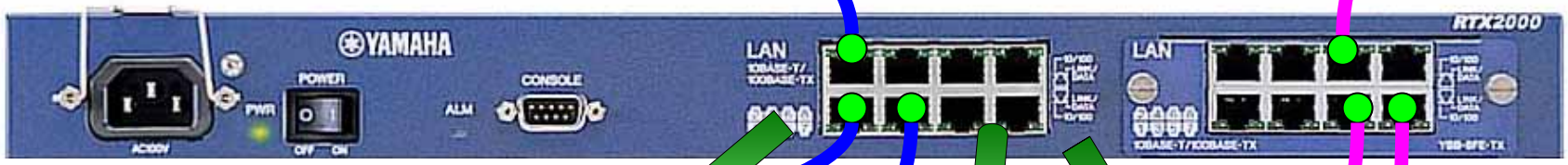
リモートアクセスサーバ(ISDN,PHS,FOMA…)



LAN間接続

「Lobby Spot!?」

網



VPN

VPN

VPN

VPN

来客

Server

PC-A
無線LAN

Server

PC-B
無線LAN

顧客PC
無線LAN

分離

移動
(来客)

PC-B'
無線LAN

AP

AP

AP

開発

営業

Lobby

無線LANは、どこでも、*パブリック・ゾーン*。

イーサアクセスVPNルーターで、*セキュリティ*と*顧客サービス*の両立

RTシリーズの蓄積されたノウハウがブロードバンドで活きる

次世代イーサアクセスVPNルーター

RTX series

高速性 & *高機能性*

RTX2000 2002年11月5日発売

RTX1000 2002年10月22日発売

広域イーサネット、インターネットVPN 、IP-VPNなど
幅広いWANサービスに適応。

YAMAHA

こんなところにヤマハが…

- NHKの朝ドラ(ちょっと古い)
- サッカー
- 携帯電話
- …

御静聴ありがとうございました

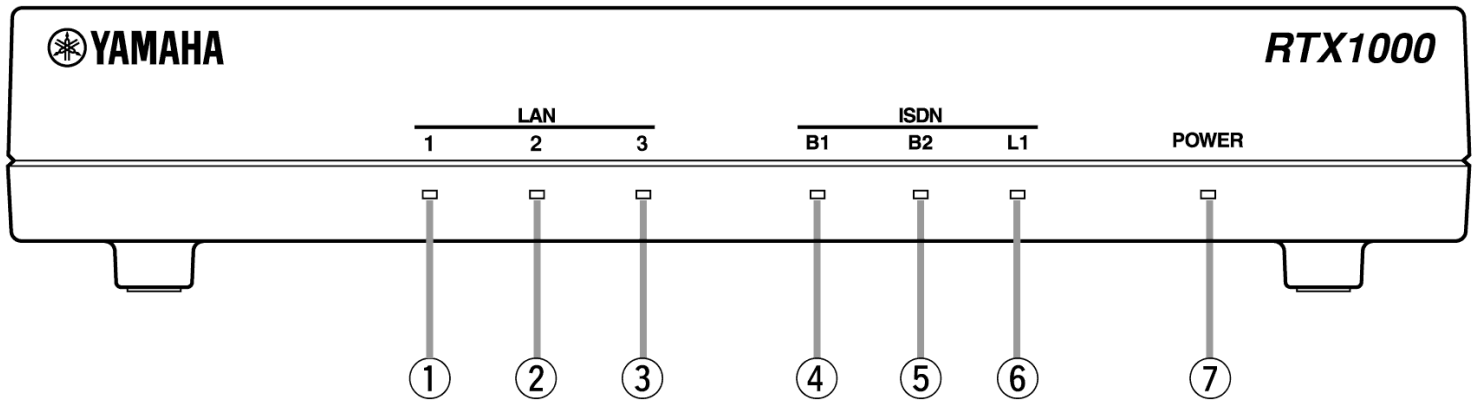
RTXシリーズ仕様

- RTX1000
- RTX2000

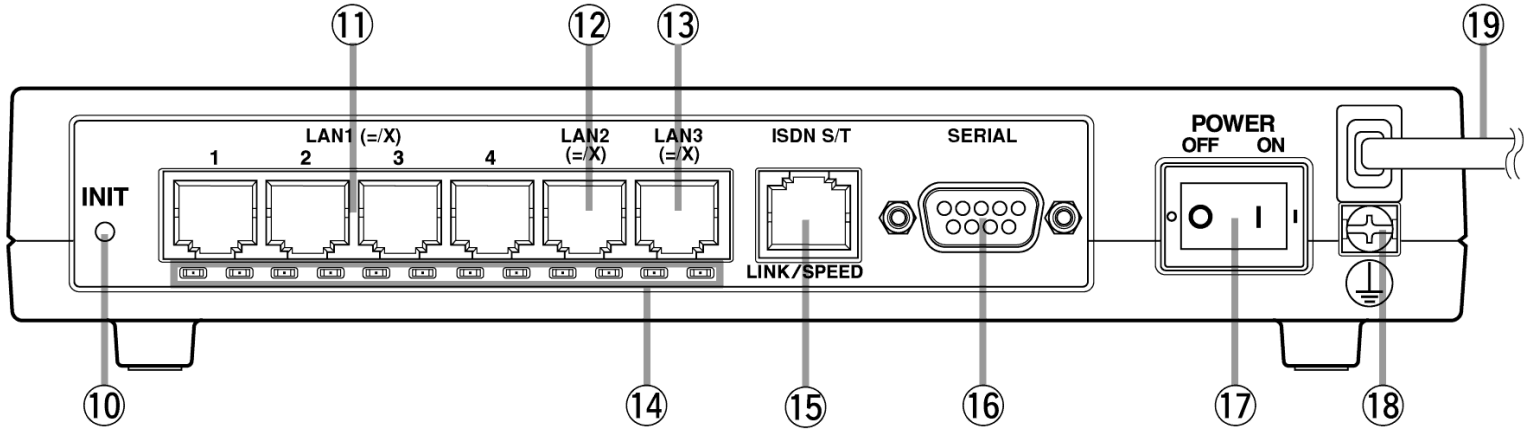
RTX1000仕様

対応回線	ADSL、CATV、FTTH（光ファイバー）、ISDN、高速デジタル専用線、 IP-VPN網、フレームリレー網、広域イーサネット網
動作環境	周囲温度0～40℃、周囲湿度15～80%（結露しないこと）
電源	AC100V（50/60Hz）
定格消費電力	7W(0.12A)
電波障害規格	VCCI　クラスA
外形寸法、重量	220(W)×141.5(D)×42.6(H)mm、 750g
付属品	取扱説明書、コマンドリファレンス、設定例集、保証書
スループット	最大100Mbit/s（3DES：最大23Mbit/s）
IPv6接続形式	ネイティブ、トンネル(IPv4 over IPv4, IPv6 over IPv4, IPv4 over IPv6, IPv6 over IPv6)、デュアルスタック
ルーティング対象プロトコル	IP、IPv6（ブリッジとIPXは除く）
IPルーティングプロトコル	RIP、RIP2、OSPF、BGP4
IPv6ルーティングプロトコル	RIPng
WANプロトコル	PPP、PPPoE、MP、フレームリレー
認証機能	RADIUS、PAP/CHAP/MS-CHAPv1/MS-CHAPv2、ISDN識別着信、 コールバック（無課金独自方式、Windows標準方式）
管理機能	SNMP、syslog
ファームウェアアップデート	TFTPによるアップデート（最新プログラムはホームページ上に公開）
設定手段	シリアル、TELNET、TFTPでのダウンロード/アップロード可、遠隔地のRTシリーズルーターよりISDN回線経由のリモートセットアップ
セキュリティ	ファイアウォール機能（静的/動的パケットフィルタリング、不正アクセス検知）、VPN（IPsec、PPTP）、ステルス機能
アドレス変換機能 (NATディスクリプタ機能)	NATディスクリプタ（NAT、IPマスカレード拡張機能）、静的IPマスカレード、PPTPパススルー(複数セッション)、IPsecパススルー(1セッション)、NetMeeting対応、FTP対応、traceroute対応、ping対応
障害冗長構成機能	VRRP
バックアップ機能	主回線断検出後、ISDNにバックアップ、VPNにバックアップ、イーサにバックアップ
その他の機能	CIDR、ProxyARP、DHCPサーバー/リレーエージェント/クライアント、DNSリカーシブサーバー、DNSサーバー選択機能、NTPクライアント、LAN側セカンダリアドレス設定、PIAFS 32k/64k、BOD(MP、BACP)、フィルタ型ルーティング、リモートアクセスサーバー、マルチホーミング、スケジューリング機能

RTX1000 [前面と背面]



①LAN1ランプ、②LAN2ランプ、③LAN3ランプ、④B1ランプ、⑤B2ランプ、⑥L1ランプ、
⑦POWERランプ、⑧INITボタン、⑨LAN1ポート、⑩LAN2ポート、⑪LAN3ポート、
⑫LINK/SPEEDランプ、⑬ ISDN S/T (BRI) ポート、⑭SERIALコネクタ、⑮POWERスイッチ、
⑯GND端子、⑰電源コード

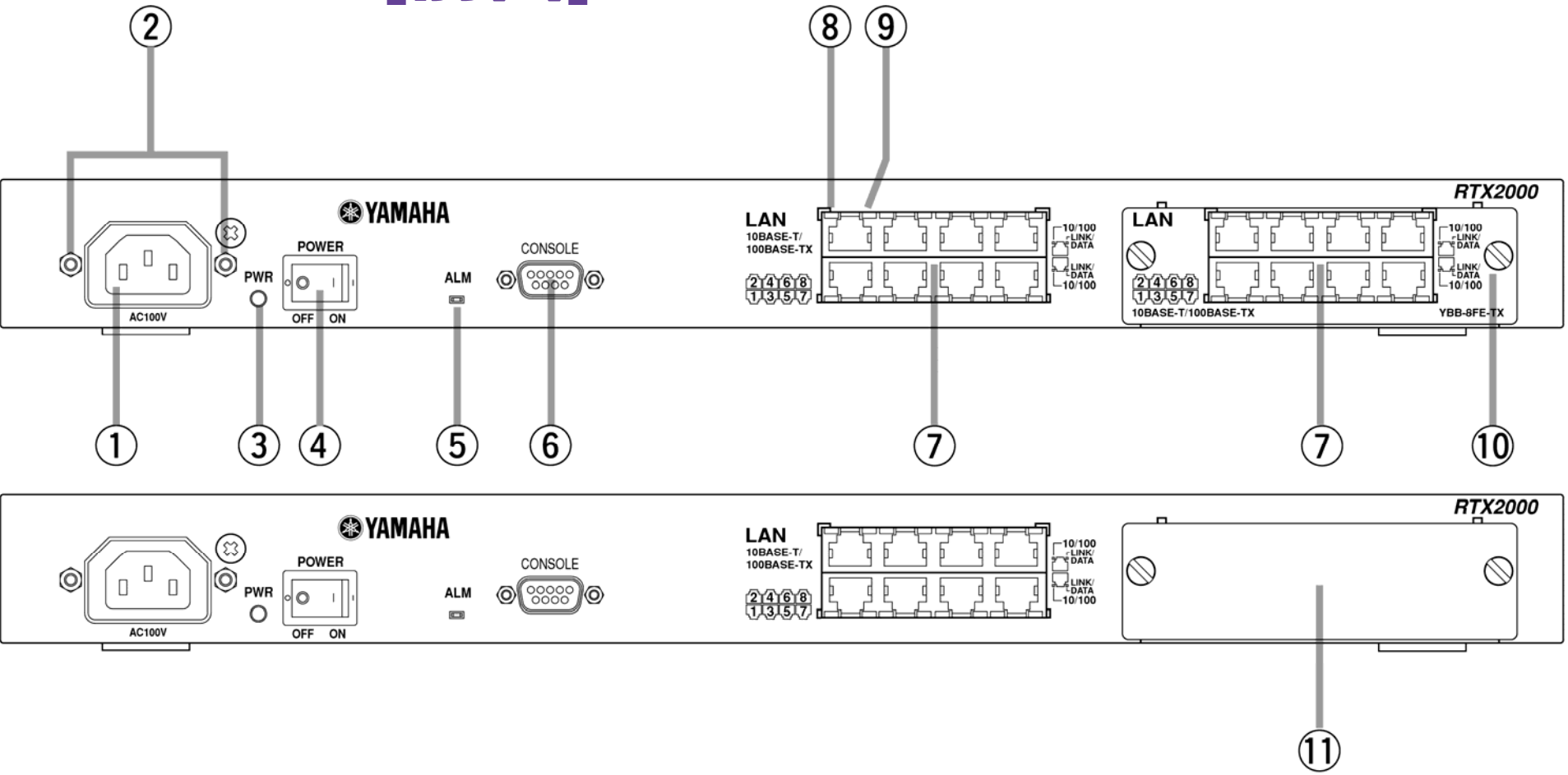


RTX2000仕様

品番	RTX2000
対応回線※	ADSL、CATV、FTTH（光ファイバー）、IP-VPN網、広域イーサネット網
動作環境	周囲温度0～40℃、周囲湿度20～85%（結露しないこと）
電源	AC100V (50/60Hz)
定格消費電力	0.35A
電波障害規格	VCCI クラスA
外形寸法、重量	445 (W) × 295 (D) × 43.7 (H) mm、 4.0kg
付属品	取扱説明書、コマンドリファレンス、設定例集、保証書
スループット	最大500Mbit/s (3DES：最大50Mbit/s)
IPv6接続形式	ネイティブ、トンネル(IPv4 over IPv4, IPv6 over IPv4, IPv4 over IPv6, IPv6 over IPv6)、デュアルスタック
ルーティング対象プロトコル	IP、IPv6（ブリッジとIPXは除く）
IPルーティングプロトコル	RIP、RIP2、OSPF、BGP4
IPv6ルーティングプロトコル	RIPng
WANプロトコル	PPPoE
認証機能	PAP/CHAP
管理機能	SNMP、syslog
ファームウェアアップデート	TFTPによるアップデート（最新プログラムはホームページ上に公開）
設定手段	シリアル、TELNET、TFTPでのダウンロード/アップロード可
セキュリティ	ファイアウォール機能（静的/動的パケットフィルタリング）、VPN（IPsec）、ステルス機能
アドレス変換機能 (NATディスクリプタ機能)	NAT、IPマスカレード、静的NAT、静的IPマスカレード、DMZホスト機能、PPTPパススルー(1セッション)、IPsecパススルー(1セッション)、NetMeeting対応、FTP対応、traceroute対応、ping対応
障害冗長構成機能	VRRP
バックアップ機能	主回線断検出後、VPNにバックアップ、イーサにバックアップ
その他の機能	CIDR、ProxyARP、DHCPサーバー/リレーエージェント/クライアント、DNSリカーシブサーバー、DNSサーバー選択機能、NTPクライアント、LAN側セカンダリアドレス設定、スケジューリング機能

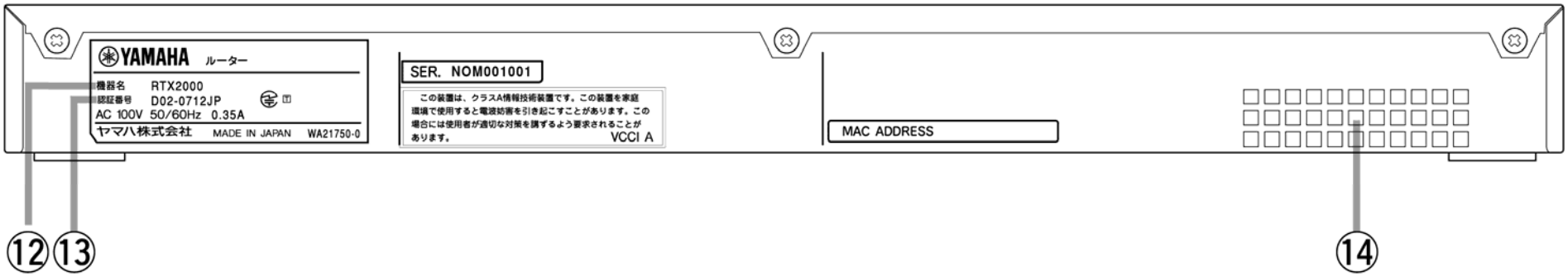
※ADSL、CATV、FTTH（光ファイバー）回線との接続には別途ADSLモデム、ケーブルモデムまたはメディアコンバーターが必要です。
また、ISDN回線をご使用の場合、別途DSUが必要です。

RTX2000 [前面]

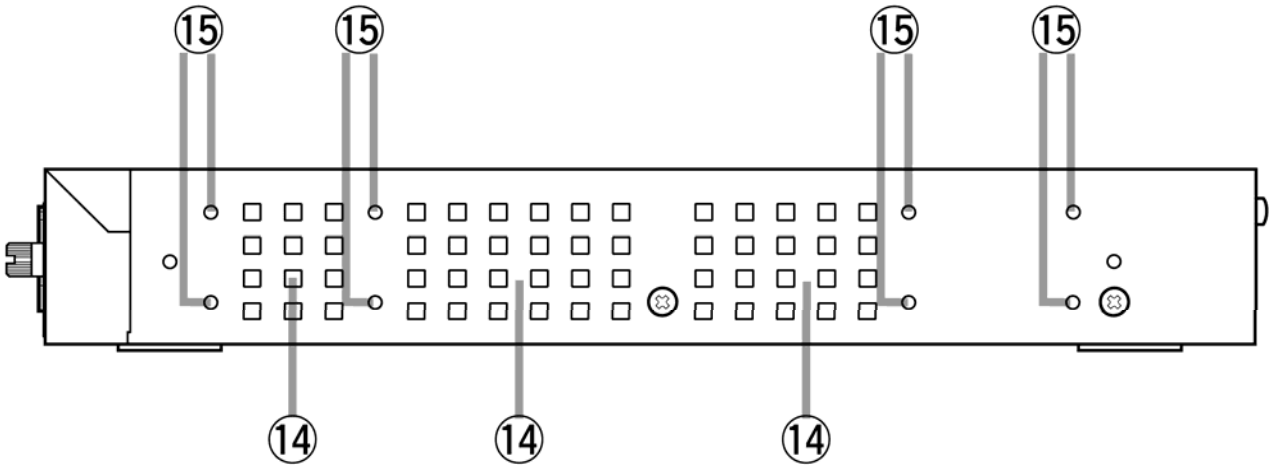


①電源インレット、②電源コード抜け防止金具、③POWERランプ、④POWERスイッチ、
⑤ALMランプ、⑥CONSOLEコネクタ、⑦LANポート、⑧10/100ランプ、⑨LINK/DATAランプ、
⑩拡張スロット、⑪ブランクカバー

RTX2000 [背面と側面]



⑫認証機器名、⑬認証番号 、⑭通風口、⑮ラック取り付け用ネジ



RTXシリーズ参考情報

○日経コミュニケーション、2002.4.1
・特集「ADSL企業ネットワーク始動」P.86〜P.105
拠点間通信にはこう生かせ
○日経コミュニケーション、2002.10.7
・特集「切れるADSL, 導入企業の奮闘」P.70〜P.87
毎日どこかの拠点が切れている
・新製品「100メガ回線対応のVPNルーター
自動バックアップ機能が充実」P.158
○N+I INTERNET Guide、2002.11
・「WAN回線の冗長化
ケース別にみる拠点間WAN接続冗長化のポイント」P.48〜P.51
○日経コミュニケーション、2002.10.21
・特集「ネットワーク単年更改に備えよ」P.110〜P.125
変わる通信サービス・機器の買い方
○日経コミュニケーション、2002.11.4
・Report「新型WANを狙い撃つ拠点ルーター」P.52〜P.53
ブロードバンド2回線に接続
切れても自動う回で障害回避

付録

・ネットボランチシリーズ
・RT/RTXシリーズ

ヤマハの通信技術の原点は、音・音楽から

キーワード	製品例
半導体の自社開発	エレクトーン(電子オルガン)
電子音源用LSI	シンセサイザー DX7
音場処理用LSI	DSP-1
ディジタルモデムLSI	9600bps FAXモデム(QFP)の外販
ISDN-LSI	LSIの外販
ISDN応用機器開発	FDわ～ぷ、ISDN-TAなど
ISDNリモートルーター	RT100i
…	…

ヤマハの通信技術

LSI開発	ISDN関連LSI開発、評価用ボード開発など
ハードウェア開発	ルーター製品開発など
ソフトウェア開発	IPv4/IPv6技術、IPv6ルーター、VoIP、VPNなど
動作検証	安定動作の検証、使いこなしノウハウの蓄積･紹介など

モジュール型VPNルーター
RT300i

ブロードバンド&VPNルーター
RT140e

ブロードバンド&小型VPNルーター
RT105e

ISDN-LSI評価ボード

ブロードバンド&ISDN
ルーター
RTA55i

ブロードバンド&ISDN
無線ルーター
RTW65i

フィルタ型ルーティング

- フィルタ型ルーティングの構造
- プロトコルによるプロバイダ選択

  メール(SMTP/POP)
- ホスト毎のプロバイダ選択
- 接続状態に応じたプロバイダ選択
- マルチホーミング(Rev.6系)

RTA50i

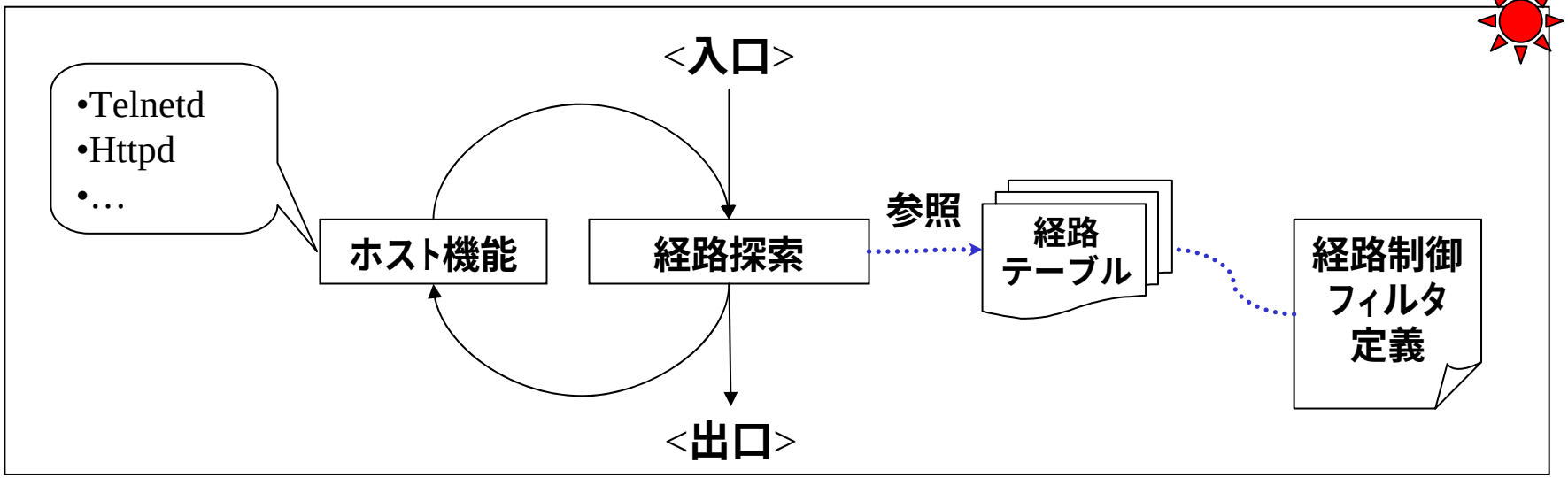
RTA52i

RTA55i

拡張

RT300i

フィルタ型ルーティングの構造



[経路を判別する内容]

☆宛先の経路

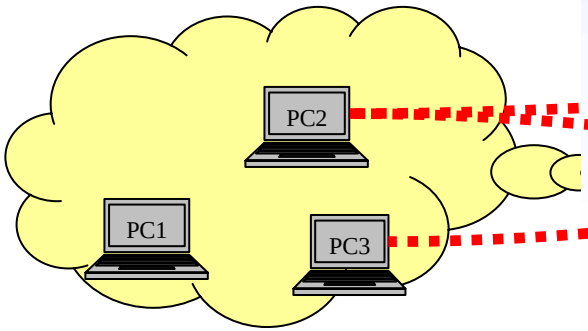
- **接続状態:pass/restrictタイプ**
- **プロトコル:tcp/udpなど**
- **IPアドレス:発信元/受信先**
- **ポート番号:発信元/受信先**

http://www.rtpro.yamaha.co.jp/RT/FAQ/TCPIP/Attic/filter-routing.html

プロトコル毎プロバイダ選択

SMTP	ISP#2
POP3	ISP#2
そのほか	ISP#1

RTA55i



WWW/FTP

通信網

電子メール

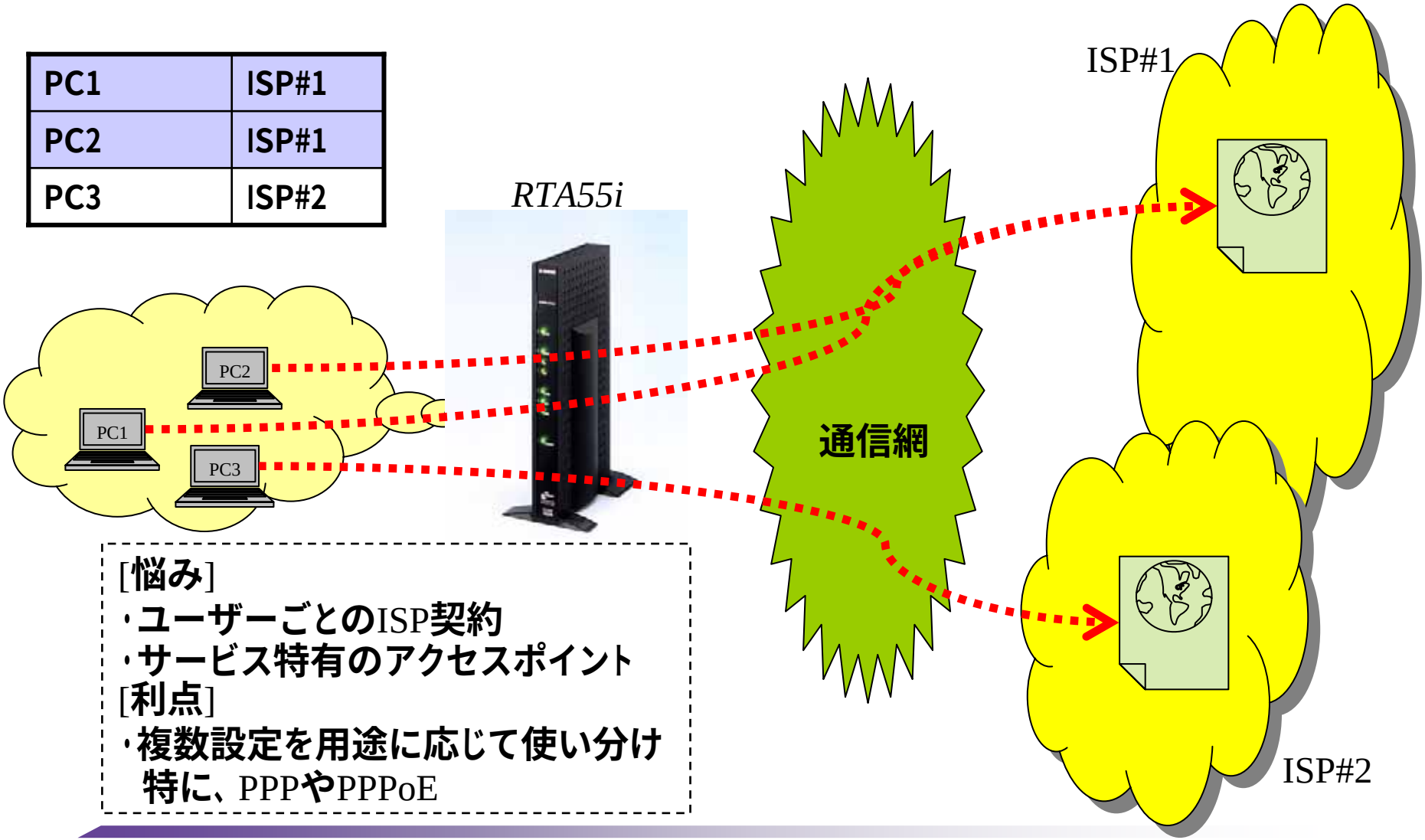
ISP#1

ISP#2

[悩み]
・サービスごとのISP契約
・サービス特有のアクセスポイント
[利点]
・複数設定を用途に応じて使い分け
　特に、PPPやPPPoE

ホスト毎プロバイダ選択

PC1	ISP#1
PC2	ISP#1
PC3	ISP#2

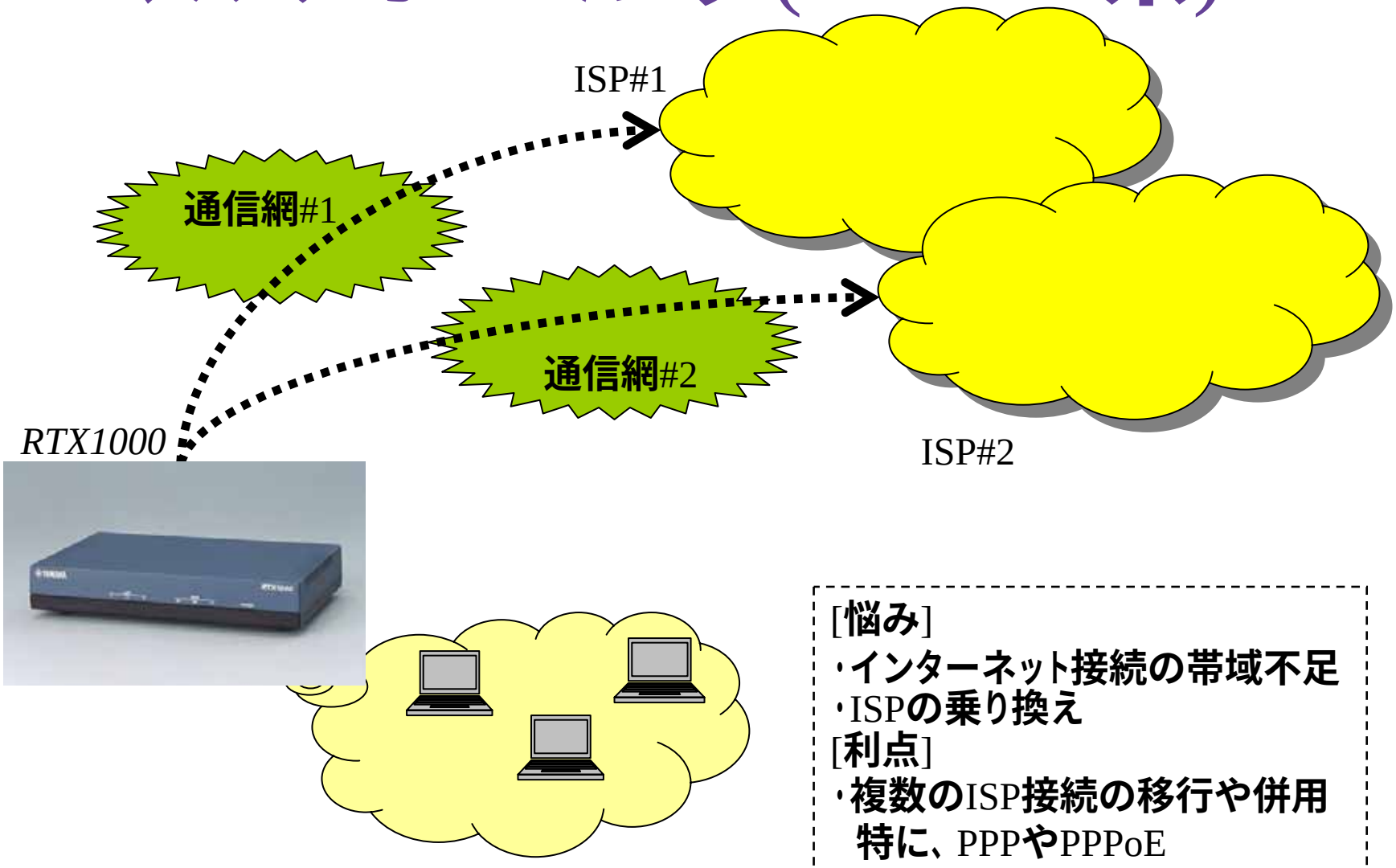


[悩み]
・ユーザーごとのISP契約
・サービス特有のアクセスポイント
[利点]
・複数設定を用途に応じて使い分け
　特に、PPPやPPPoE

接続状態に応じたプロバイダ選択

[悩み]
・インターネット接続のバックアップ
・サービス特有のアクセスポイント
[利点]
・複数設定を用途に応じて使い分け
特に、PPPやPPPoE

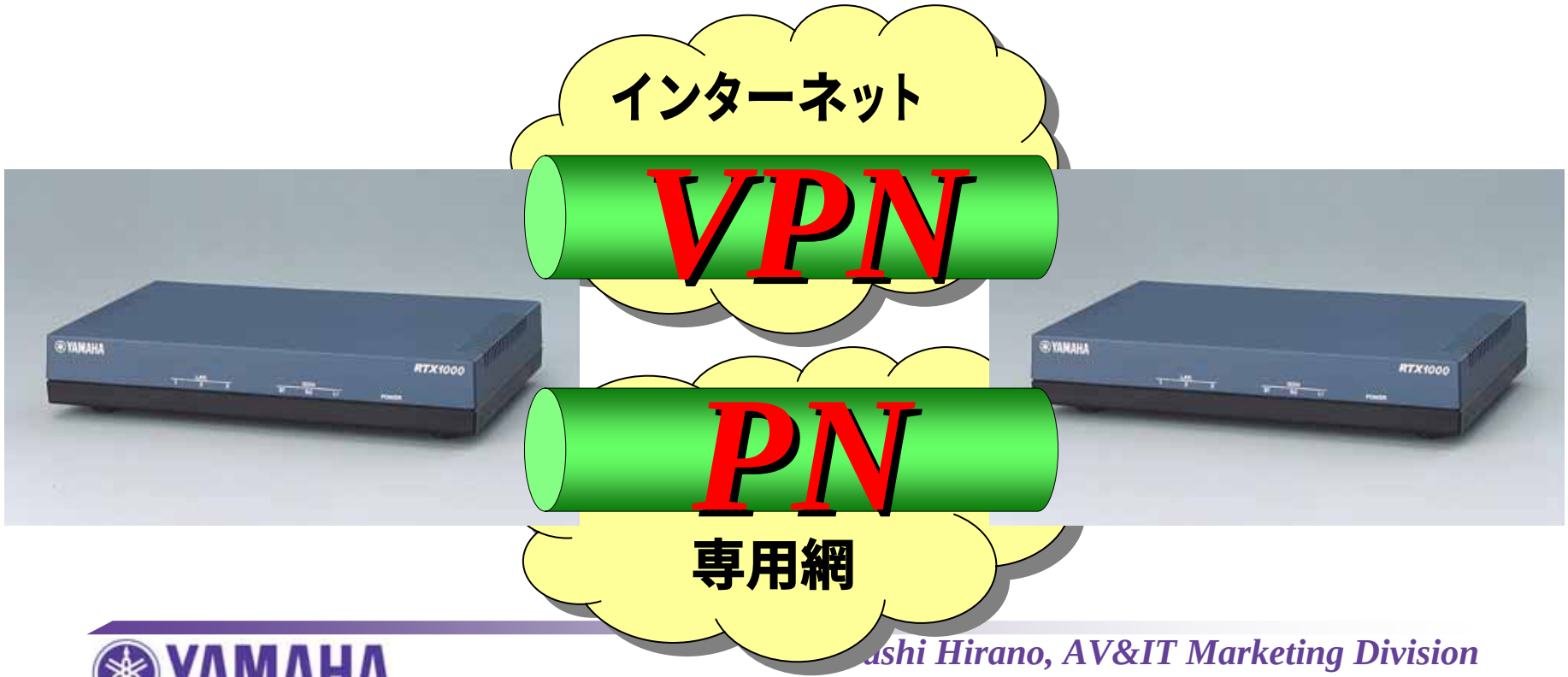
マルチホーミング(Rev.6/7系)



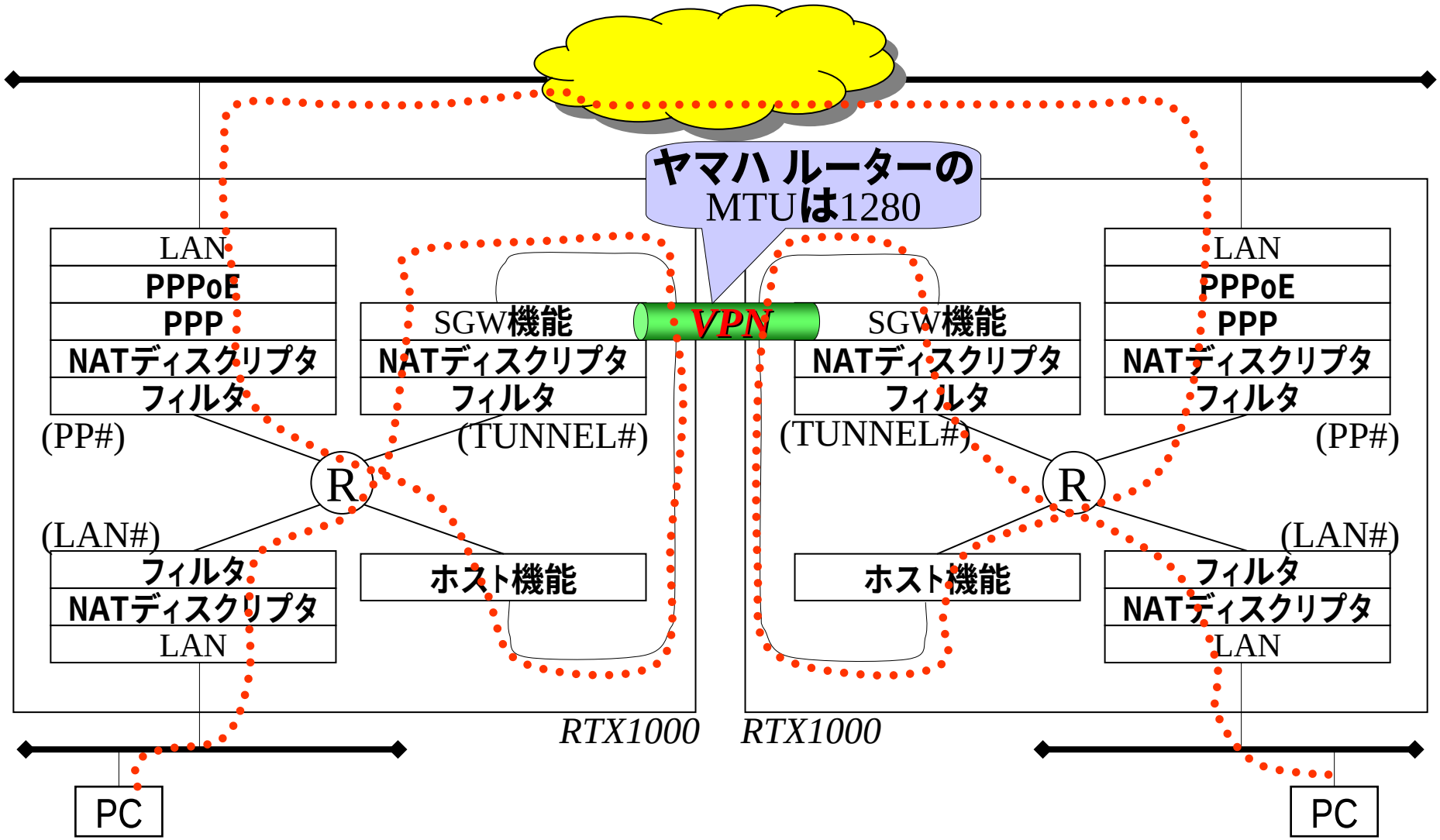
[悩み]
・インターネット接続の帯域不足
・ISPの乗り換え
[利点]
・複数のISP接続の移行や併用
　特に、PPPやPPPoE

http://www.rtpro.yamaha.co.jp/RT/docs/multi-homing.html

VPN
(Virtual Private Network)
仮想専用線

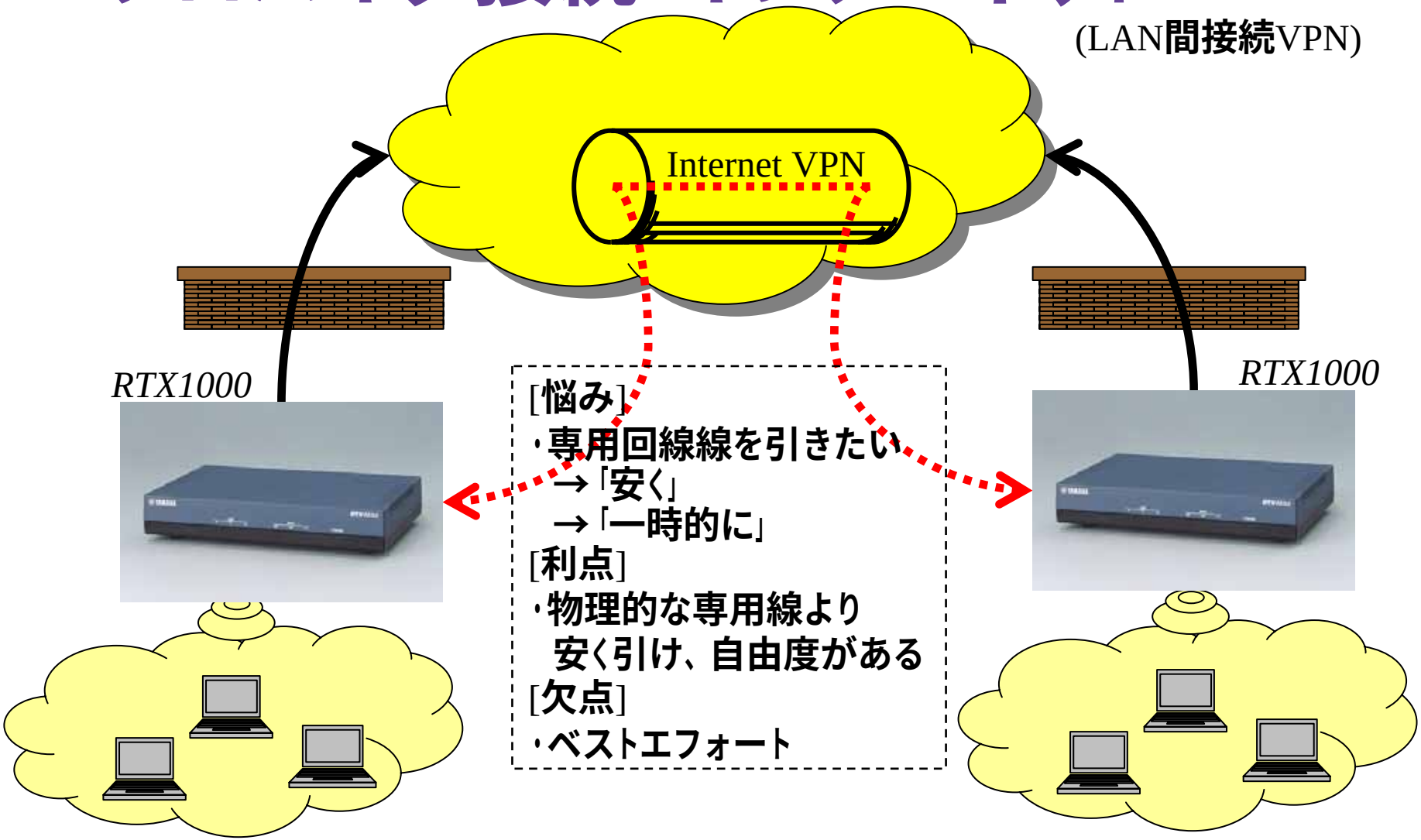


トンネリングGW機能(IPsec, PPTP, IP over IP)



プロバイダ接続+インターネットVPN

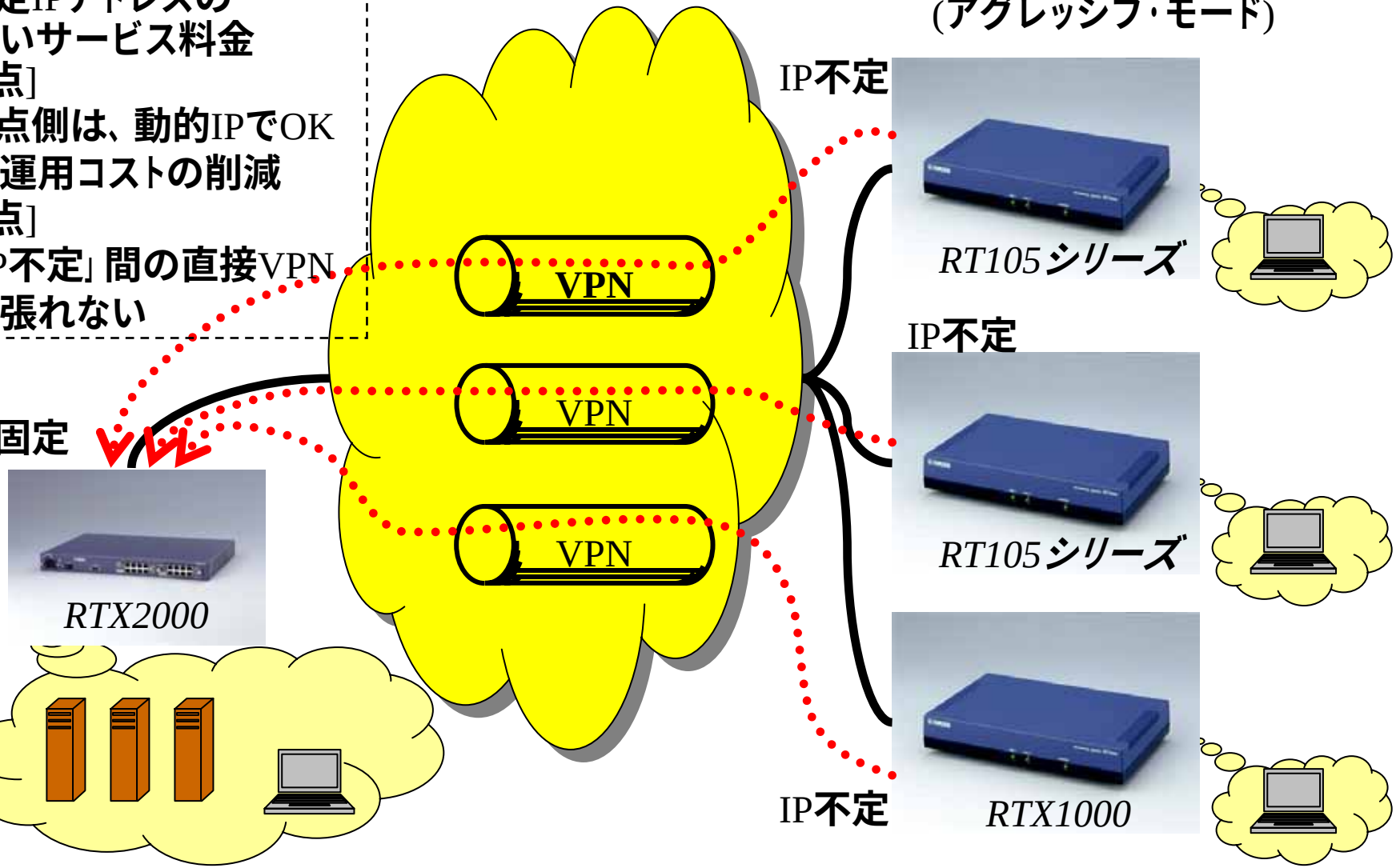
(LAN間接続VPN)



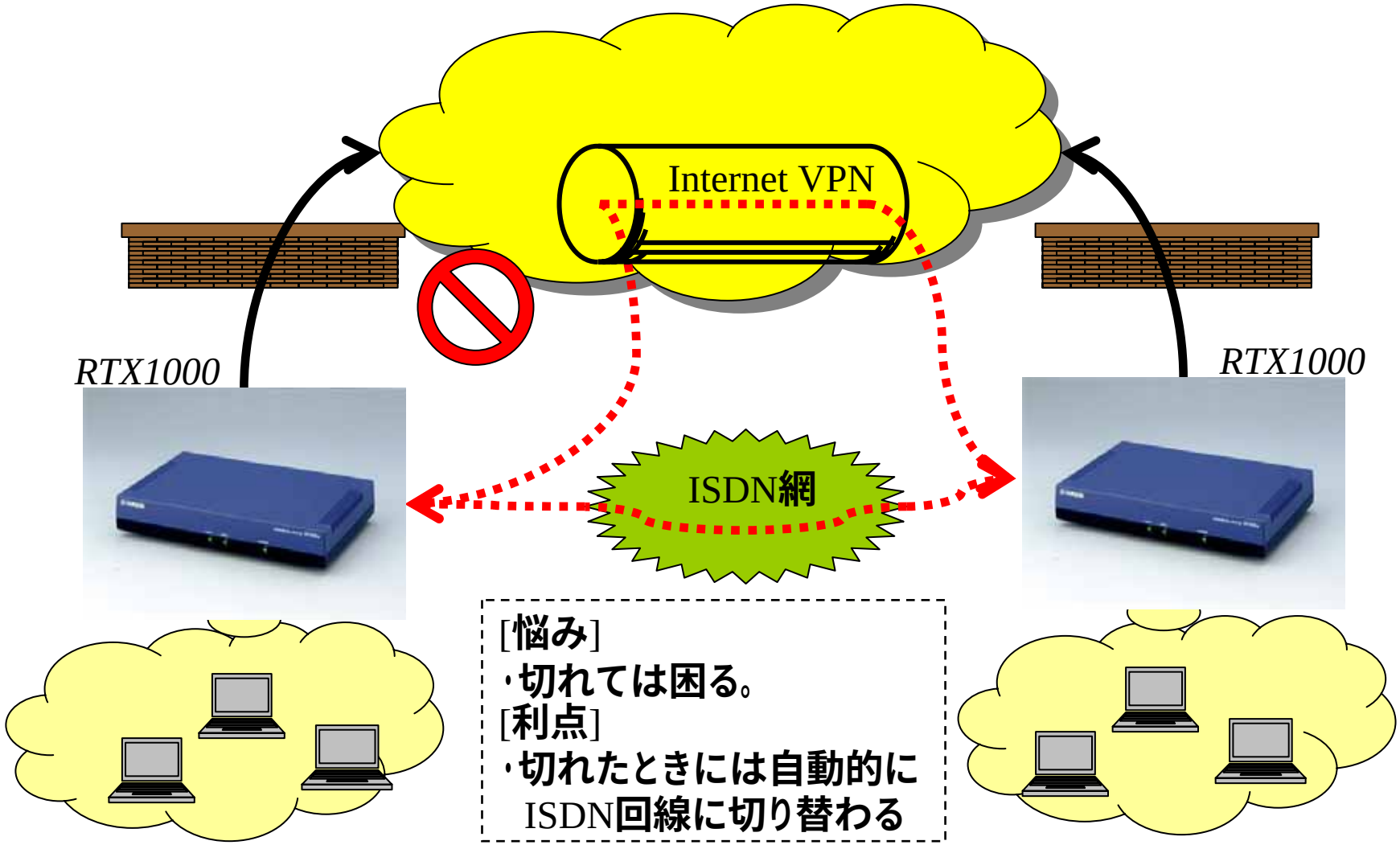
ダイヤルアップVPN

(アグレッシブ・モード)

[悩み]
・固定IPアドレスの
　高いサービス料金
[利点]
・拠点側は、動的IPでOK
　→運用コストの削減
[欠点]
・「IP不定」間の直接VPN
　が張れない



インターネットVPNのISDNバックアップ



[悩み]
・切れては困る。
[利点]
・切れたときには自動的に
ISDN回線に切り替わる

http://www.rtpro.yamaha.co.jp/RT/docs/ipsec/index.html

VPNのトンネル方式(PPTPとIPsec)

PPTP ・・・・・・・・・・・・・	・・・・・・・・・・・・・▶IPsec
・Point to Point Tunneling Protocol PPPの拡張 ・Windows95以降で標準実装されているVPNプロトコル(MS-DUN 1.4等) ・認証方式 MS-CHAP/MS-CAHP v2 ・暗号方式 なし、RC4(40bit/128bit) ・メリット お手軽、安い、相互接続性 ・デメリット セキュリティの強度	・IP Security Architecture 通常は、IPsec Version 2(RFC) ・IPv4でオプション、IPv6で標準 ・鍵交換 IKE(Internet Key Exchange) ・認証方式 HMAC-MD5、HMAC-SHA-1 ・暗号方式 DES-CBC、3DES-CBC、AES-CBC ・メリット セキュリティの強度 ・デメリット コスト(VPN Client)、相互接続性(?)

VPNクライアント(PPTPとIPsec)

PPTP	IPsec
・Windows95以降 Microsoft VPNアダプタ (MS-DUN 1.4等) 動作確認:Windows98SE以降 ・Mac OS X 10.2	・Windows 2000 Professional(※) ・Windows XP Professional(※) ・SSH Sentinel Ver.1.3.1

○IPsecのVPNクライアントとの相互接続例
http://www.rtpro.yamaha.co.jp/RT/docs/example/vpnclient/vpn_client.html
(※:注意) Windows(アグレッシブ・モードなし)とのIPsec相互接続のためには、
Windowsで固定アドレス、ルーターでフィルタ型ルーティング機能が必要
○NETSCREEN製品との相互接続例
http://www.rtpro.yamaha.co.jp/RT/docs/example/ns-5xp/index.html
○PPTPのFAQ
http://www.rtpro.yamaha.co.jp/RT/FAQ/PPTP/index.html

VPNの暗号方式 (DESからAESへ)

DES →	AES
・Data Encryption Standard - 最近まで標準だった ・DESのポリシー - ハードウェア化しやすい - ソフトウェア処理が難しい ・鍵長: 56bitの固定長 - 計算能力の向上で不十分	・Advanced Encryption Standard - DESの後継 (次世代標準) ・2000年10月 RijndaelがAESに採用される ・AESのポリシー - 可変長の鍵 - ハード/ソフトでの実装 - ロイヤリティ・フリー

[参考文献]
http://www.soi.wide.ad.jp/class/20010012/slides/10/
http://www.soi.wide.ad.jp/class/20010012/materials_for_student/10/NetArch10-2.pdf
村井純氏のネットワークアーキテクチャの講義の「セキュリティ」

VPN(IPsec)の暗号処理速度

	ソフトウェア処理	ハードウェア処理
一般論	・暗号強度: AES>3DES>DES ・処理速度 AES,DES>3DES ※AESを使おう	・搭載ハードウェアに依存 →機種依存
RTX1000	AESは、遅い。 ※AESは相互接続に使おう	3DES,DESは、同等で速い。 ※3DESを使おう
RTX2000 YBB-VPN-A	AESは、遅い。 ※AESは相互接続に使おう	3DES,DESは、同等で速い。 ※3DESを使おう

IP-VPN

通常のオープンなインターネットとは異なり、
IP網上に仮想的な専用の通信路を確保し、
セキュリティを伴って通信できる仕組み
[IP-VPNの利点]
・セキュリティ、管理はお任せ
[RT105シリーズの利点]
・BGP4対応

RTX2000

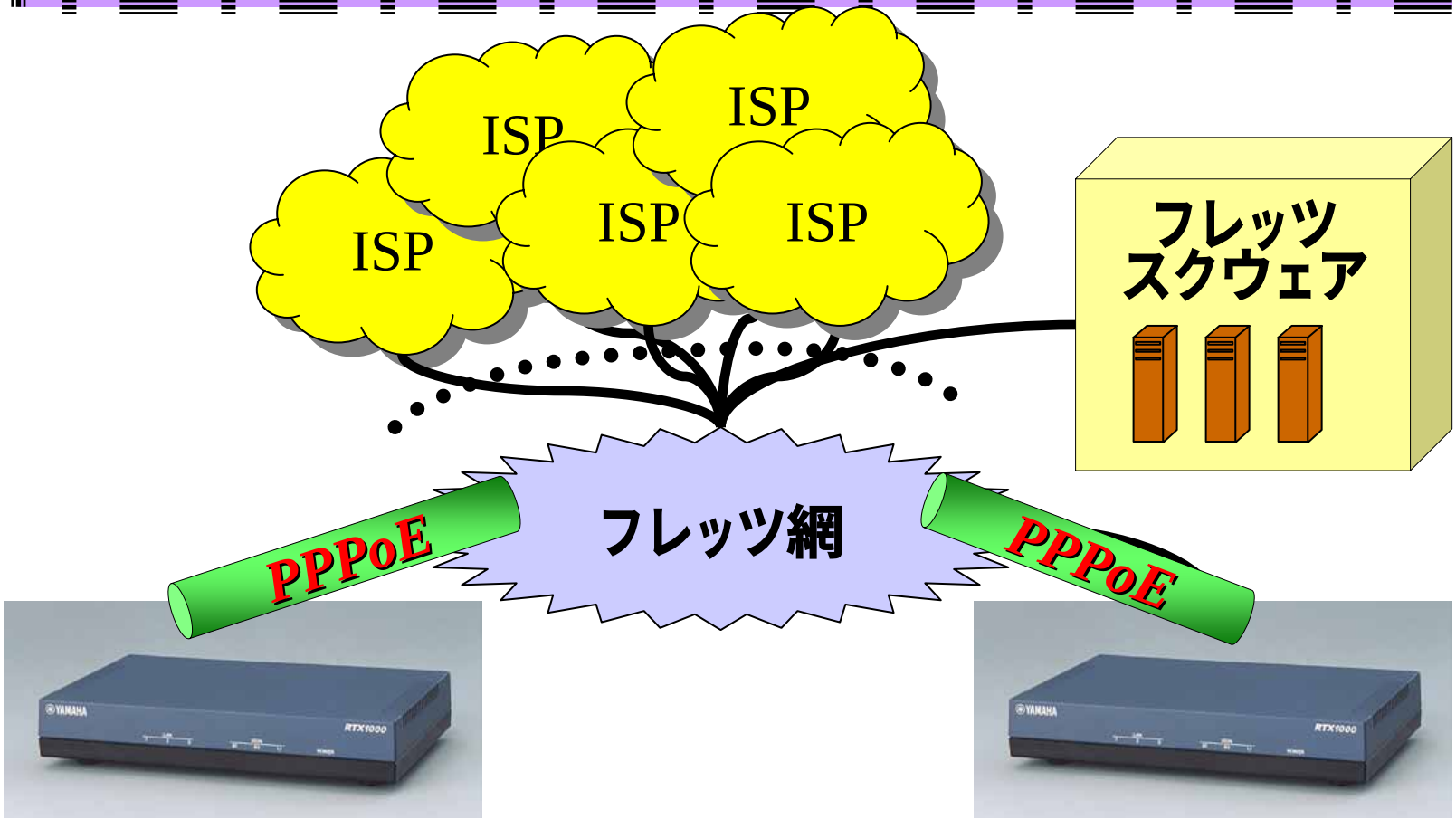
IP-VPN網

RT105シリーズ

RTX1000

RTX1000

フレッツ・シリーズ & PPPoE



フレッツ・スクウェア(PPPoE&マルチセッション)

[悩み]
・毎回、切り替えななきゃ(;_;)
rt100i-users: 28620,…

ISP

フレッツ網

フレッツ
スクウェア

フレッツ・ADSL
Bフレッツ

RTA55i

・接続先切り替え
・同時接続

[前提]
PP01: ISP
PP02: フレッツ・スクウェア
[追加コマンド例(環境依存)]
ip route default gateway pp *1*
ip route *172.26.0.0/16* gateway pp *2*
dns server select 1 pp *2* any *flets*
clear dns cache

cf.ASCII, NETWORK MAGAZINE, 2003/1, P.106〜P.107

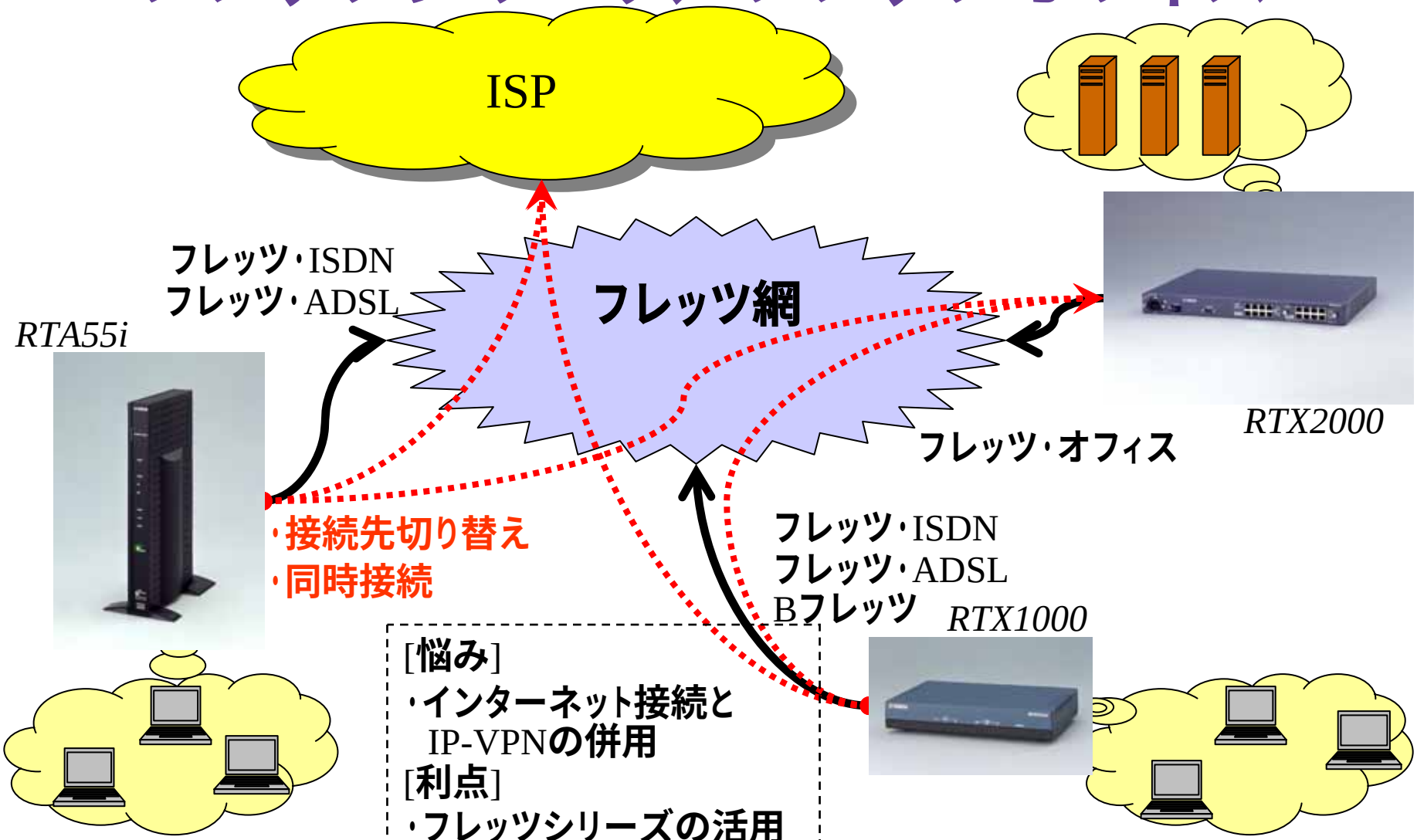
http://www.rtpro.yamaha.co.jp/RT/FAQ/PPPoE/multi-session-example.html

PPPoEの同時接続対応

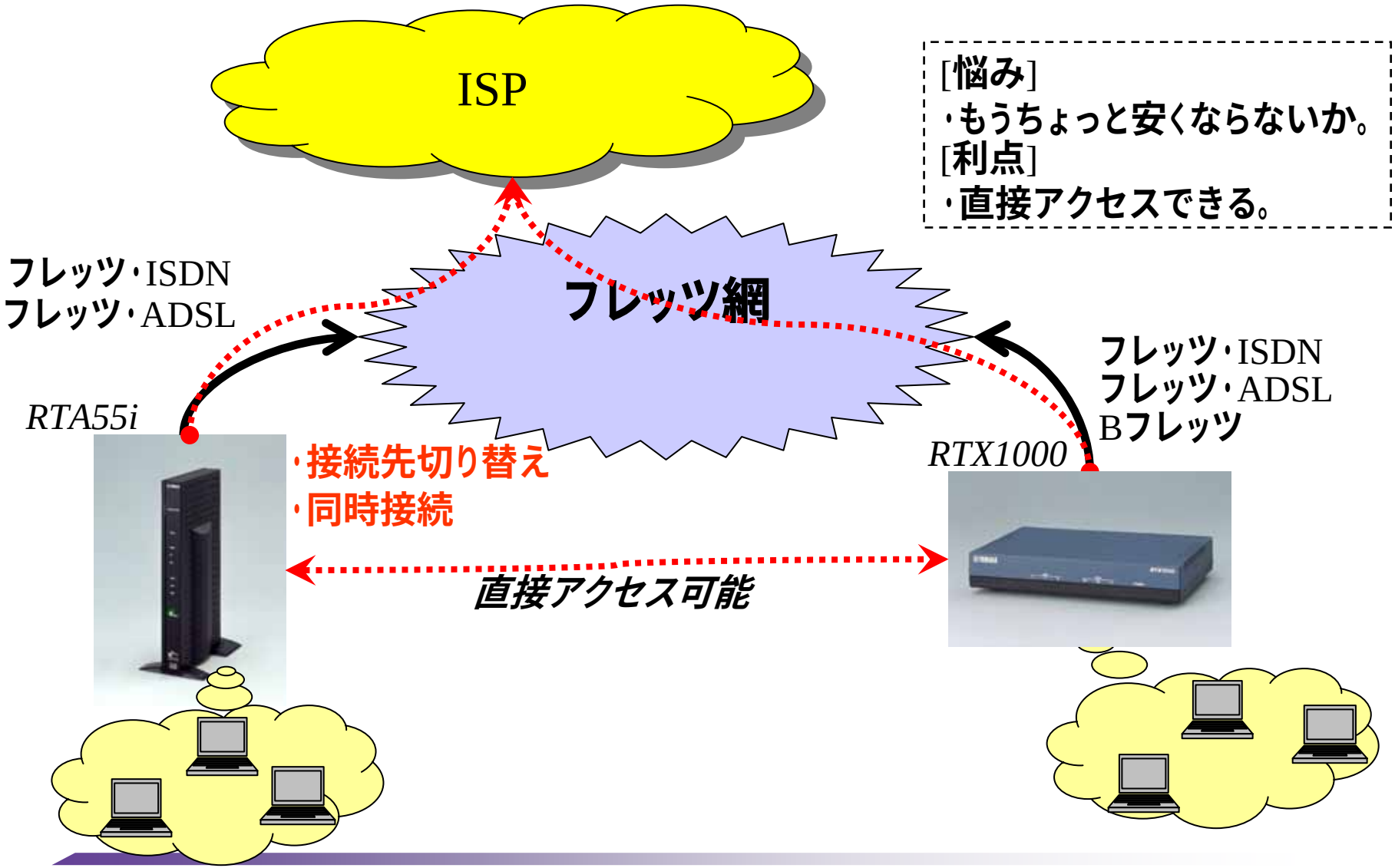
RTシリーズ/RTXシリーズ	同時接続数	備考
RTX2000	32〜64	・Rev.6.02.20以降 →実装LANインタフェース数*4 ・Rev.6.02.19以前 →2
RTX1000	12	
RT300i	4〜20	
RT140f、RT140e、RT105e	8	
RT140i、RT140p、 RT105i、RT105p	4	
ネットボランチシリーズ	**同時接続数**	**備考**
RTW65i RTW65b RT60w RT56v RTA55i RTA54i	2	

http://www.rtpro.yamaha.co.jp/RT/FAQ/PPPoE/concurrent-connection-number.html

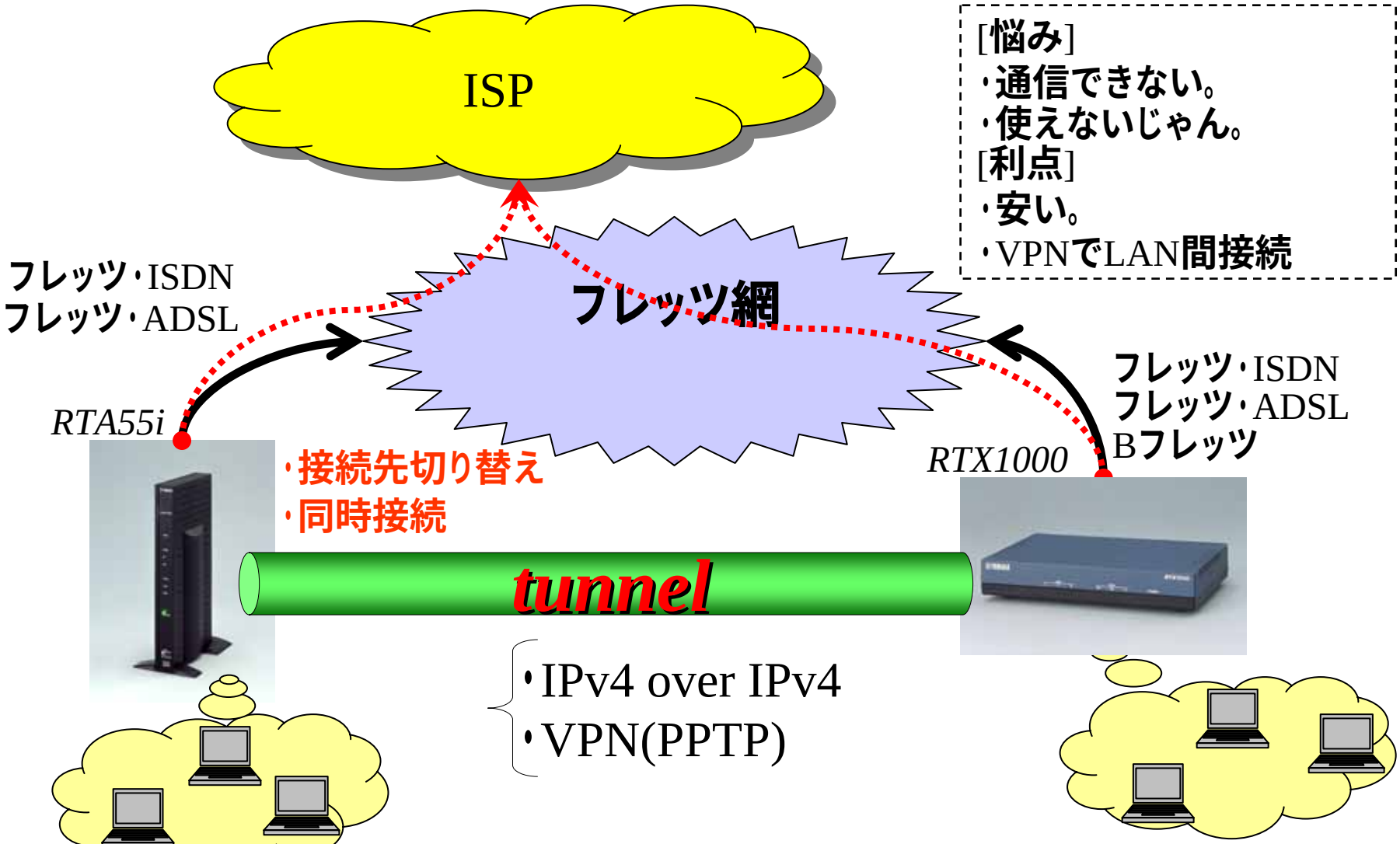
フレッツシリーズ+フレッツオフィス



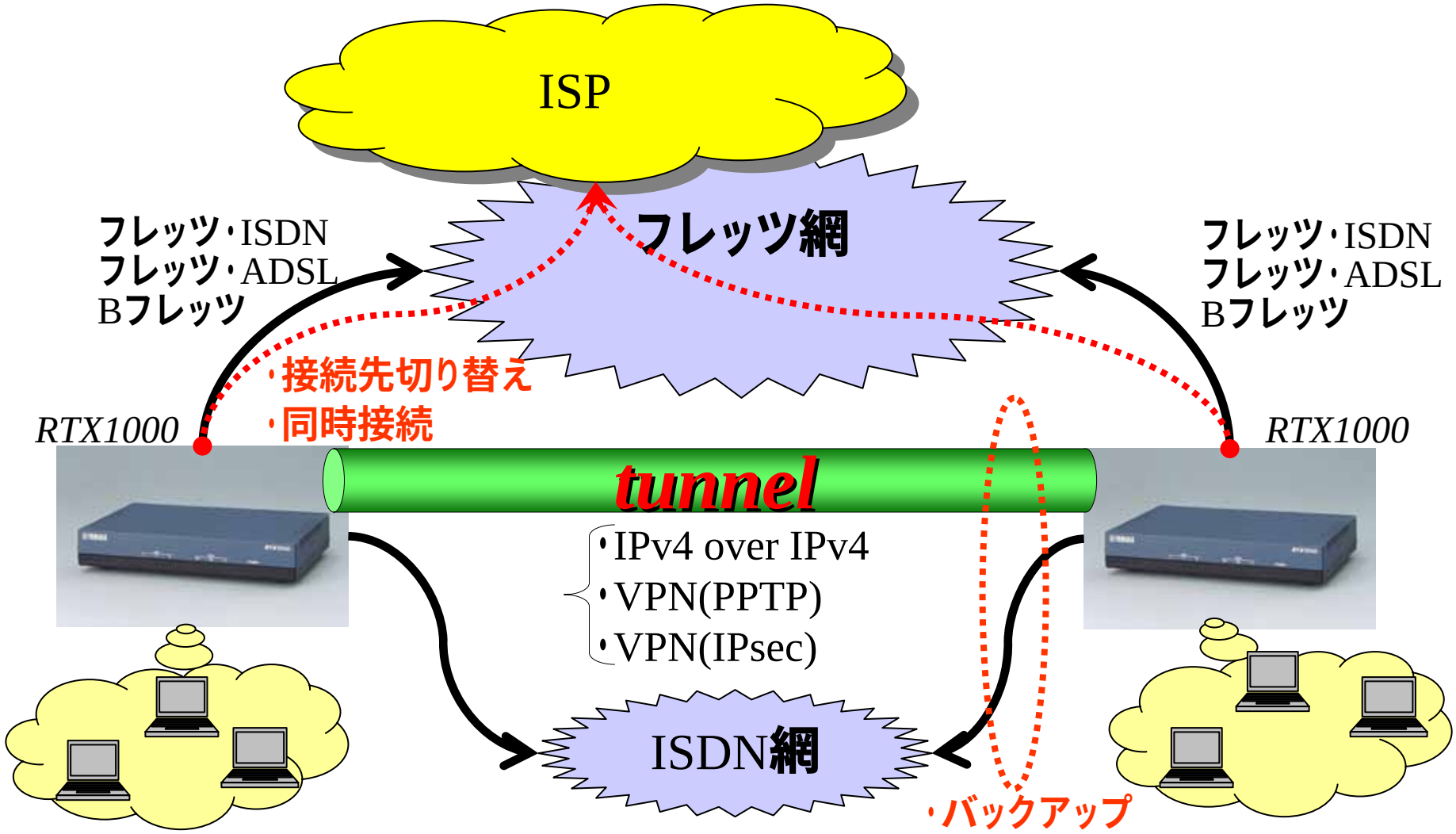
フレッツ・グループアクセス・プロ(LAN型)



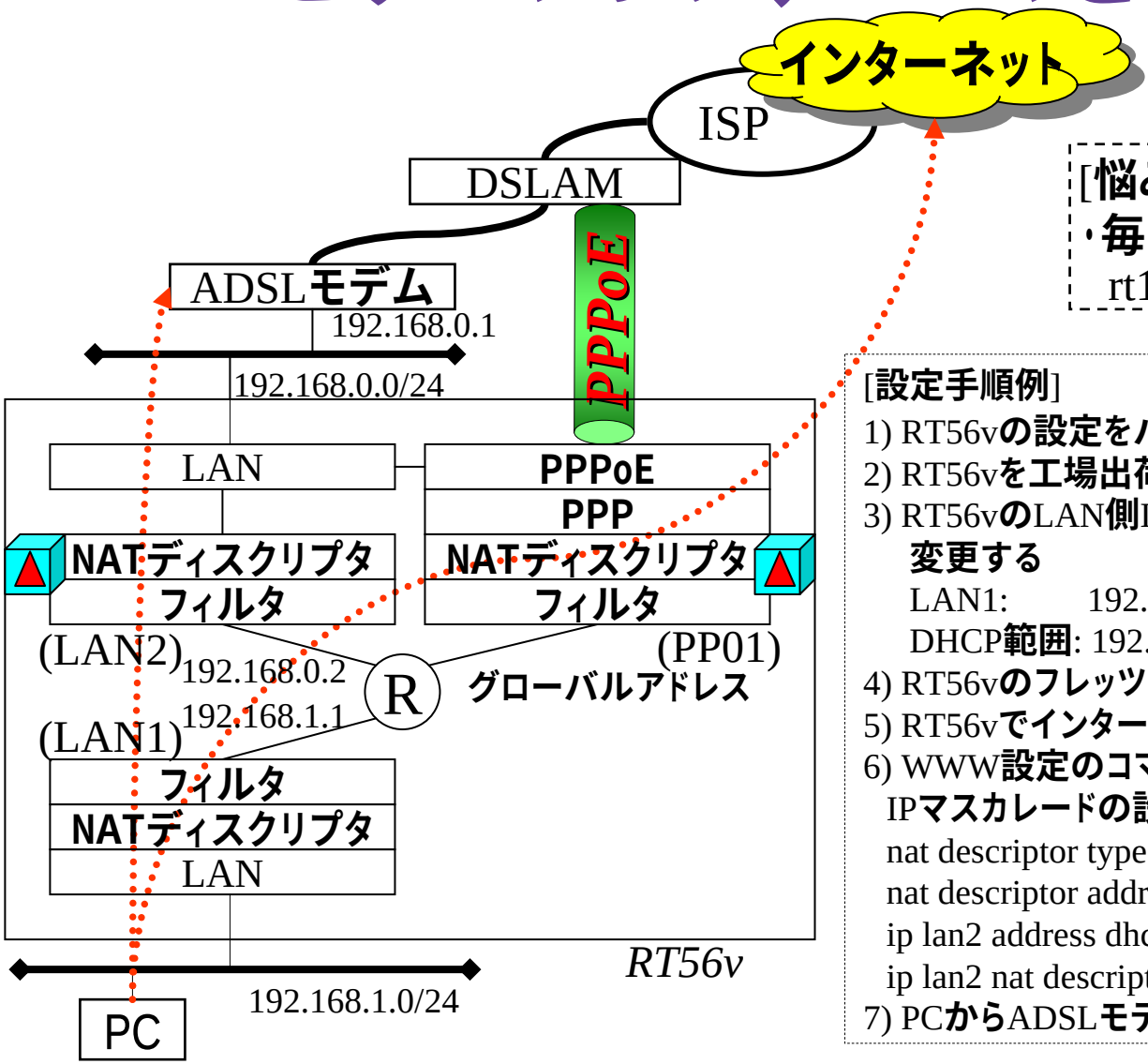
フレッツ・グループアクセス(端末型)



フレッツ・グループアクセス(端末型)



ADSLモデムのファームを更新できる?



[悩み]
・毎回、繋ぎ変えななきゃ(;_;)
rt100i-users: 29193,…

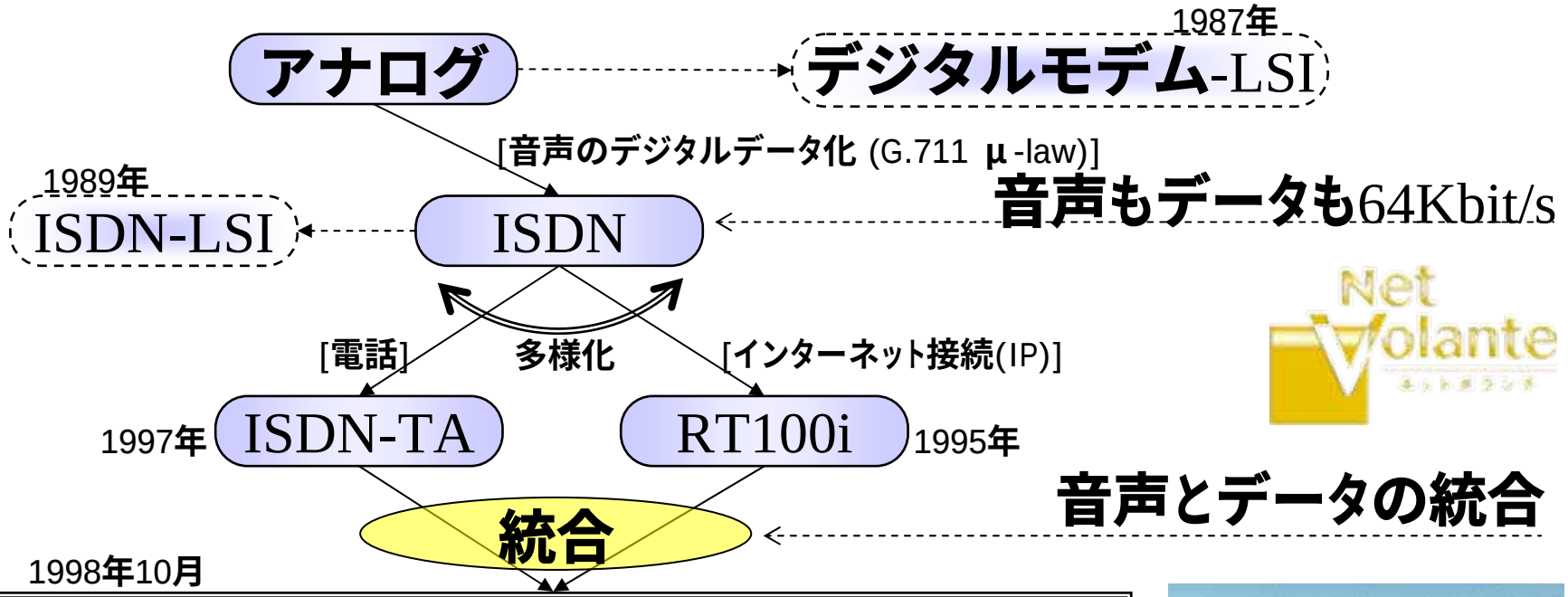
[設定手順例]
1) RT56vの設定をバックアップする。
2) RT56vを工場出荷状態に戻す。
3) RT56vのLAN側IPアドレスとDHCPの割り当て範囲を変更する
LAN1: 192.168.1.1/24
DHCP範囲: 192.168.1.2-192.168.1.192/24
4) RT56vのフレッツ・ADSL接続設定をする。
5) RT56vでインターネットアクセスの動作確認をする。
6) WWW設定のコマンド入力でWANにIPアドレスとIPマスカレードの設定を追加する。
nat descriptor type 2 masquerade
nat descriptor address outer 2 primary (192.168.0.2)
ip lan2 address dhcp (192.168.0.2/24)
ip lan2 nat descriptor 2
7) PCからADSLモデムにpingなどで疎通確認をする。

http://www.rtpro.yamaha.co.jp/RT/FAQ/PPPoE/adsl-modem-access.html

オールインワン・ソリューション
NetVolante(ネットボランチ)
～トピックス～

●トピックス
●インターネット電話
●VPN

1998年10月ネットボランチが生まれた



[ネットボランチRTA50i]

LANも電話もインターネットも

簡単 快適 ネットワークなら

ヤマハ ネットボランチ

ネットボランチのトピックス#0

製品	内容
RT80i ’97.10	＜ネットボランチの兄貴分＞ ・ISDNリモートルーター機能…「ISDNダイヤルアップルーター」 ・TELポート: 独立2ポート ・OCNエコノミーの登場 (ネットワーク型常時接続…IP8/IP16) ・デフォルトのセキュリティポリシー ・ヤマハ初のWWW設定機能 (コマンドと1対1に対応) 

ネットボランチのトピックス#1

製品	内容
RTA50i ’98.10	＜進化するルーター＞ ・ISDN-TA機能とルーター機能のオールインワン ・TELポート: 独立3ポート ・かんたん設定(超シンプル型) ・デフォルトのセキュリティポリシー ・メール機能(着信確認,転送) ・フィルタ型ルーティング ・TA版とLAN版のRVS-COM対応
RTA52i ’00.3	＜ISDNを活用するルーター＞ ・液晶ディスプレイと前面操作ボタン ・かんたん設定(LAN間接続、リモートアクセス) ・LAN-TA機能 ・メール機能(通知)

ネットボランチのトピックス#2

製品	内容
RT60w ’00.10	＜無線LANを活用するルーター＞ ・IEEE 802.11b (WEP 64bits) ・MGCPによる機器間アナログ通話 (内線VoIP) ・無線ブリッジ機能 
RTA54i ’01.7	＜ISDNとブロードバンドを活用するルーター＞ ・ブロードバンド対応(2 ether…WANポート)、PPPoE搭載 ISDNとブロードバンドの併用など ・ファイアウォール機能 静的フィルタ、動的フィルタ、不正アクセス検知 7段階のセキュリティレベル ・USB-TA機能 ・IPv6標準搭載 

ネットボランチのトピックス#3

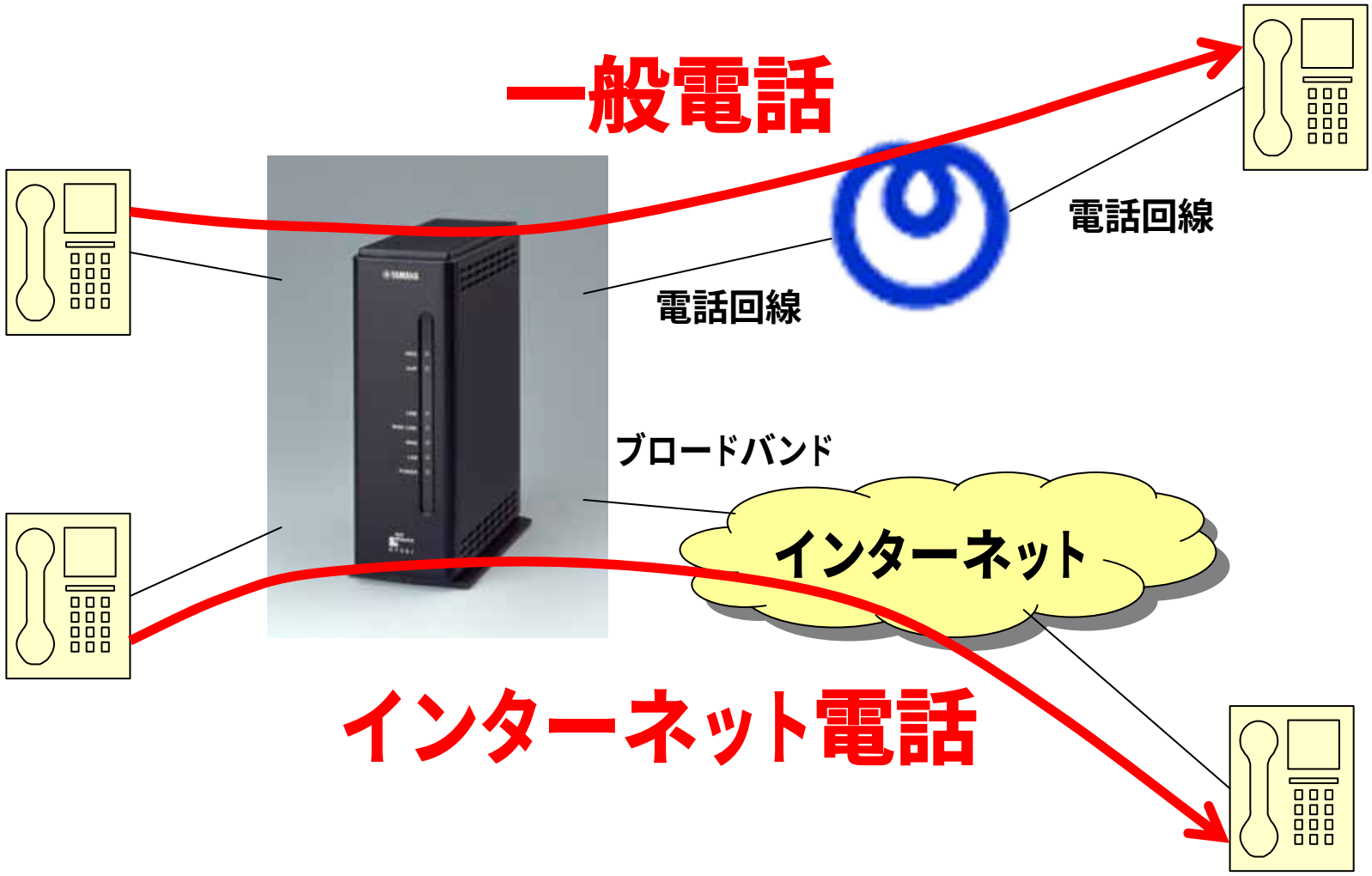
製品	内容
RTW65b ’01.11 RTW65i ’02.1	・ブロードバンドTA機能 ・IEEE 802.11b (WEP 128bits) ・外部アンテナオプション  
RTA55i ’02.5 RT56v ’02.7	＜ブロードバンドにつながる進化するルーター＞ ・PPTPによるVPN機能 ・SIPによるインターネット電話機能 ・ネットボランチDNS ・UPnP対応とWindows Messenger対応 ・NetMeeting 3.0対応 ・IPv6ファイアウォール機能  

インターネット電話への取り組み (ヤマハのVoIP関連技術)

[外から見える取り組み]
2000年12月「機器間アナログ通話機能(MGCP)」をRT60wに提供
2001年6月 Networld + Interop Tokyo 2001会場にて
RTA54iを使用した「IPv6版MGCP」をデモンストレーション
2001年12月 RTA54i/RT60w/RTW65iにてIPv4/IPv6版SIPによる
VoIP機能のβ1版ファームウェアの提供開始
2002年5月 RTA55i発売。
RTA54i/RT60w/RTW65iにてIPv4/IPv6版SIPによるVoIP機能の
β2版ファームウェアの提供開始
2002年7月 RT56v発売。

- MGCP:Media Gateway Control Protocol、RFC2705
- SIP:Session Initiation Protocol、RFC2543

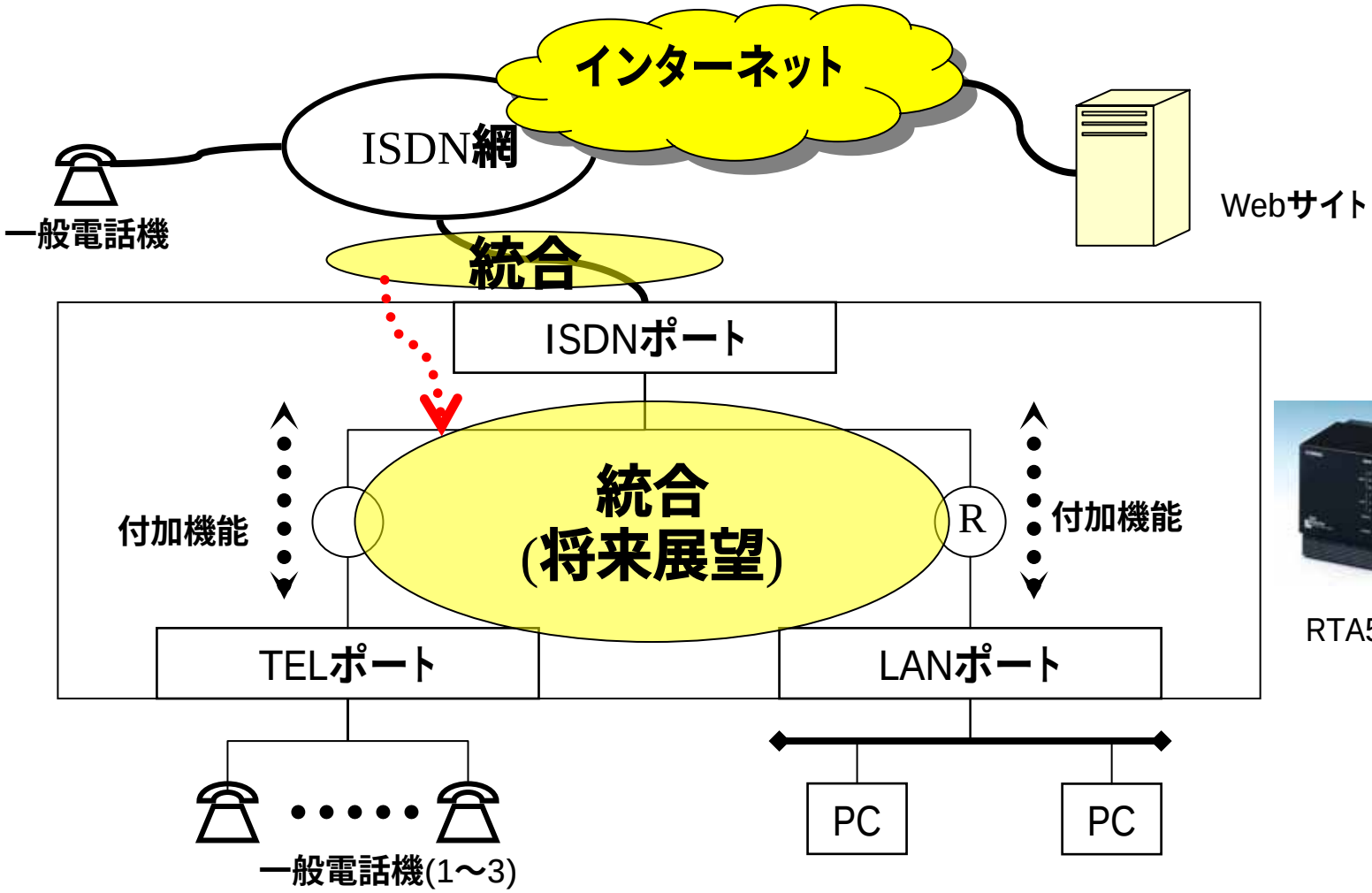
インターネット電話



インターネット電話(VoIP)への取り組み

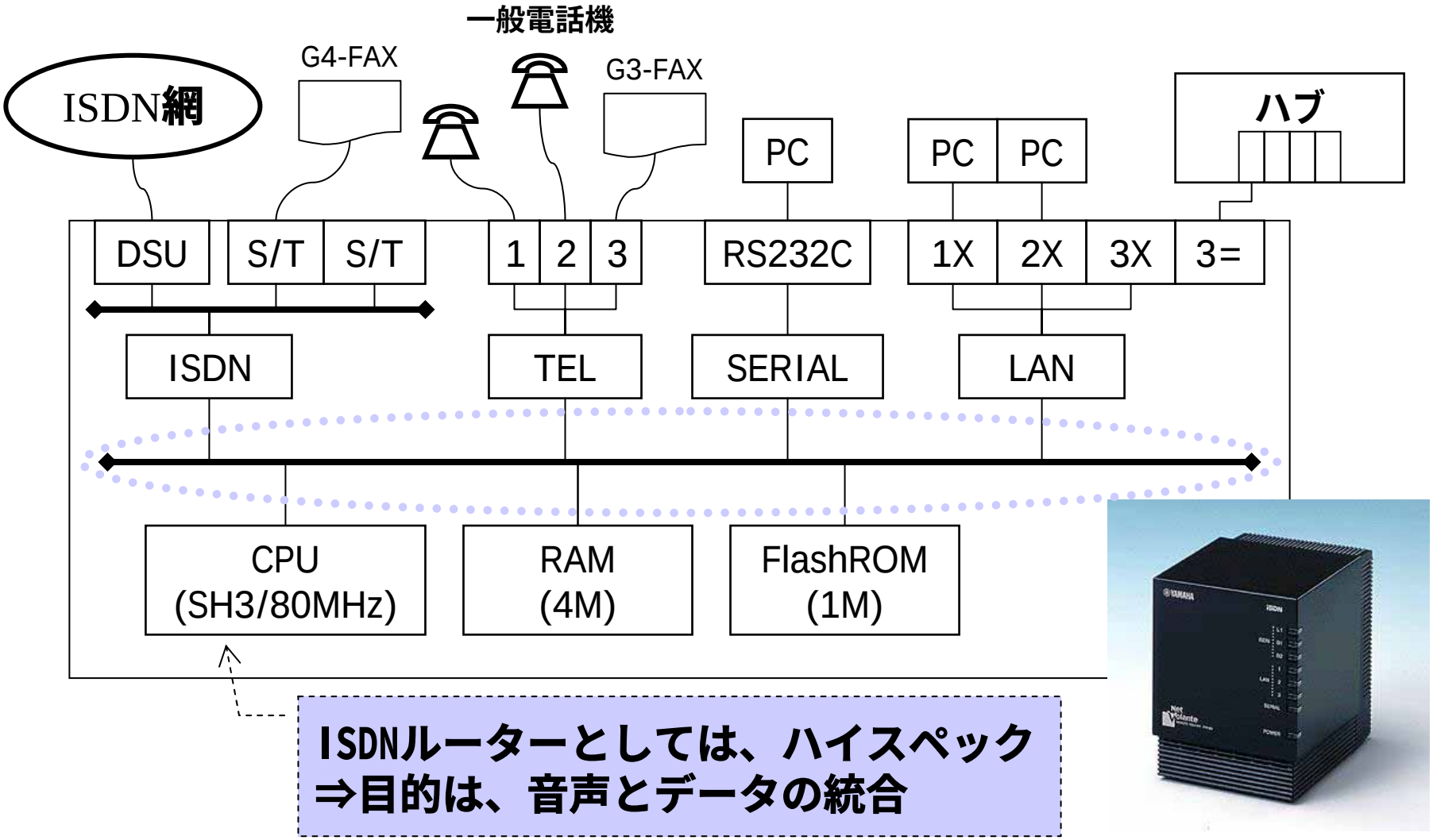
日付	Revision	内容
1998年10月		◯RTA50i発売
2000年11月	Rev.5.00.10	◯RT60w発売
2000年12月	Rev.5.01.14	・機器間アナログ通話(VoIPプロトコルのMGCPを利用した内線通話)
2001年6月		・RTA54iによるIPv6版機器間アナログ通話のデモンストレーション 会場: Networld+Interop Tokyo 2001のIPv6 ShowCaseなど
2001年7月	Rev.4.00.10	◯RTA54i発売
2001年12月		・ISDN回線用IPv6+VoIPゲートウェイ機能の協力 (ソフトフロント) ・RT60w用IPv4/IPv6対応SIPによるインターネット電話(VoIP)機能β1
2002年1月		・RTA54i用IPv4/IPv6対応SIPによるインターネット電話(VoIP)機能β1 ・RTW65i発売
2002年2月		・RTW65i用IPv4/IPv6対応SIPによるインターネット電話(VoIP)機能β1
2002年3月		・IPv4/IPv6対応SIPによるインターネット電話(VoIP)機能β2
2002年5月～		・ネットボランチDNSサービス β版 ◯RTA55i、RT56v発売

ISDNルーターの構成(音声とデータの統合)



RTA50i

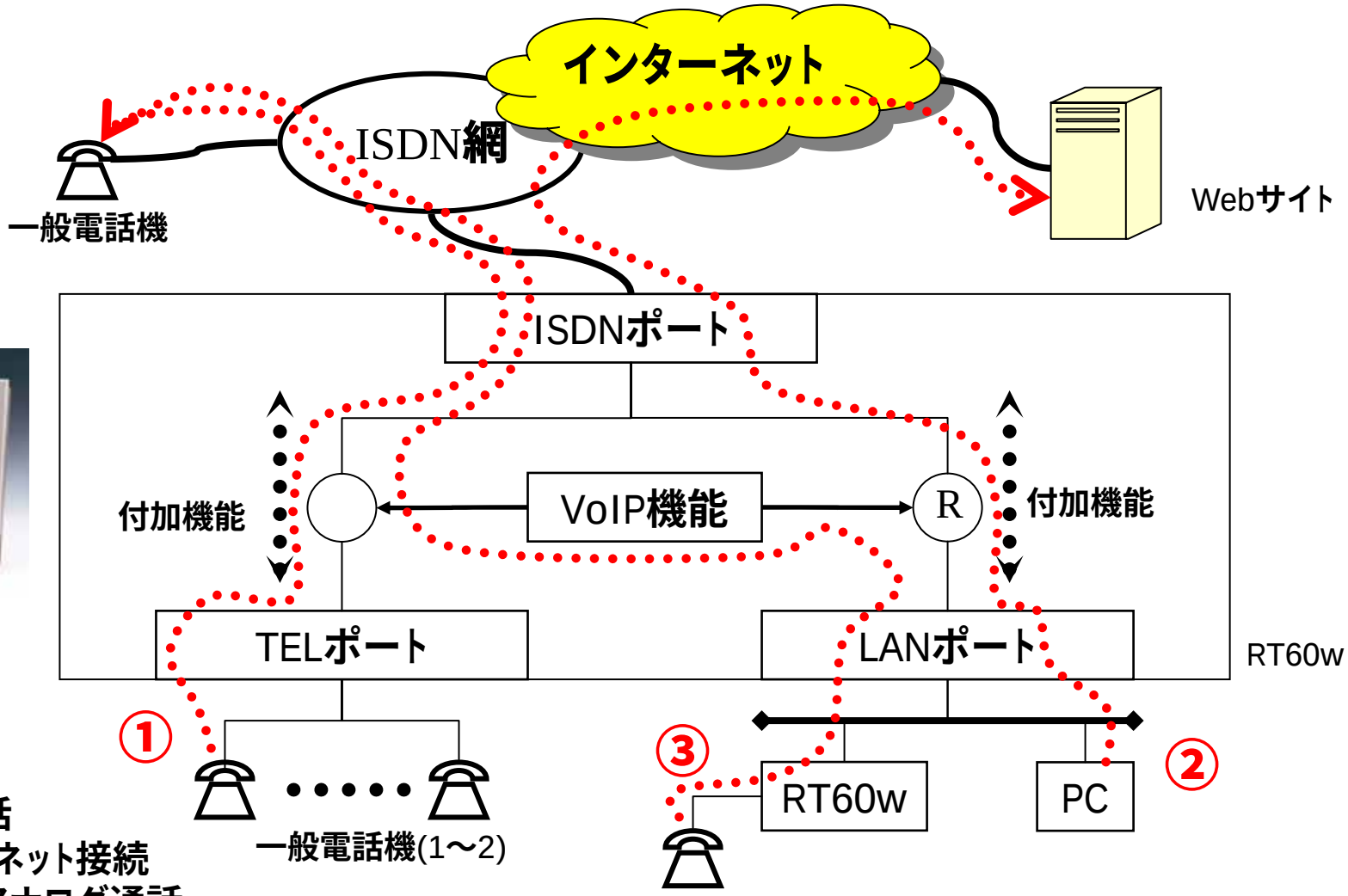
ネットボランチ RTA50iのアーキテクチャ



ISDNルーターとしては、ハイスペック
⇒目的は、音声とデータの統合

VoIPルーターの構成(ナローバンド時代)

MGCP:Media Gateway Control Protocol、RFC2705



[通信路]
①一般電話
②インターネット接続
③機器間アナログ通話

ネットボランチのインターネット電話機能

[要素]

◎ TELポート

ISDNルーターで培ったアナログ技術

◎ 機器間アナログ通話 (かんたんPBX、機器間内線通話)

ISDNルーターで培ったVoIP技術

◎ ネットボランチDNSの電話アドレスサービス

・ブロードバンドルータの要素

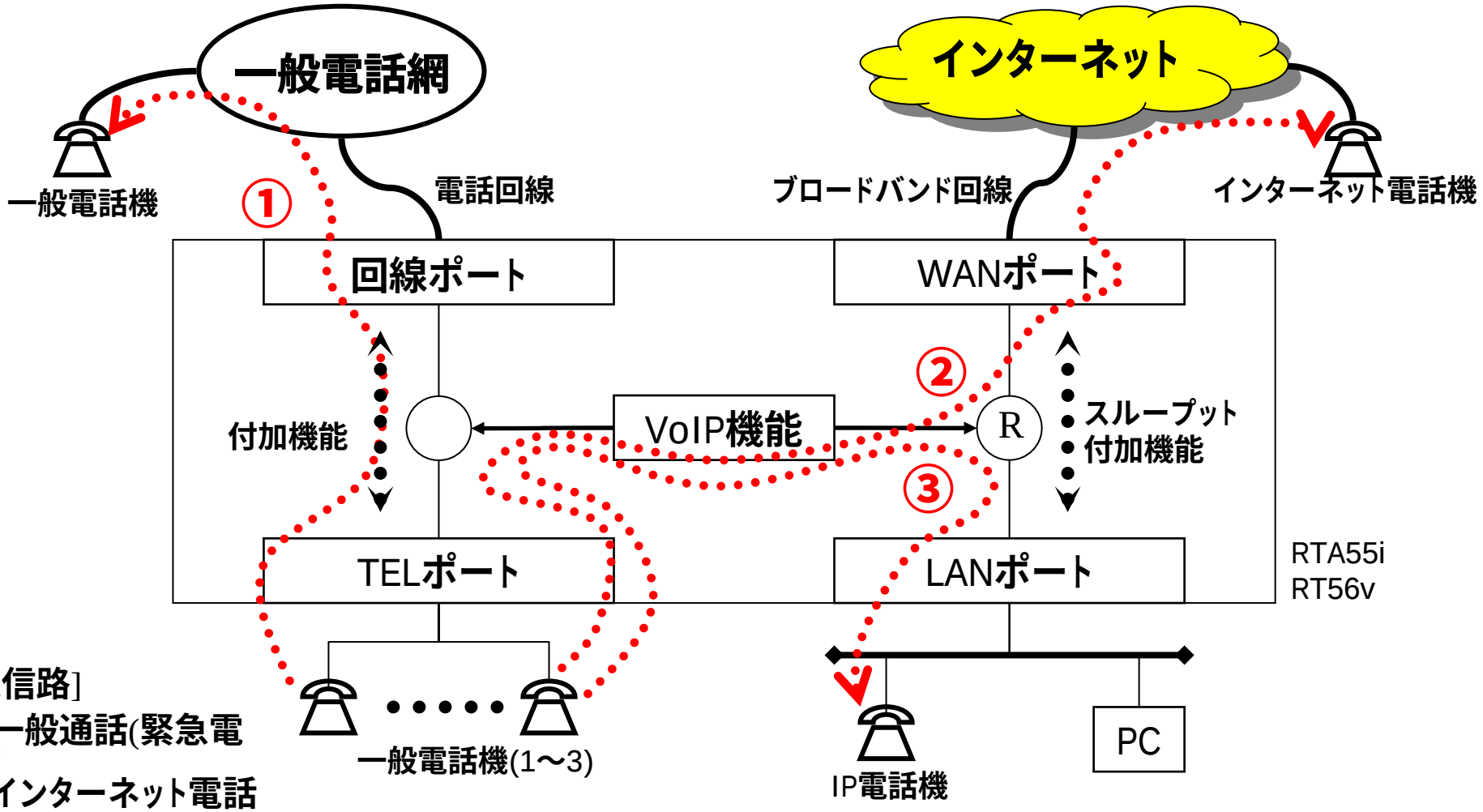
・ビジネスホン/ホームテレホンの要素

・インターネット電話(VoIP-TA)の要素

・VoIPゲートウェイの要素(提供未定)

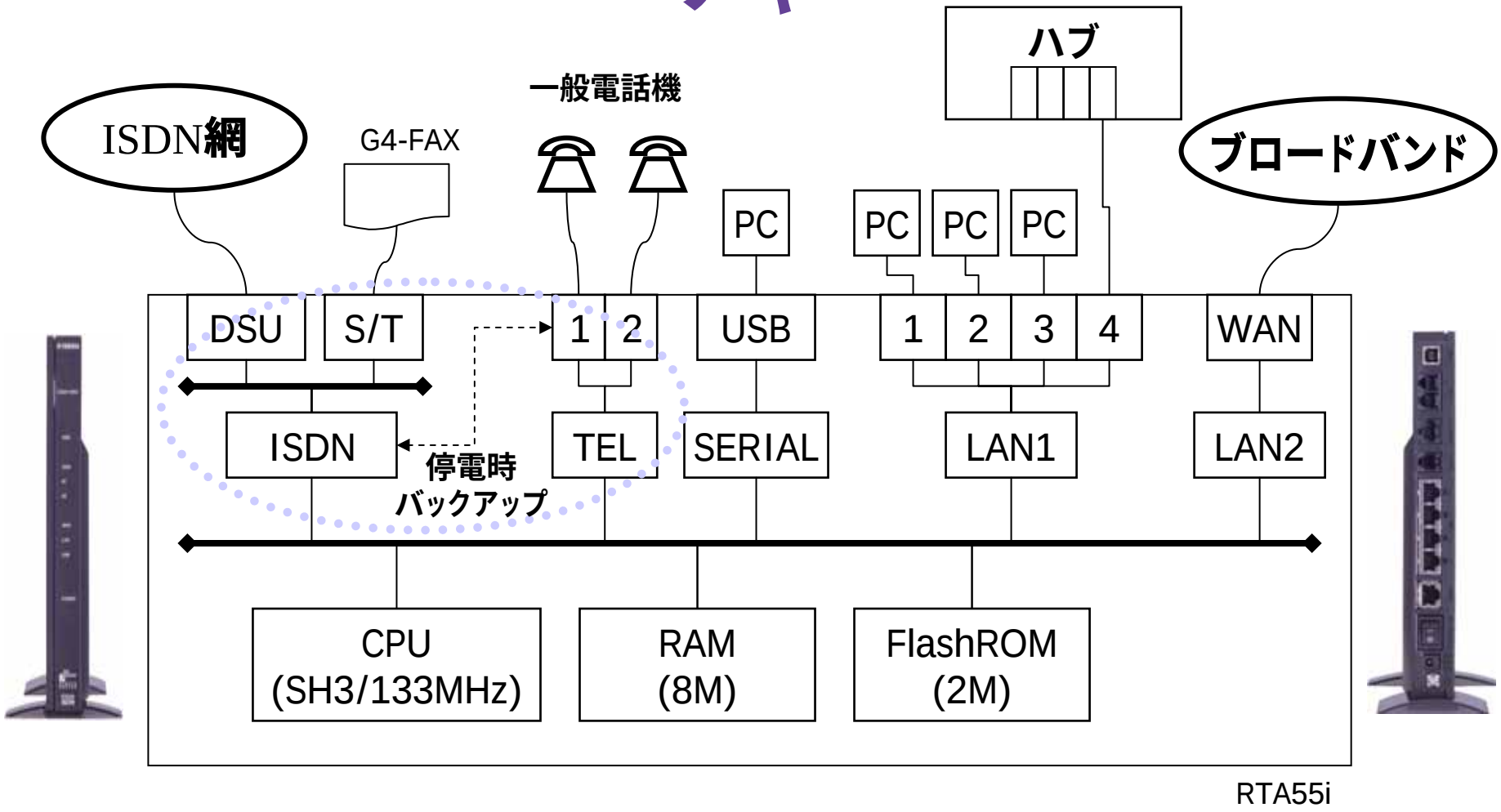
VoIPルーターの構成(ブロードバンド時代)

SIP:Session Initiation Protocol、RFC2543

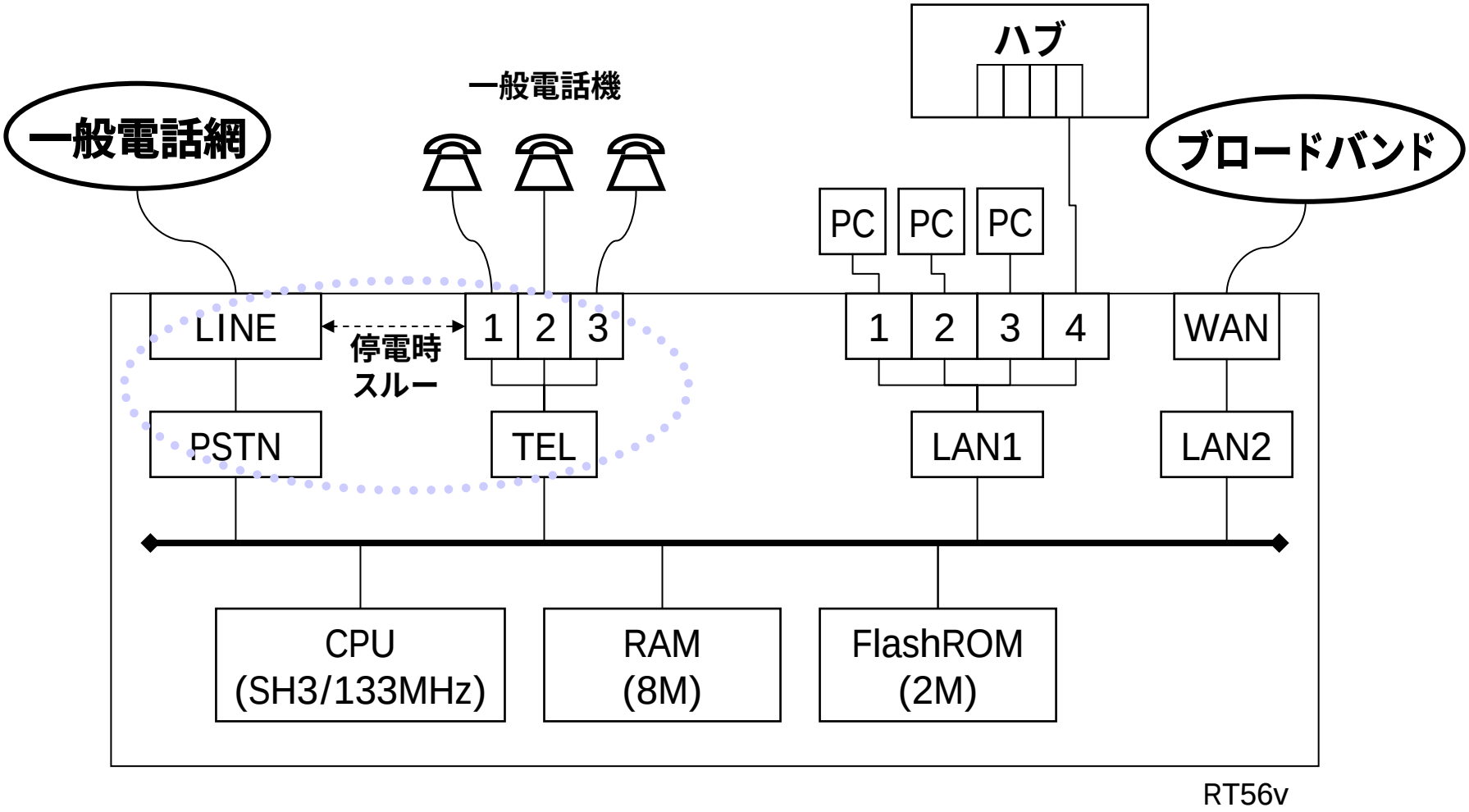


[通信路]
①一般通話(緊急電話)
②インターネット電話
③内線のIP電話

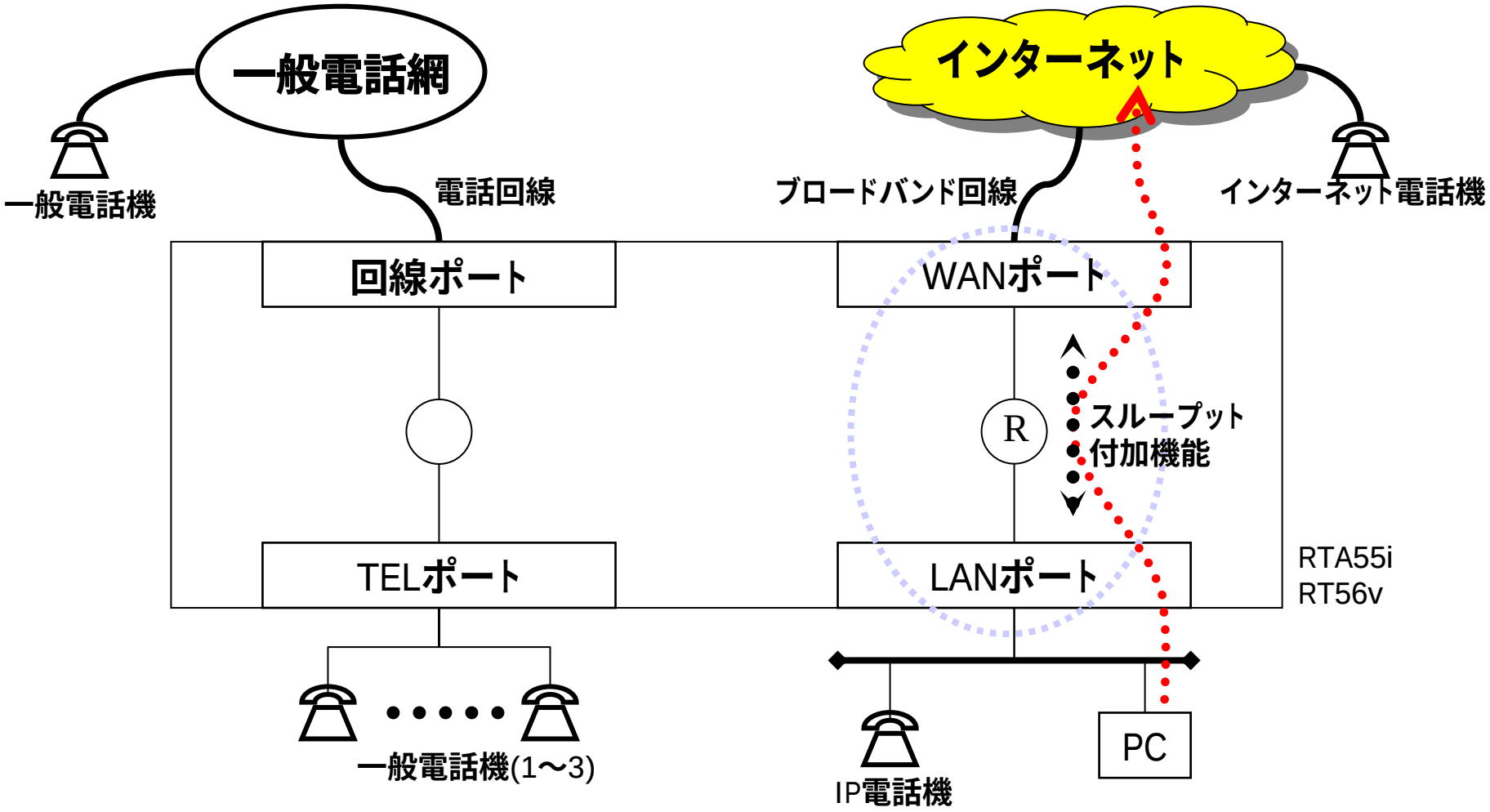
ネットボランチ RTA55iのアーキテクチャ



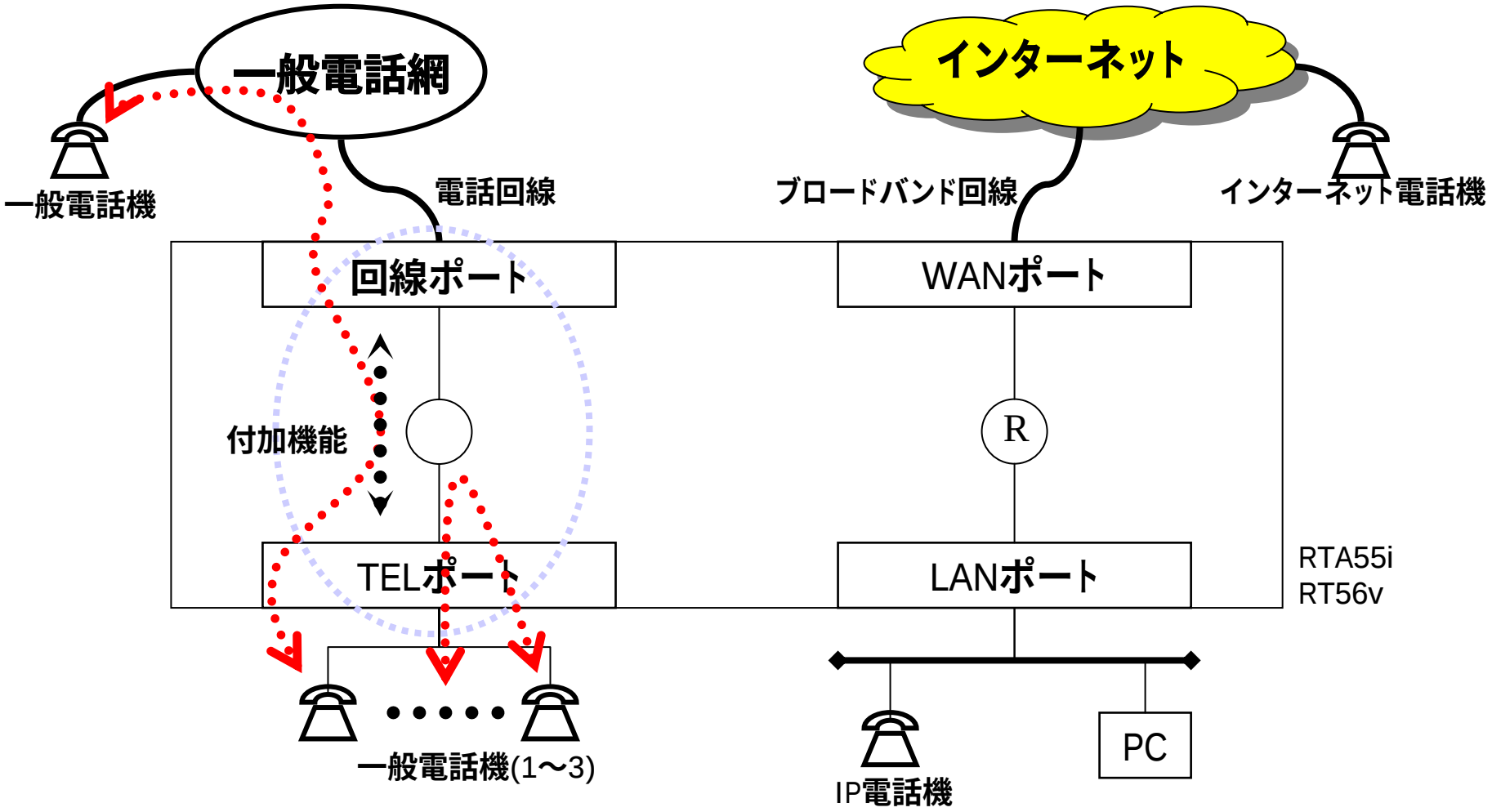
ネットボランチ RT56vのアーキテクチャ



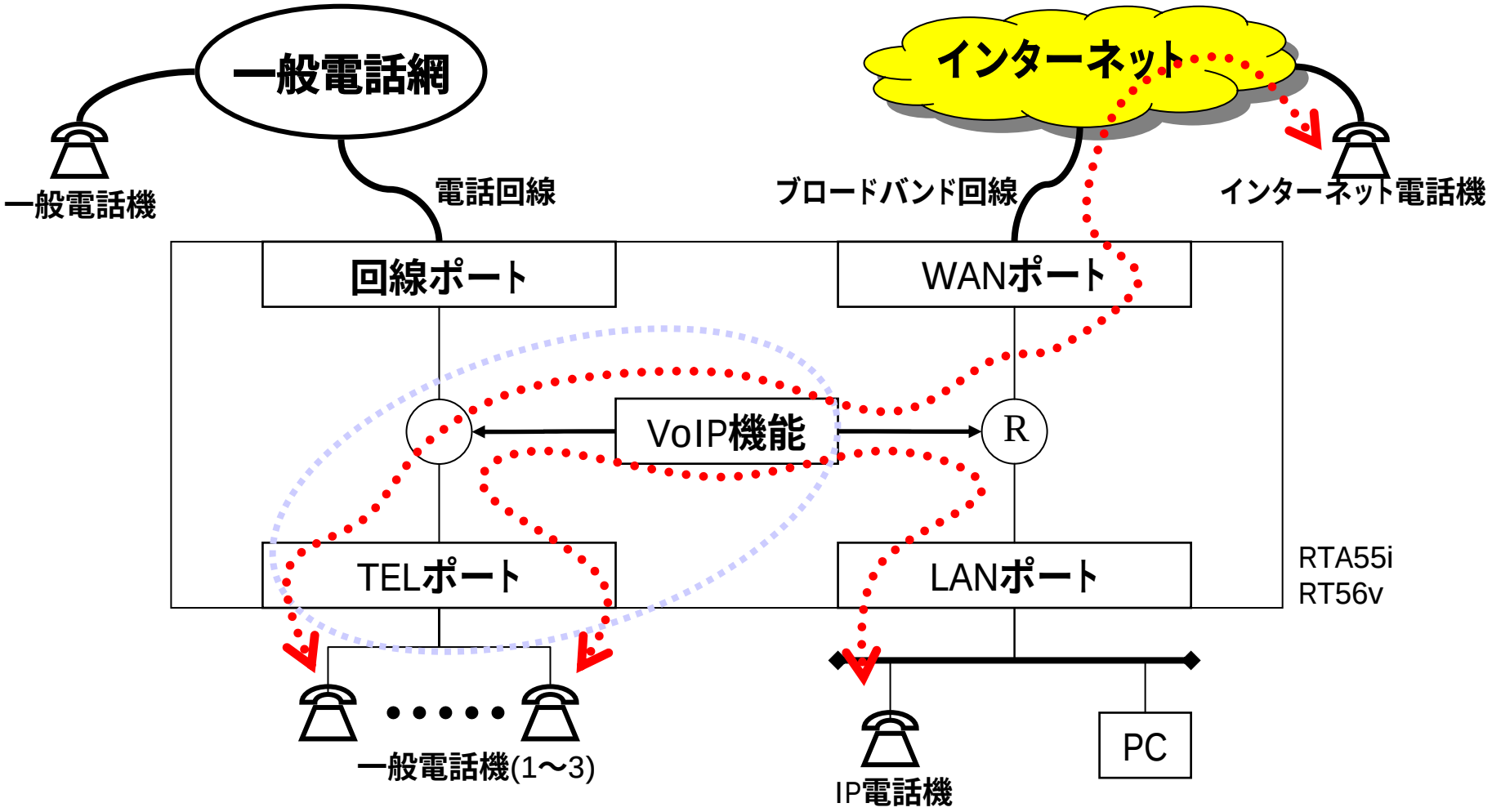
ブロードバンドルータの要素



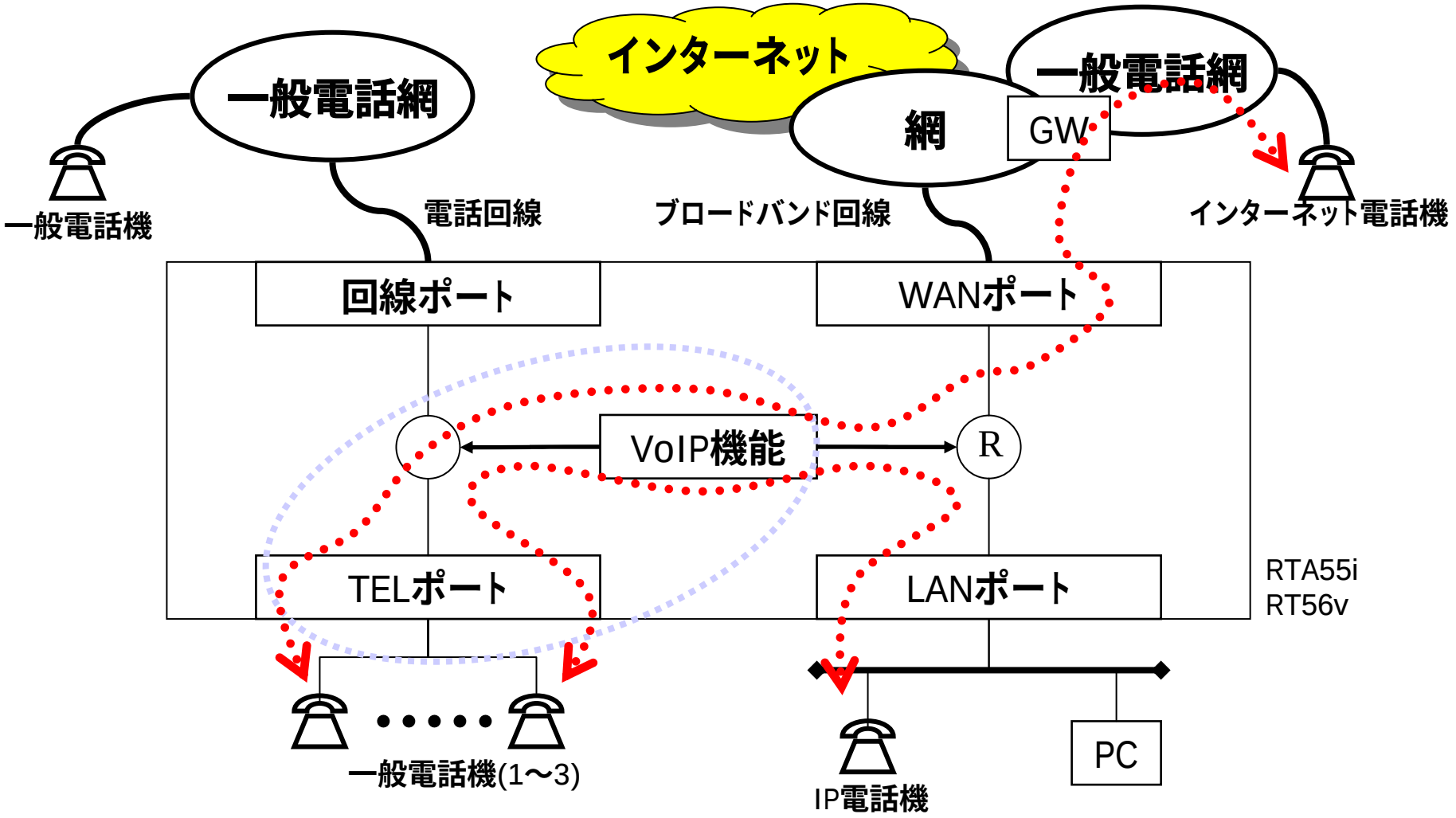
ビジネスホン/ホームテレホンの要素



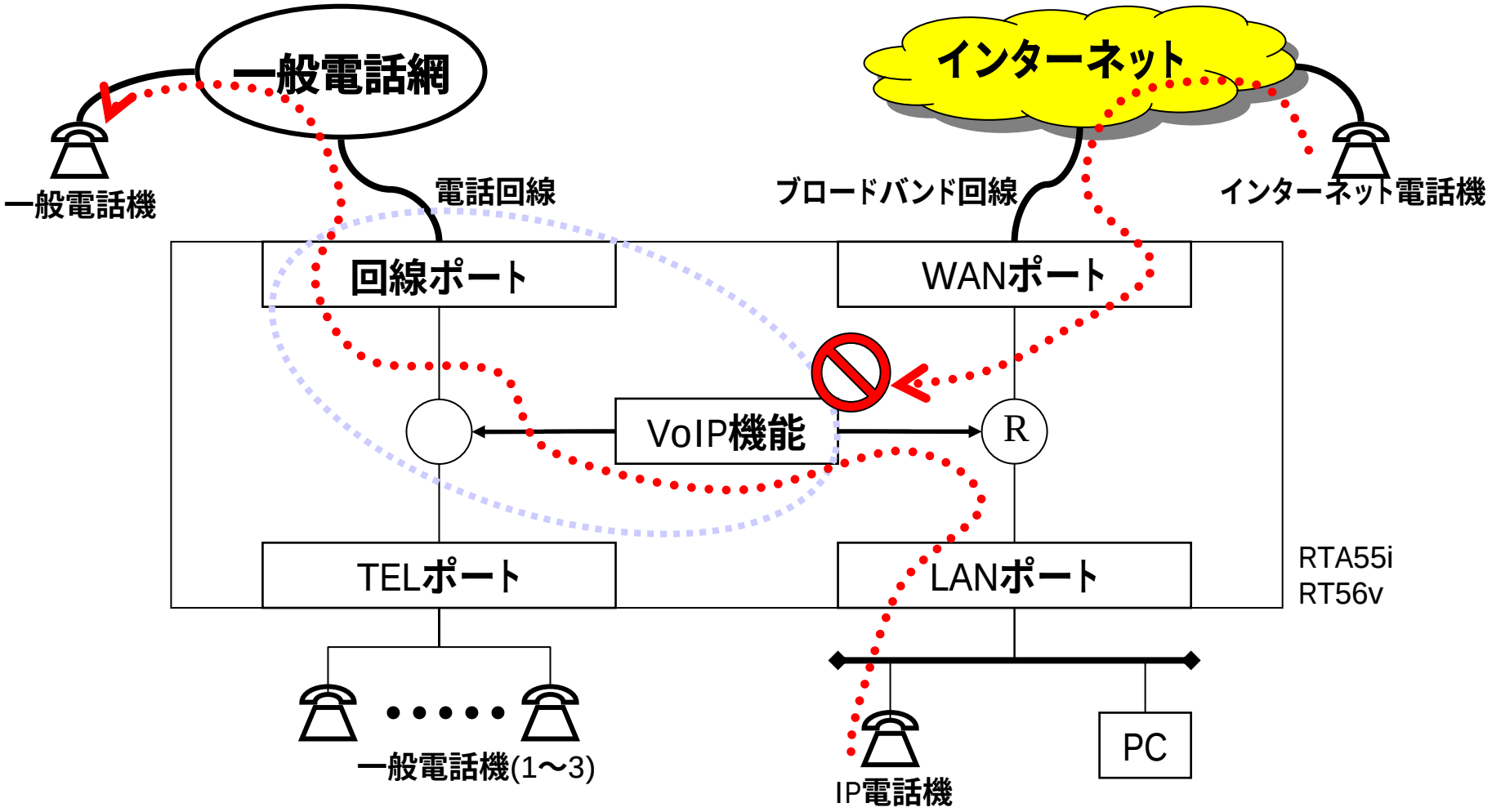
インターネット電話の要素(VoIP-TA,P2P)



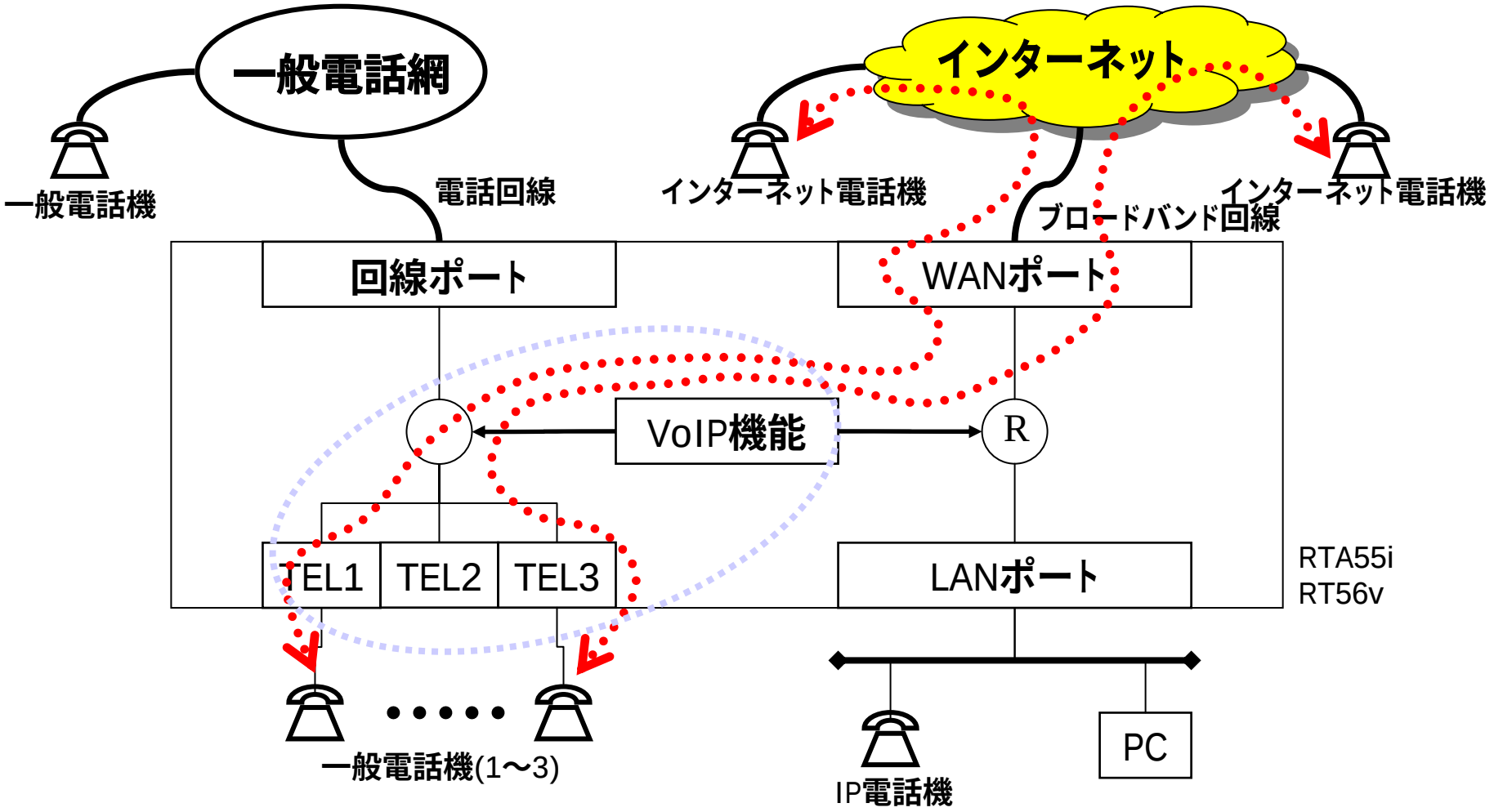
IP電話機の要素(VoIP-TA,SIPサーバ対応)



VoIPゲートウェイの要素(提供未定)

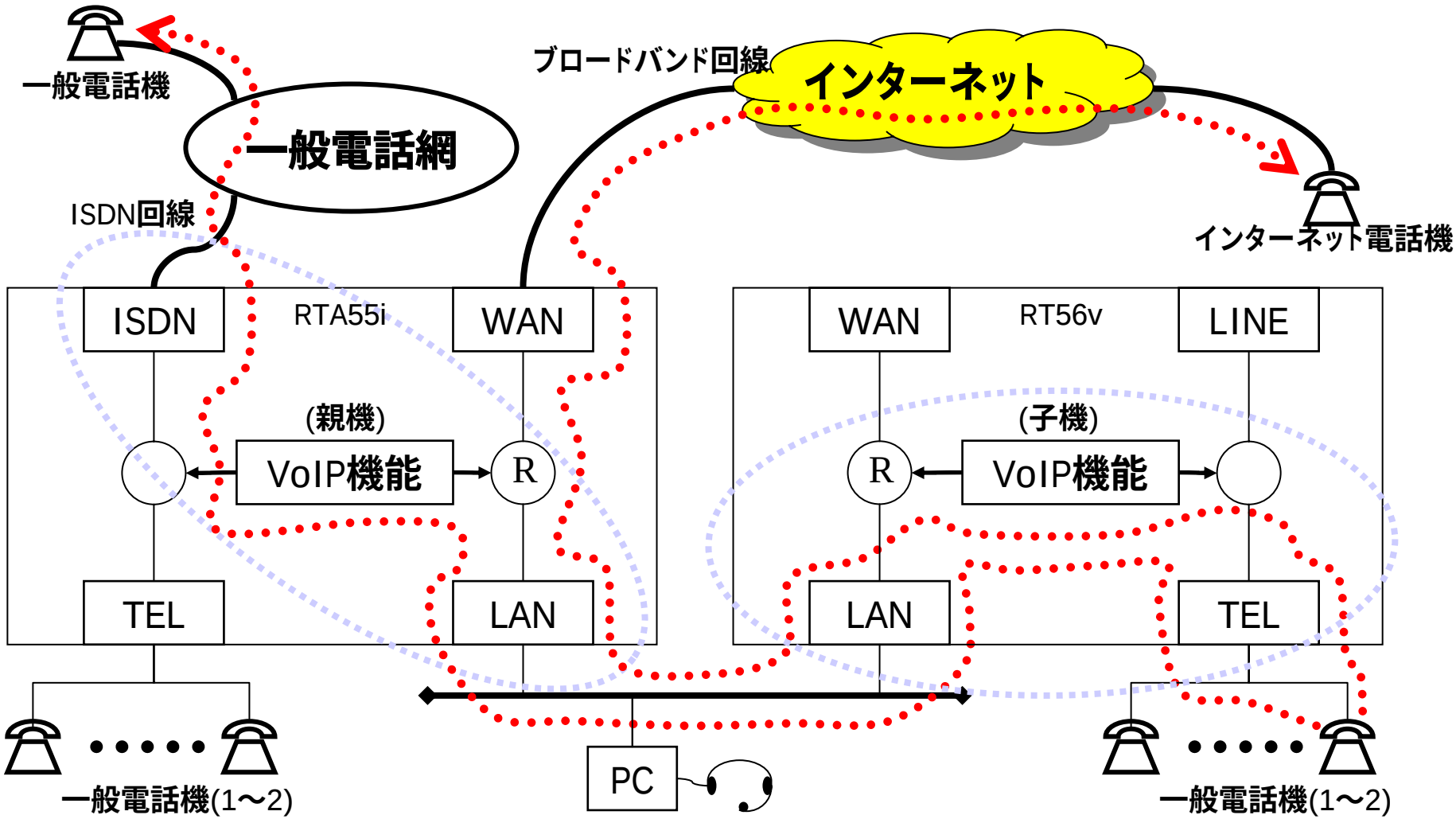


インターネット電話の同時通話

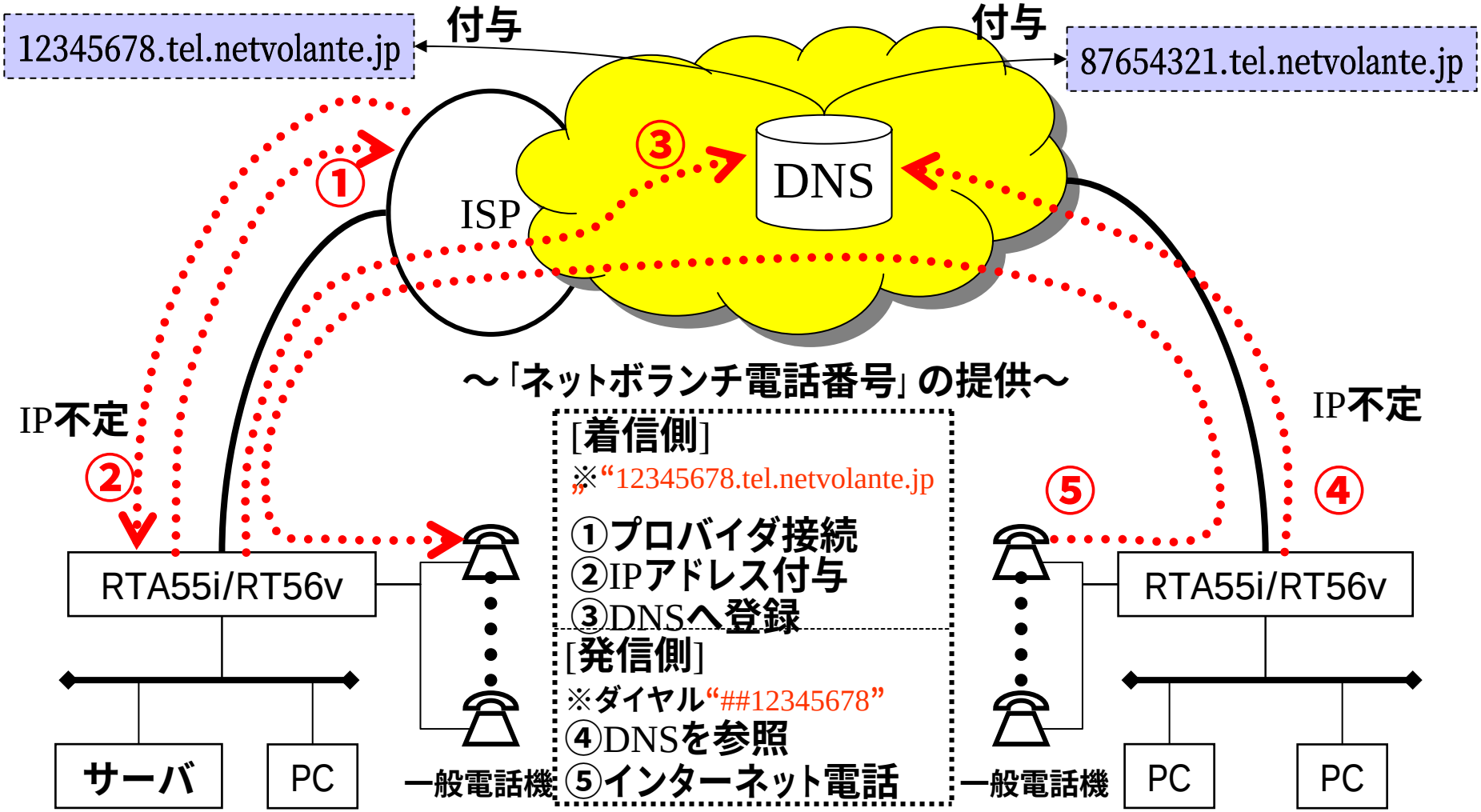


機器間アナログ通話(TELポートの増設)

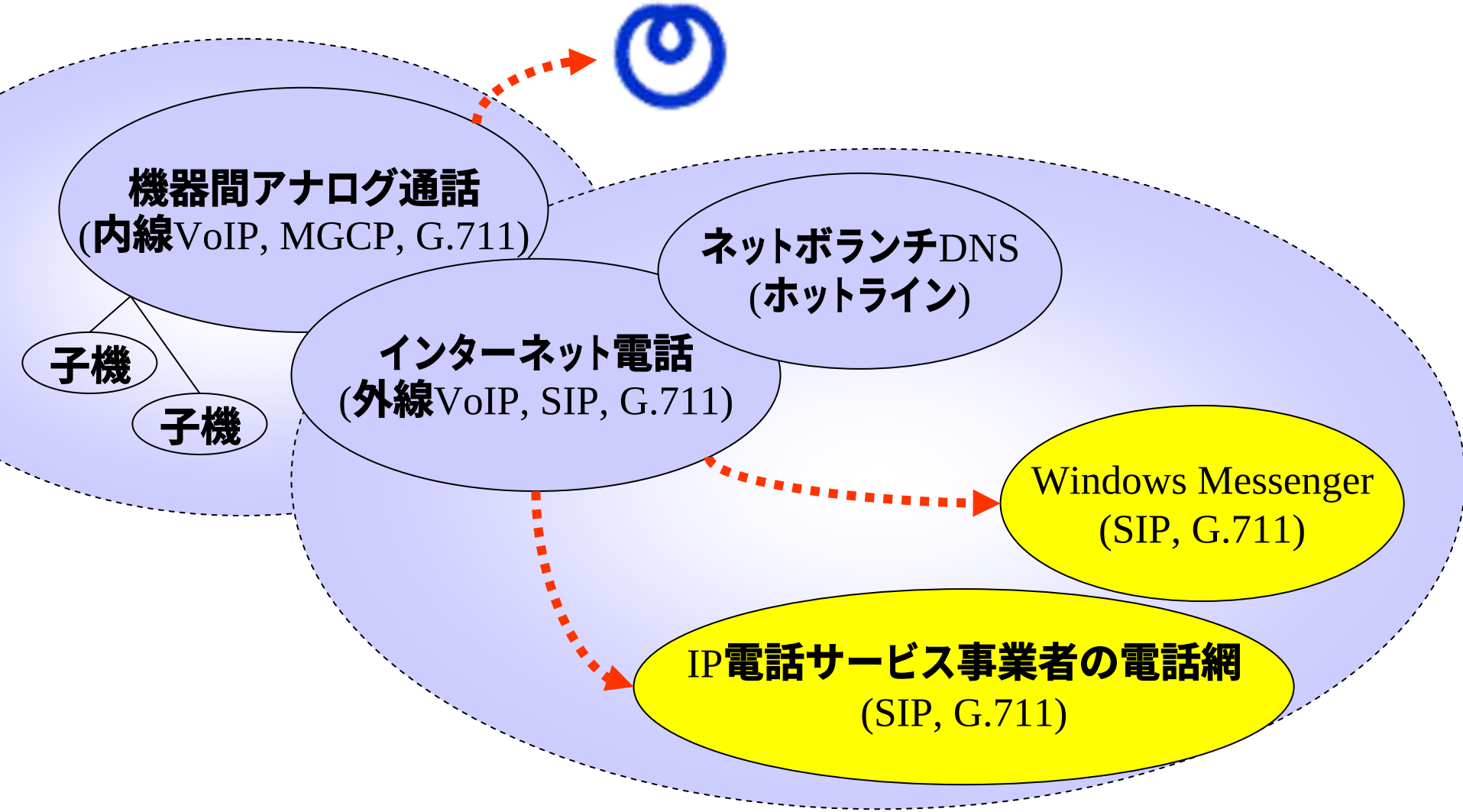
MGCP:Media Gateway Control Protocol、RFC2705
SIP:Session Initiation Protocol、RFC2543



ネットボランチDNSサービス
(電話アドレスサービス)



インターネット電話の将来性



VPNへの取り組み (ヤマハのVPN関連技術)

[外から見える取り組み]
1998年5月 IPsecによるVPN機能をRTシリーズで提供
　続けて、VPN内でのNAT機能、ファイアウォール機能、
　バックアップ機能、ダイヤルアップVPN機能などの拡張機能を提供
2002年春 PPTPによるVPN機能をRTシリーズで提供

ネットボランチのVPN機能

[要素]

◎ VPNプロトコルPPTPの相互接続性

Rev.6系RTシリーズ(RTX1000、RT300i、RT105シリーズ)など

Microsoft Windows系OS(Microsoft VPN Adapter)

MacOS X 10.2(対応予定)

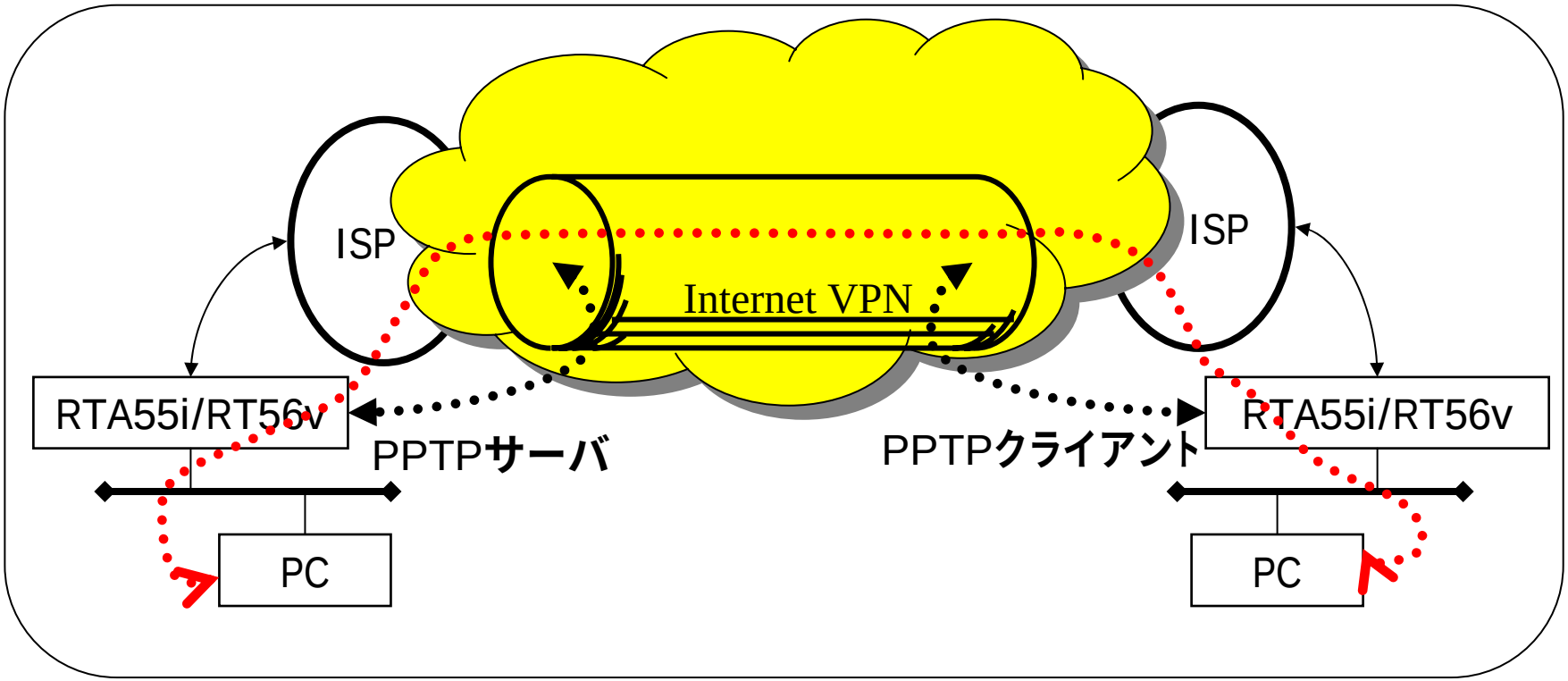
◎ 暗号機能:RC4 (RSAセキュリティ社よりライセンス)

Microsoft Windows系OS(Microsoft VPN Adapter)で必須

◎ ネットボランチDNSのホストアドレスサービス

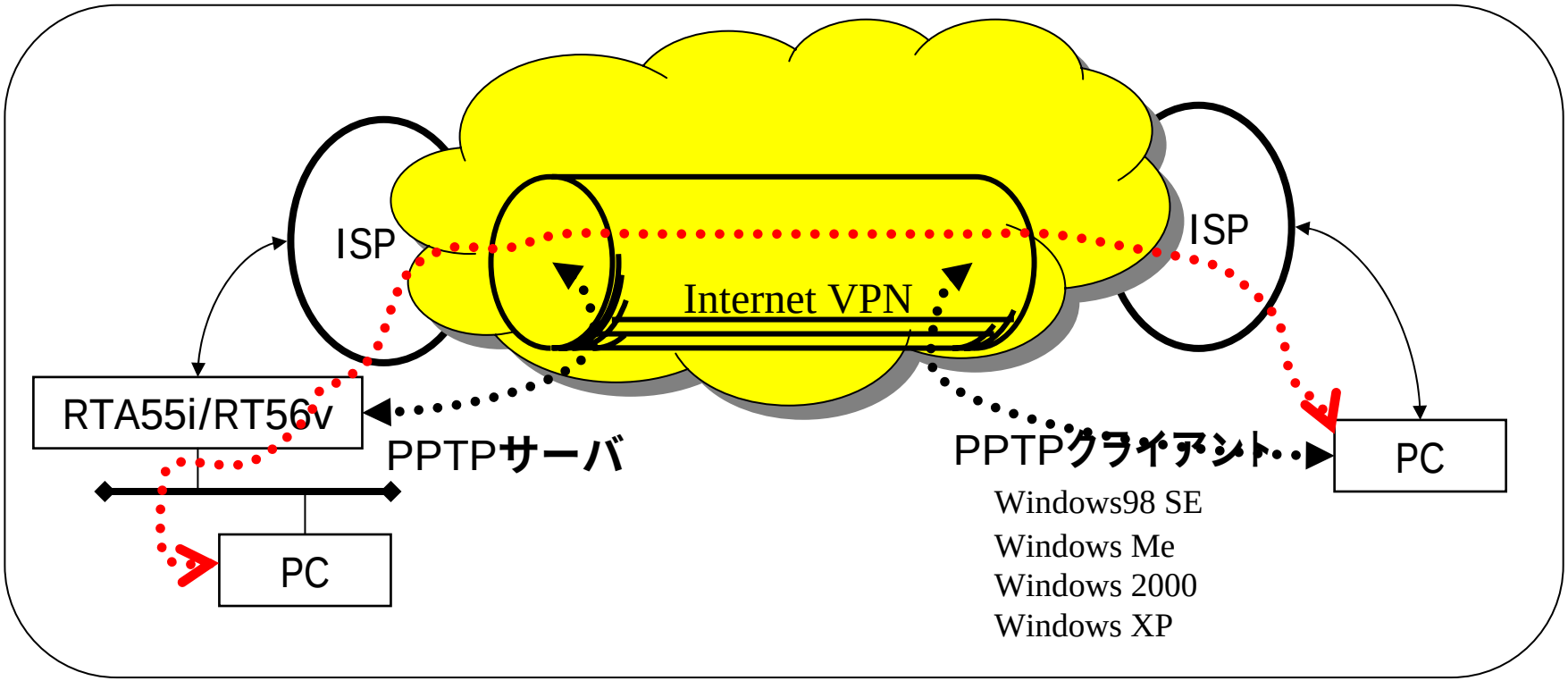
- LAN間接続VPN
- リモートアクセスVPN

LAN間接続VPN (PPTP+RC4)



PPTPによるLAN間接続VPNにより、遠隔地のPCとpeer to peer (P2P)の通信が可能になる。

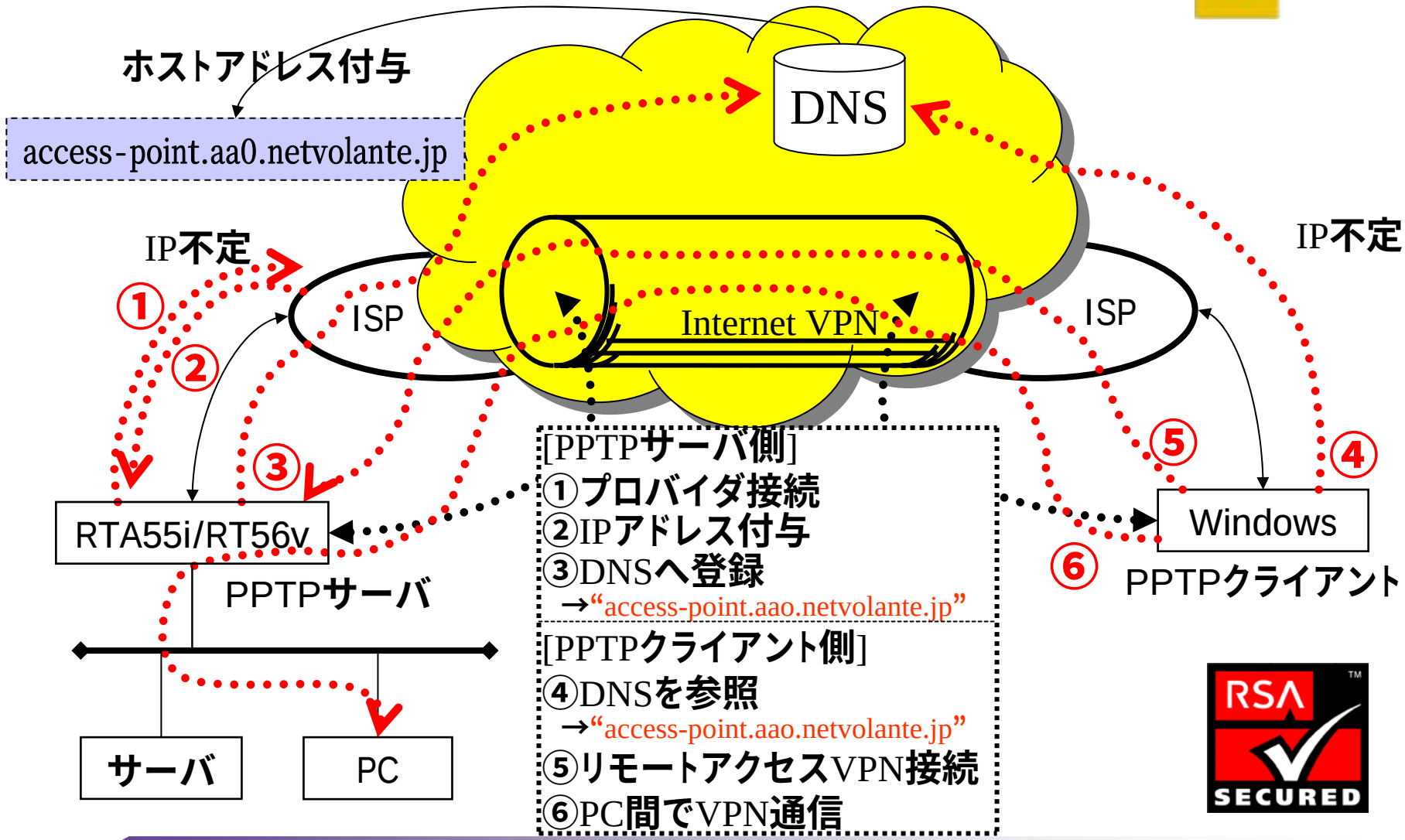
リモートアクセスVPN (PPTP+RC4)



PPTPによるリモートアクセスVPNにより、遠隔地のWindowsからpeer to peer (P2P)なリモートアクセスが可能になる。

※Windows 95/98は、MS-DUN 1.4が必要
http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q285189

ネットボランチDNSサービス
(ホストアドレスサービス)



新機能対応表






	RT60w	RTA54i	RTW65b	RTW65i	RTA55i	RT56v
ISDN	○	○	－	○	○	－
LINE	－	－	－	－	－	○
WAN	△	○	○	○	○	○
TEL	3	2	－	3	2	3
LAN	4	4	1	1	4(SW)	4(SW)
無線LAN	○	－	○	○	－	－
USB	－	○	○	○	○	－
ネットボランチ DNS	○	○	○	○	○	○
インターネット電話 (VoIP)	○	○	－	○	○	○
VPN (PPTP+RC4)	－	－	○	○	○	○

スループット値

機種	リビジョン	最大	実効
RTA55i	Rev.4.06.15	12.0Mbps	8.5Mbps
RT56v	Rev.4.07.08	12.0Mbps	8.5Mbps
RTA54i	Rev.4.03.10	5.5Mbps	4.0Mbps
	Rev.4.04.05	6.0Mbps	4.5Mbps
RTW65b	Rev.5.03.10	7.5Mbps	5.5Mbps
RTW65i	Rev.5.03.10	7.0Mbps	5.0Mbps

最大: アドレス変換なし、フィルタ設定なし(ローカル・ルータ)
実効: アドレス変換あり、フィルタ設定あり(CATV型セキュリティレベル4)
※スループットは使用環境によって異なる場合がある。
セキュリティレベル6/7の実効スループットは、レベル4より高い。

ネットボランチ RTA55i/RT56v
いろいろな機能や使い方

		RTA55i	RT56v
WAN ポート	・CATV ・ADSL/フレッツ・ADSL ・FTTH/Bフレッツ	OK	OK
ISDN ポート	・ISDN/フレッツ・ISDN ・128kbps専用線 ・OCNエコノミー ・ISDNによるLAN間接続 ・ISDNによるダイヤルアップサーバ	OK	×

ネットボランチのかんたん設定

- ユーザフレンドリーなコンセプト
  - a)設定/使い方の統一
    回線や用途が変わっても、変わらない操作性
  - b)使い方で分類された階層構造
  - c)全体が見渡せ、位置を知らせるメニューシステム
    「くすだま」「いまどこ」
  - d)多様なメニューモード
- セキュリティレベルの簡単操作で高度なセキュリティ
- 丁寧で扱いやすいファイアウォール編集機能
- 便利な付加機能(メール機能、ブザー通知)
- 多機能な管理画面(コマンド設定/入力、ログ)

NetVolanteの入出力一覧

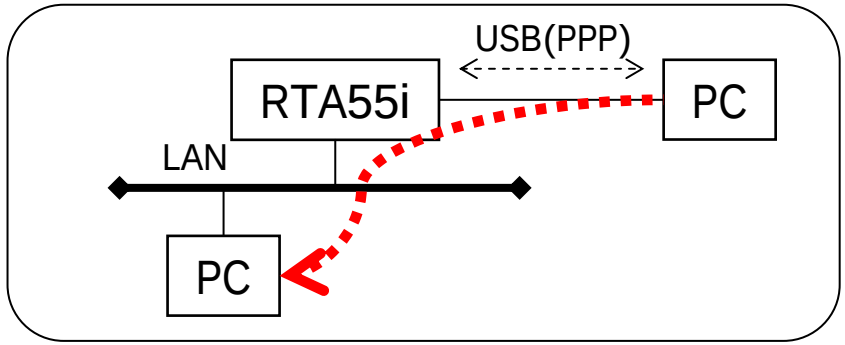
	RTA55i	RT56v	RTW65b	RTW65i
ISDN回線	1	–	–	1
アナログ回線	–	1	–	–
TELポート	2	3	–	3
WANポート	1	1	1	1
LANポート	4 (スイッチ)	4 (スイッチ)	1	1
無線LAN (IEEE 802.11b)	–	–	1	1
USBポート	1	–	1	1
LED	8(前)+4(後)	6(前)+5(後)	7	9

NetVolanteにおけるUSBポート

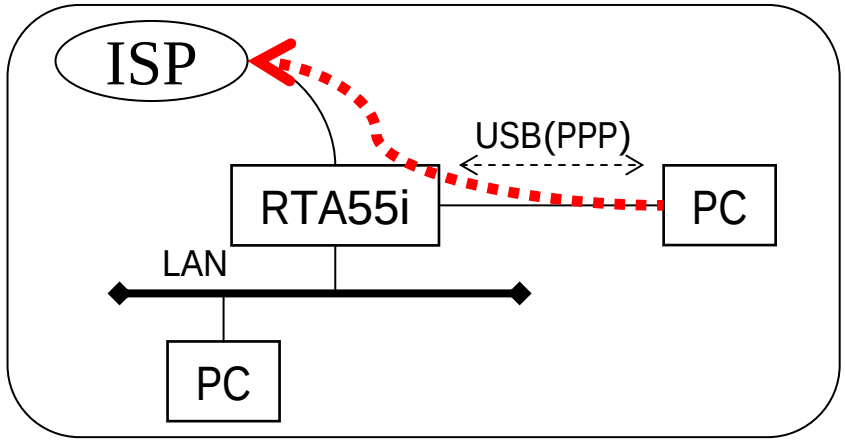
[用途]

- **a) ISDN-TA機能**
- **b) ブロードバンドTA**
- **c) 擬似LAN機能**
- **d) コンソール操作(設定)**

	RTA55i	RT56v
USBポート	OK	×

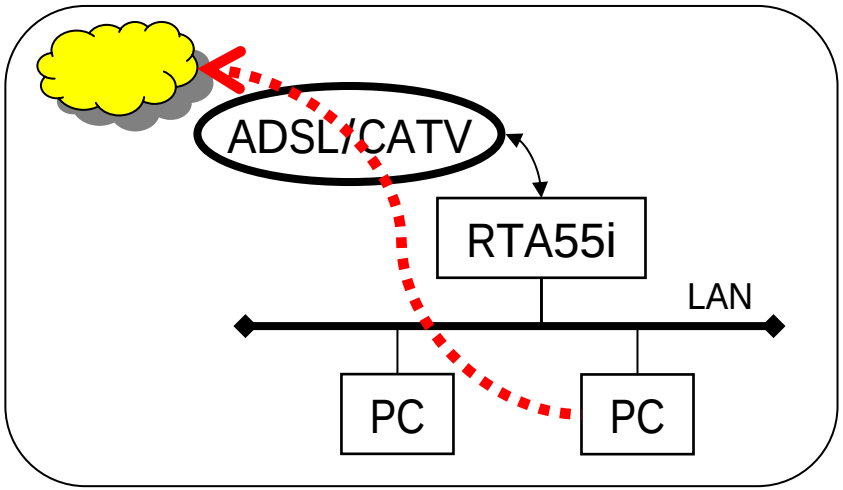


USBの擬似LAN→LANアクセス

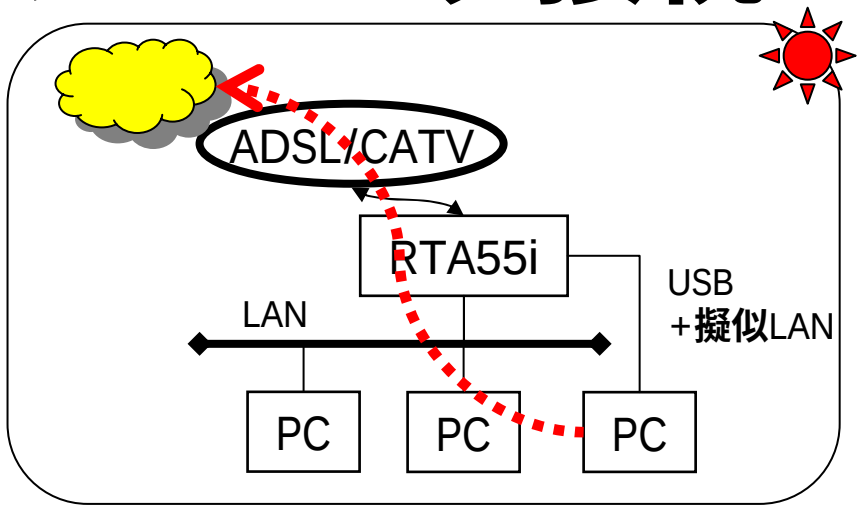


USBの擬似LAN→インターネットアクセス

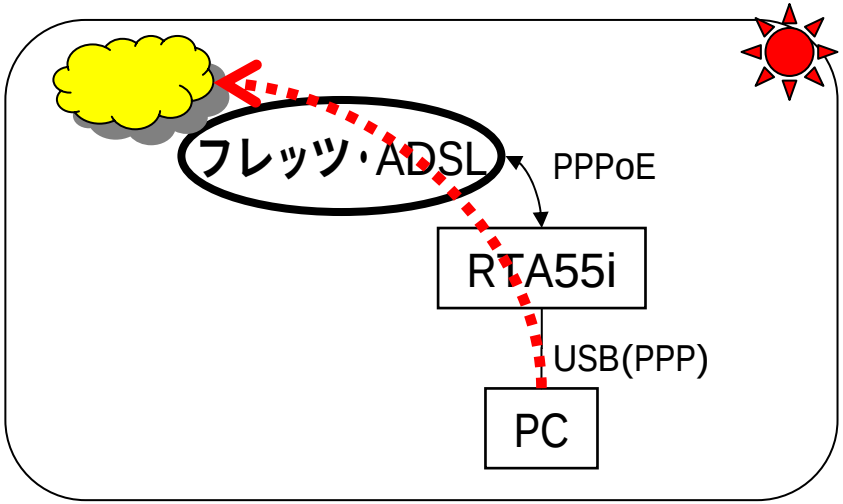
ブロードバンドのプロバイダ接続



ADSL/CATV**プロバイダ接続**(LAN)

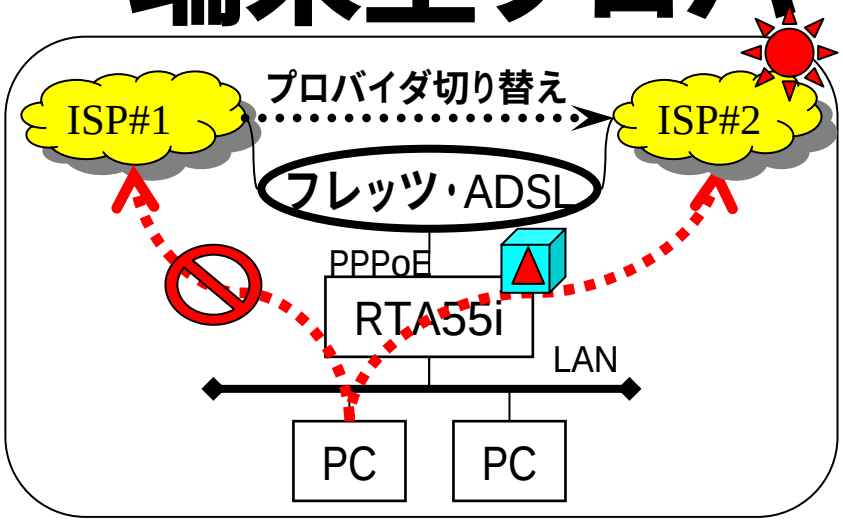


ADSL/CATV**プロバイダ接続**(USB**の擬似**LAN)

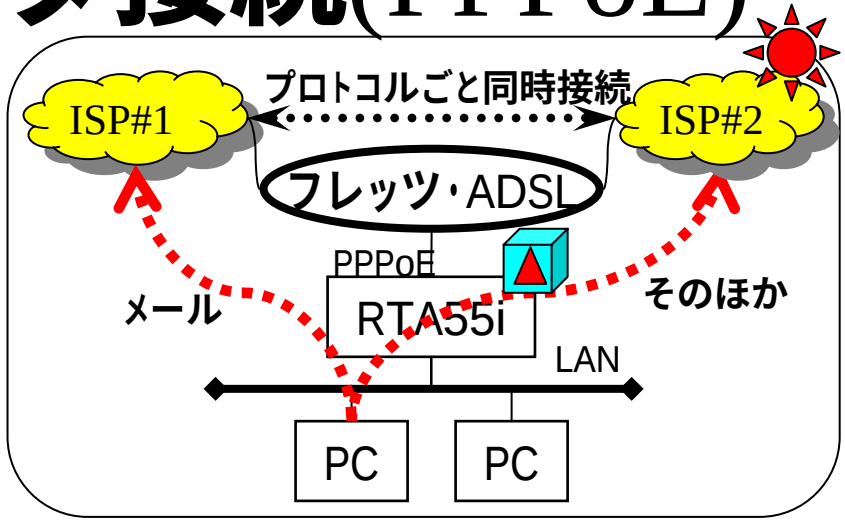


ブロードバンドTA(**フレッツ**・ADSL,USB)

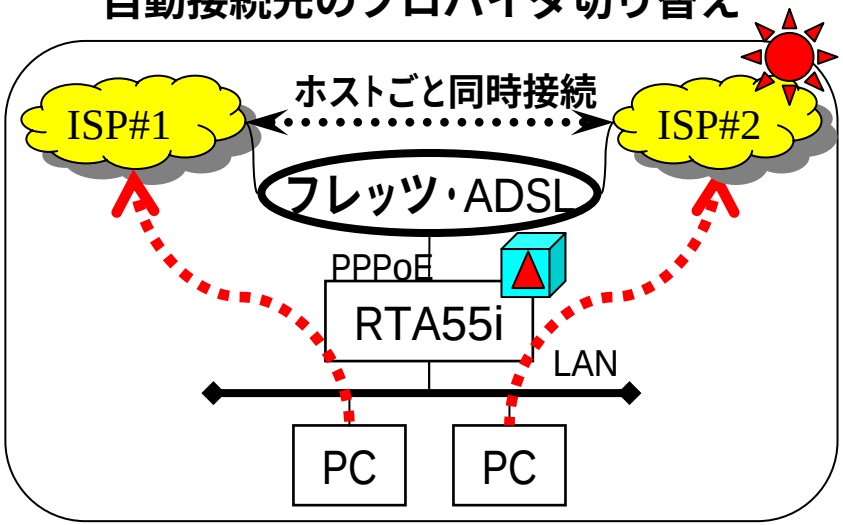
端末型プロバイダ接続(PPPoE)



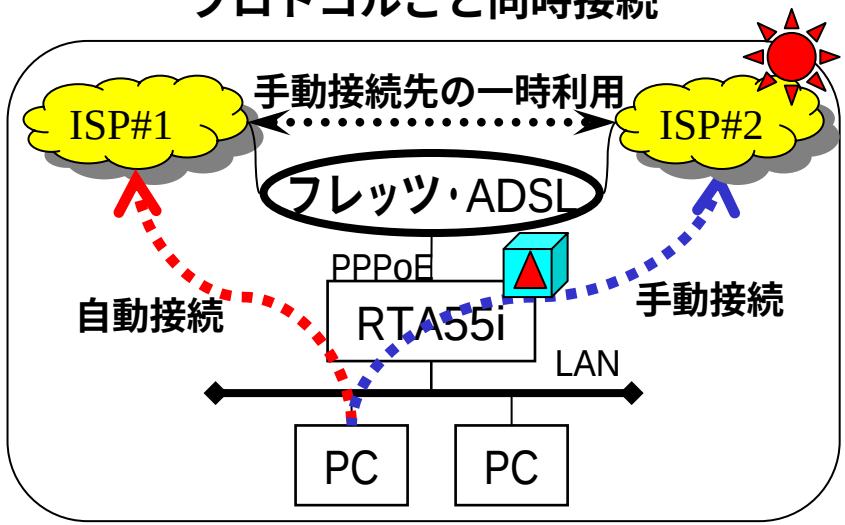
自動接続先のプロバイダ切り替え



プロトコルごと同時接続

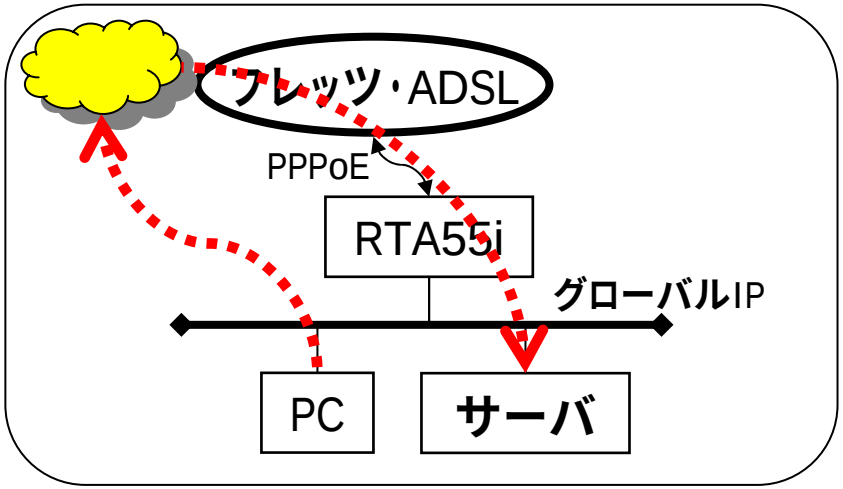


ホストごと同時接続

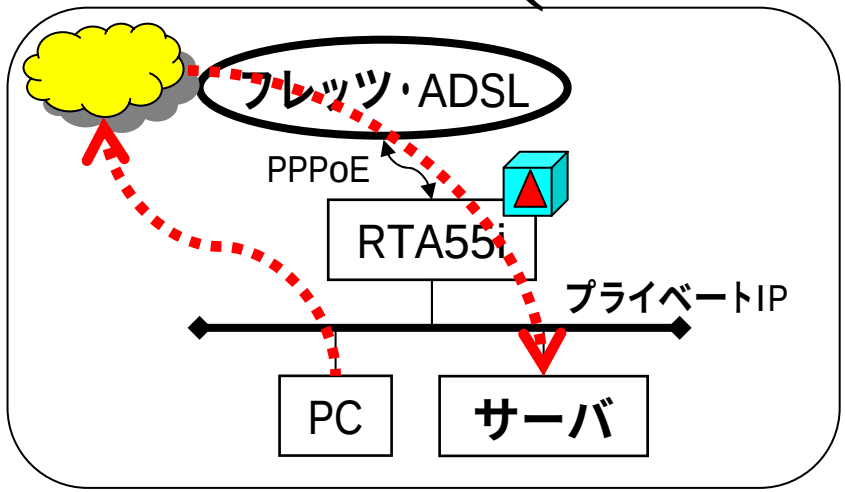


手動接続先の一時切り替え

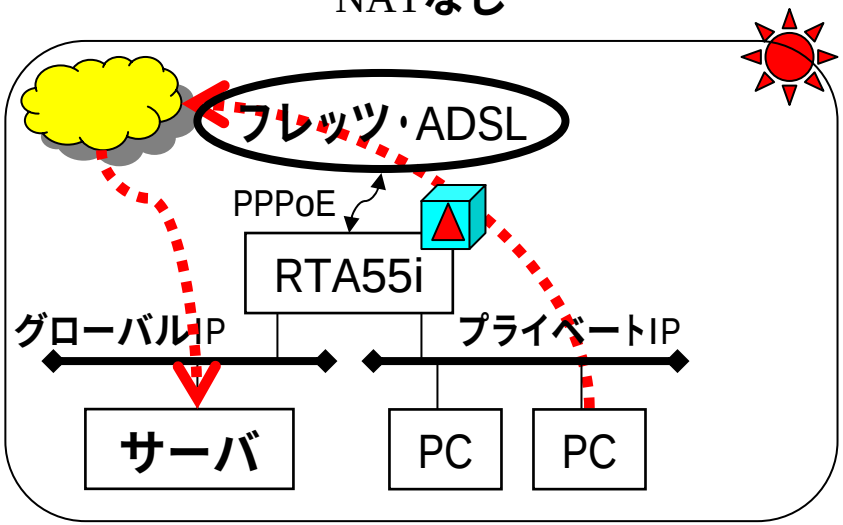
ネットワーク型プロバイダ接続(PPPoE)



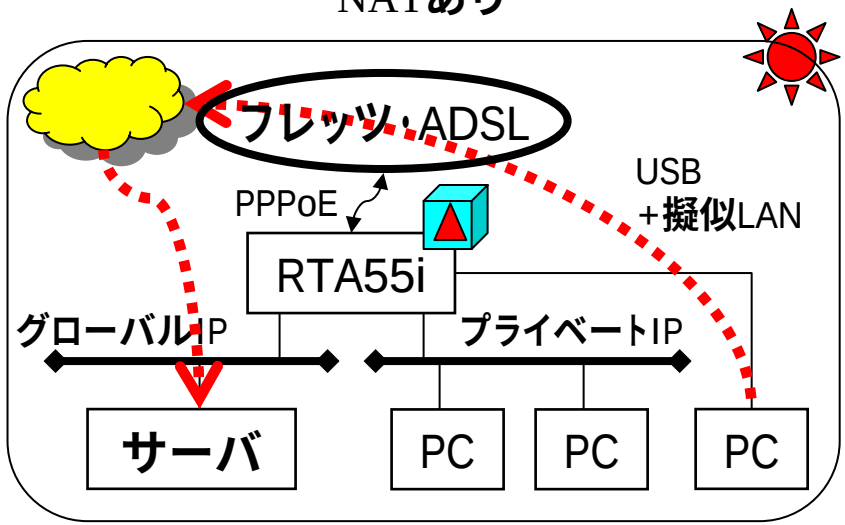
NATなし



NATあり

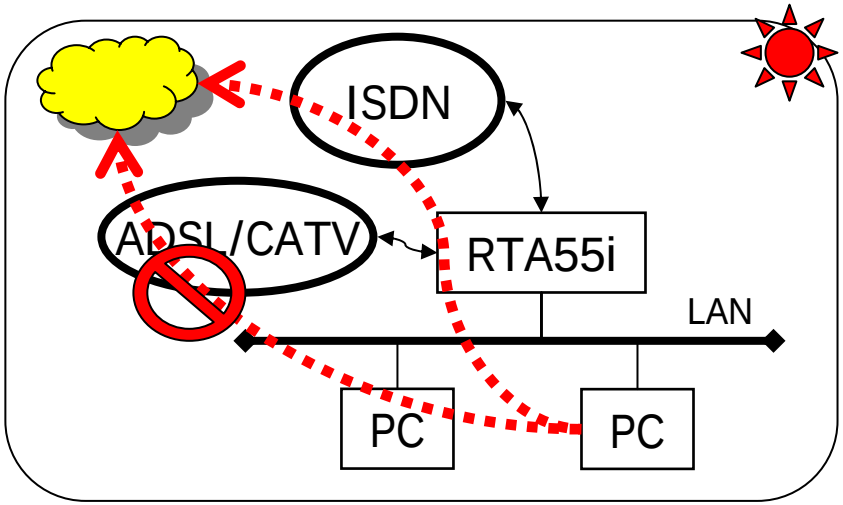


NATなし&あり(primary/secondary)

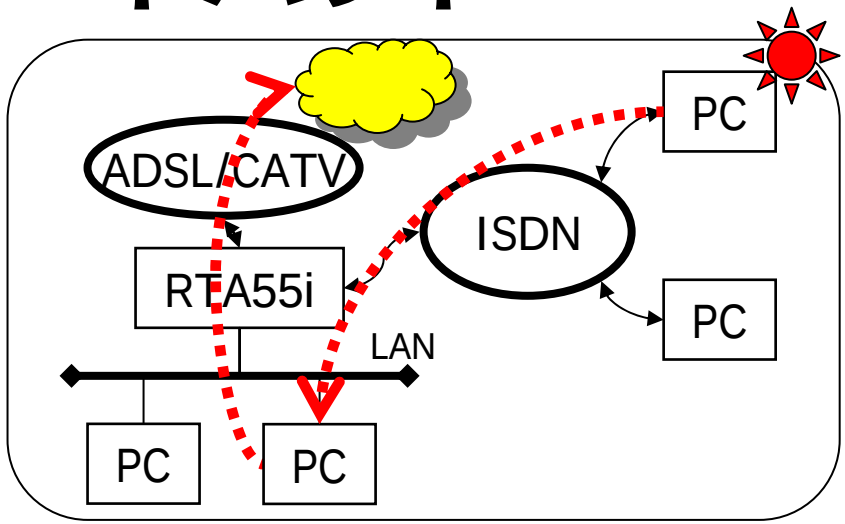


NATなし&あり(USB+擬似LAN)

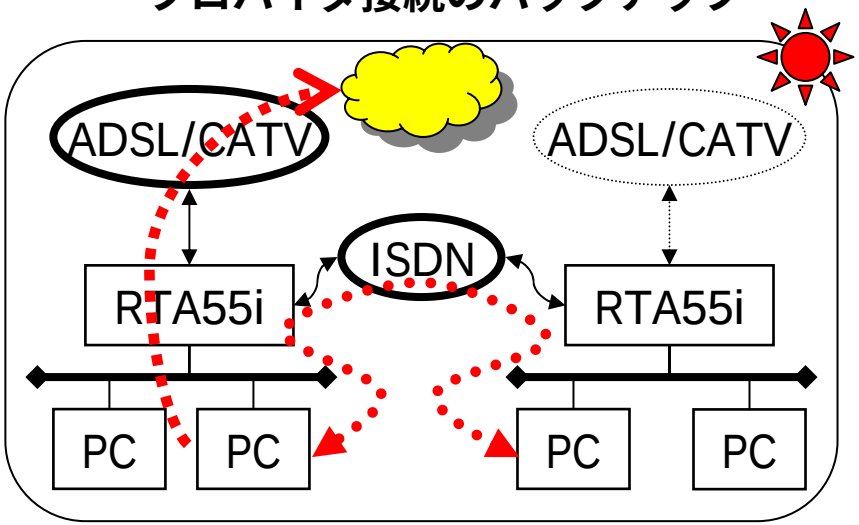
ISDN+ブロードバンド



プロバイダ接続のバックアップ

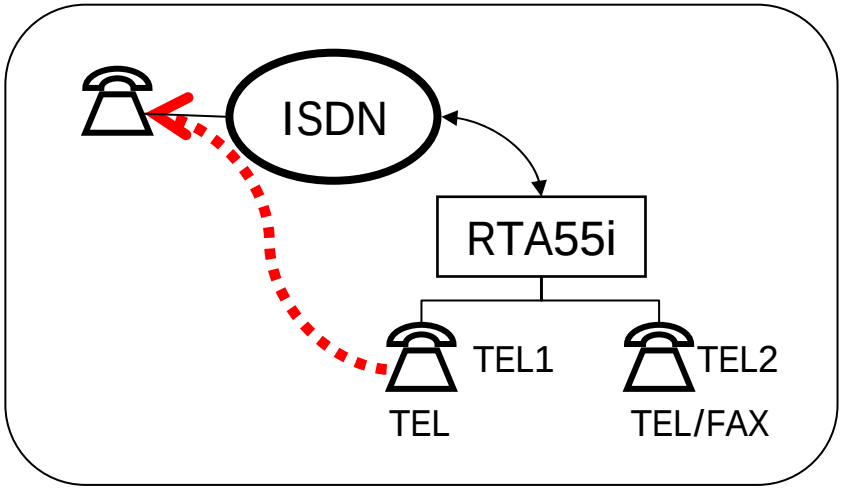


プロバイダ接続+リモートアクセスサーバ

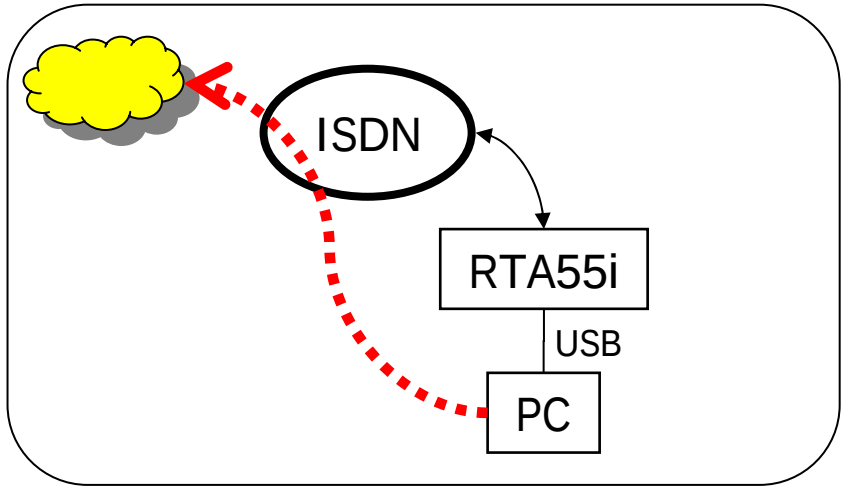


プロバイダ接続+LAN間接続

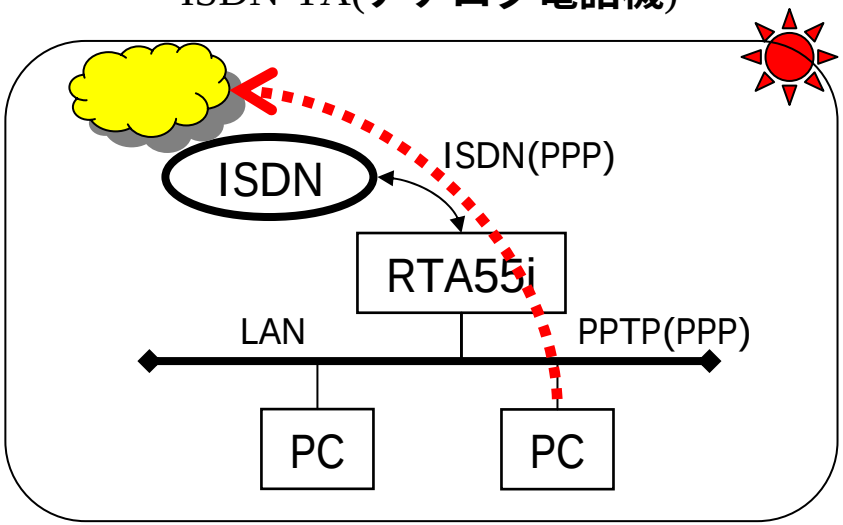
ISDN回線の基本



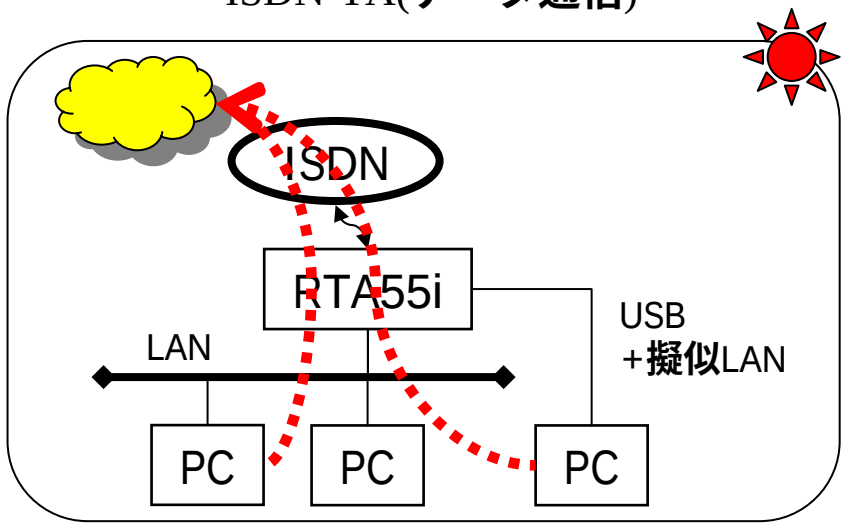
ISDN-TA(**アナログ電話機**)



ISDN-TA(**データ通信**)

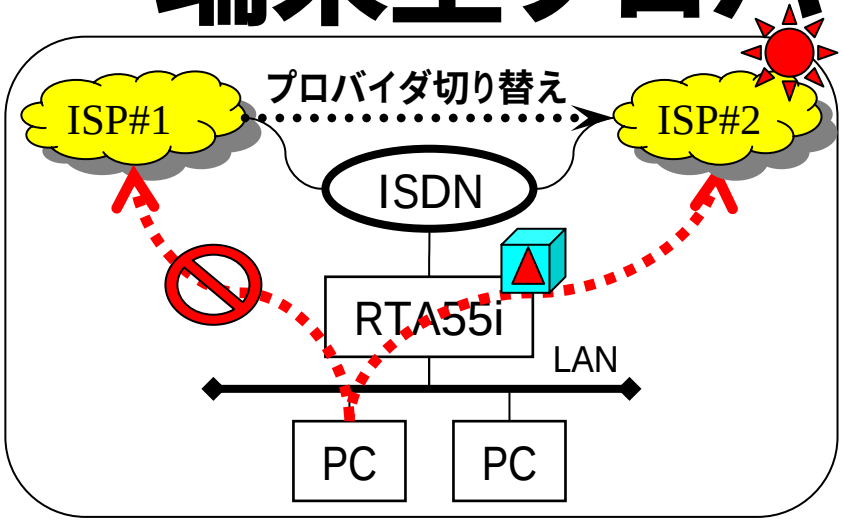


LAN-TA (PPTP client,MS VPN Adapter)

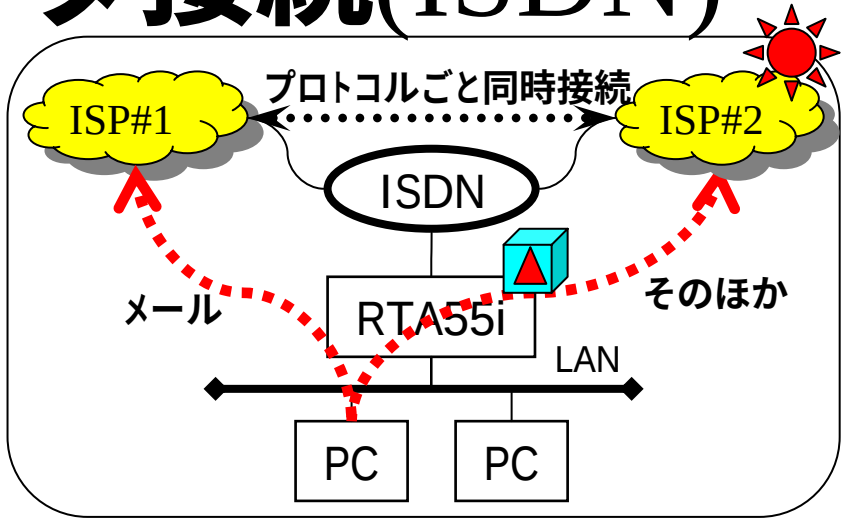


ダイヤルアップ・プロバイダ接続(LAN/USB)

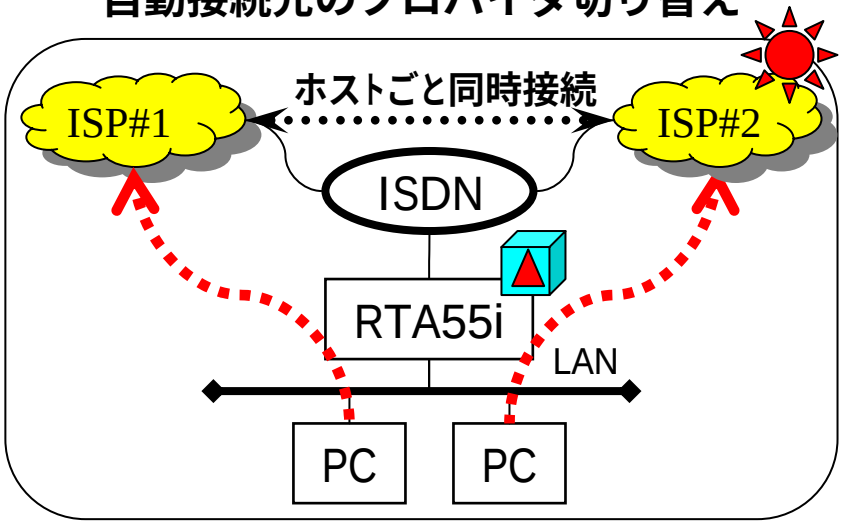
端末型プロバイダ接続(ISDN)



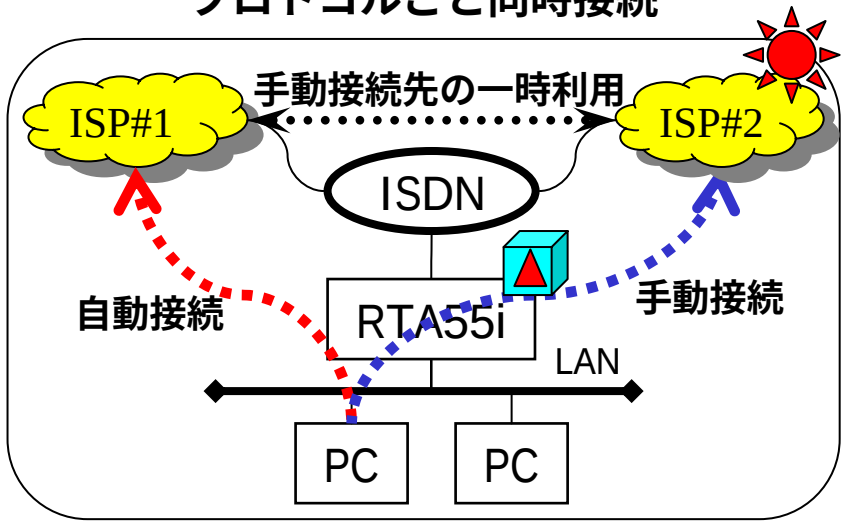
自動接続先のプロバイダ切り替え



プロトコルごと同時接続

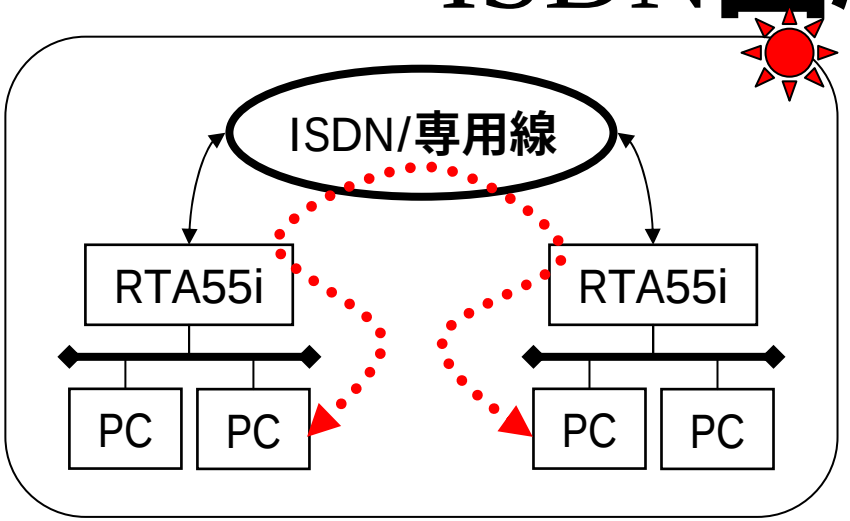


ホストごと同時接続

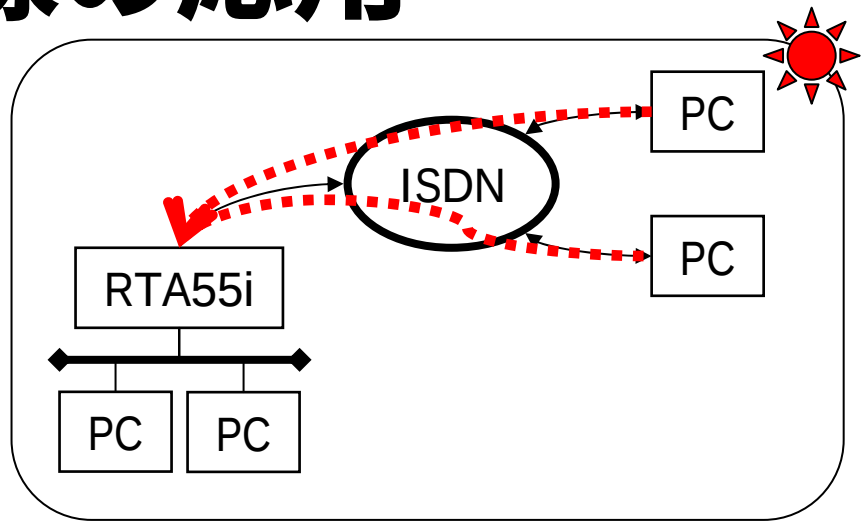


手動接続先の一時切り替え

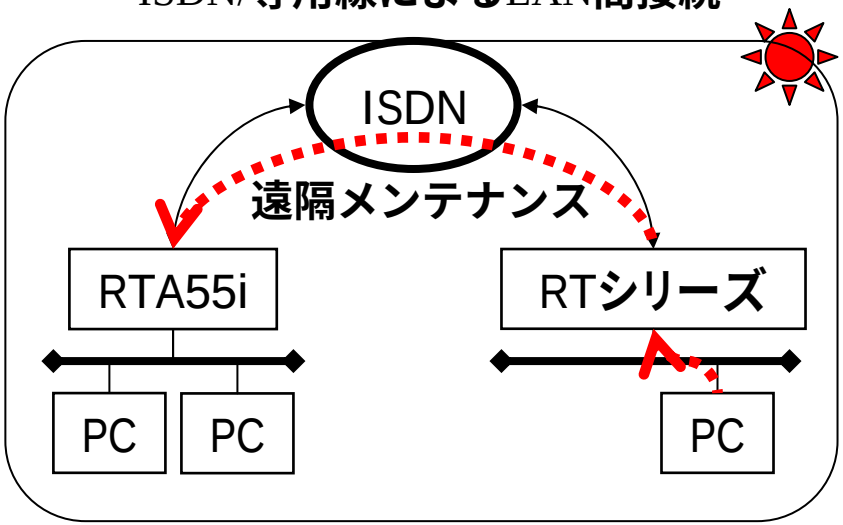
ISDN回線の応用



ISDN/専用線によるLAN間接続

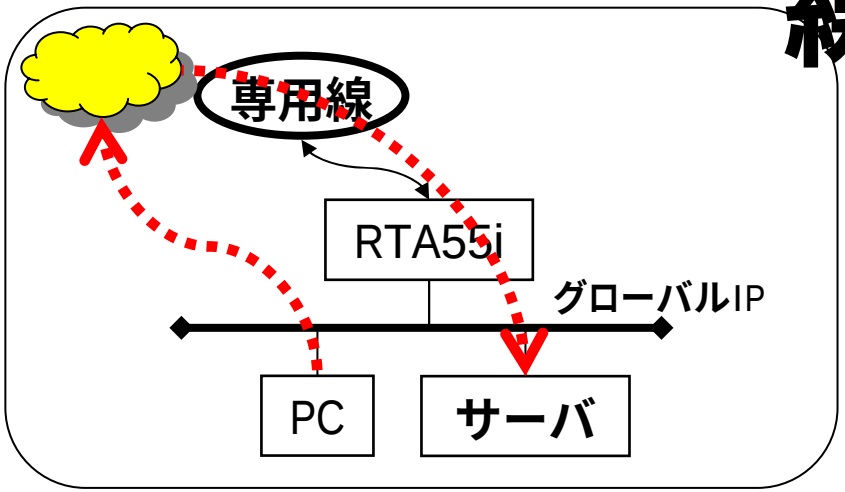


ダイヤルアップサーバ

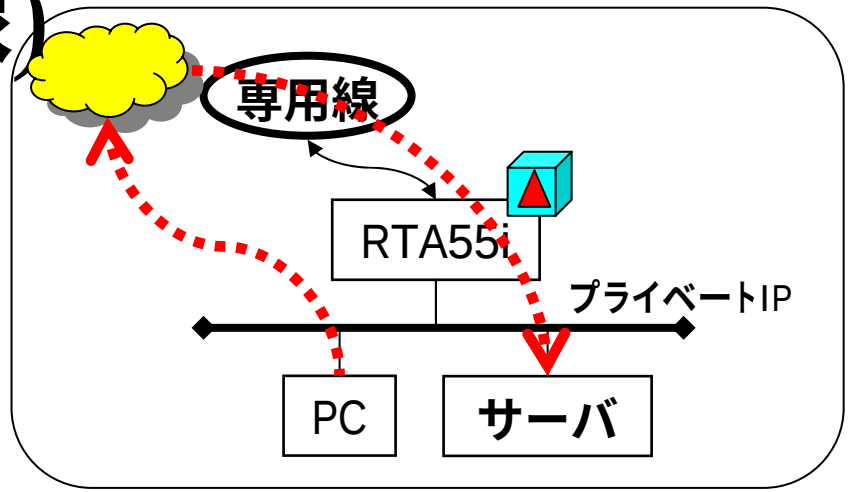


リモートセットアップ

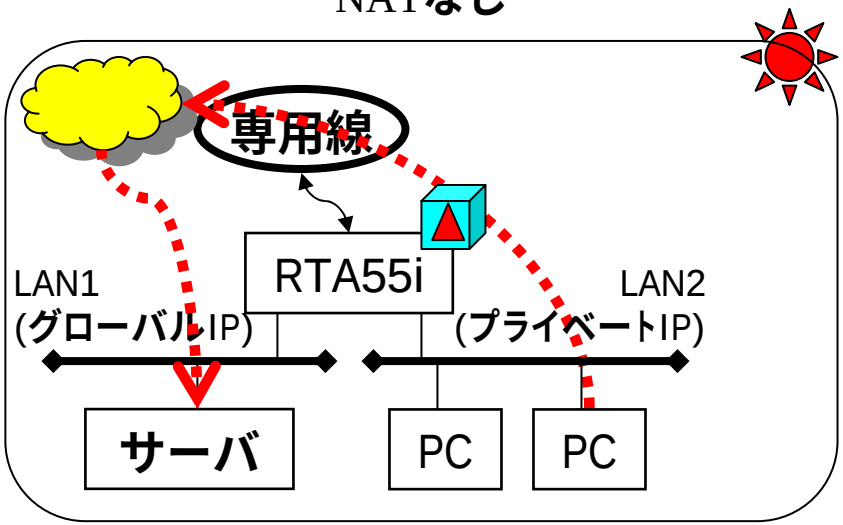
ネットワーク型プロバイダ接続(専用線)



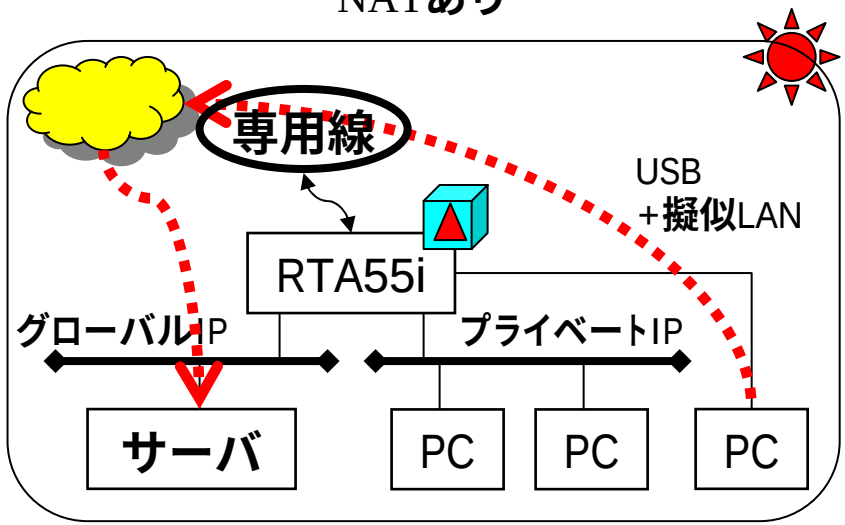
NATなし



NATあり



NATなし&あり(LAN1/LAN2)



NATなし&あり(USB+擬似LAN)

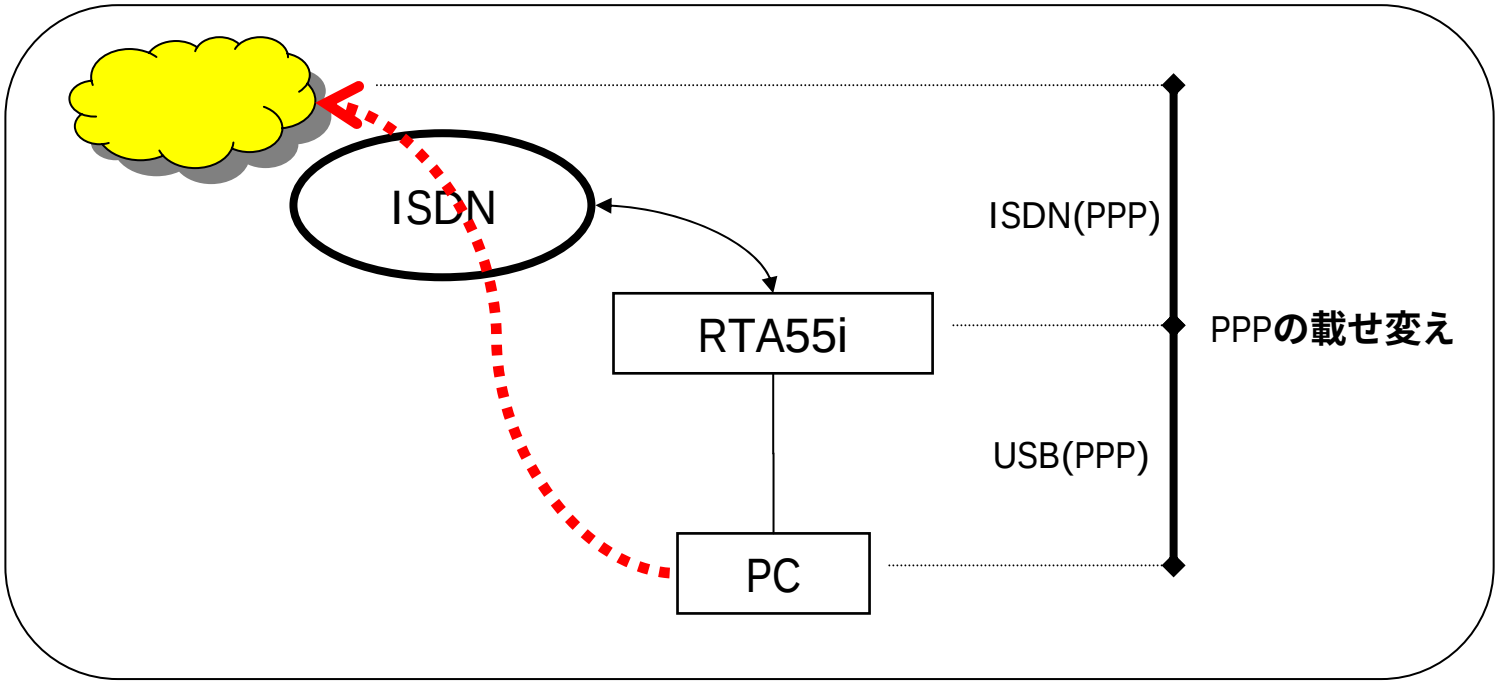
ネットボランチのネットアプリ対応

1) ISDN-TA
2) LAN-TA機能
3) ブロードバンドTA
4) IPマスカレード対応
   ・静的IPマスカレード
   ・IPマスカレードの例外処理(パケット書き換えなど)
     ping,traceroute,ftp,CU-SeeMe,NetMeeting Version 3.0,など
5) DMZホスト機能

	RTA55i	RT56v
ISDN-TA	OK	×
LAN-TA	OK	×
ブロードバンドTA	OK	×
IPマスカレード	OK	OK
DMZホスト機能	OK	OK

ISDN-TA(データ通信)

	RTA55i	RT56v
ISDNポート	OK	×
USBポート	OK	×

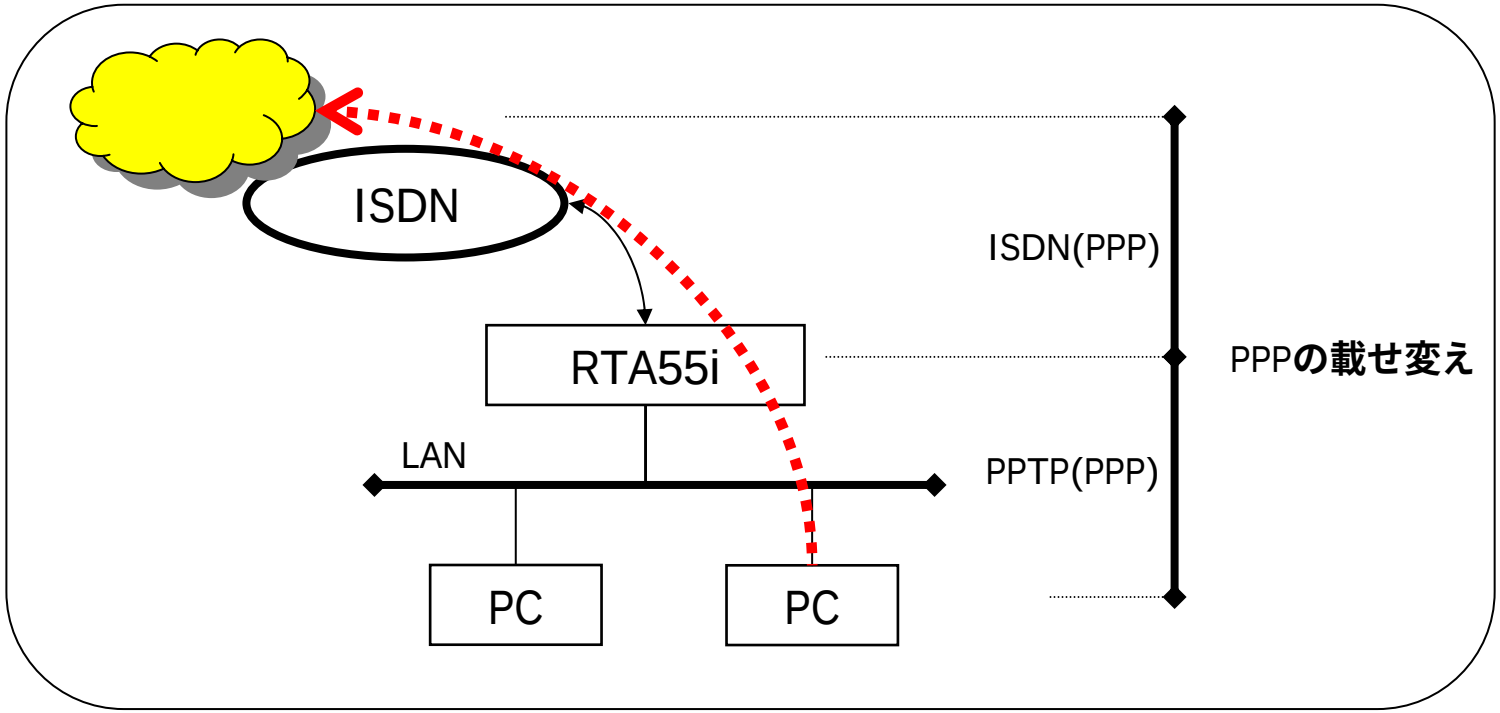


モデムと同等のPPP接続(PPP Adapterおよびダイヤルアップネットワーク)が可能となる機能

http://www.rtpro.yamaha.co.jp/RT/FAQ/USB-TA/index.html

LAN-TA機能

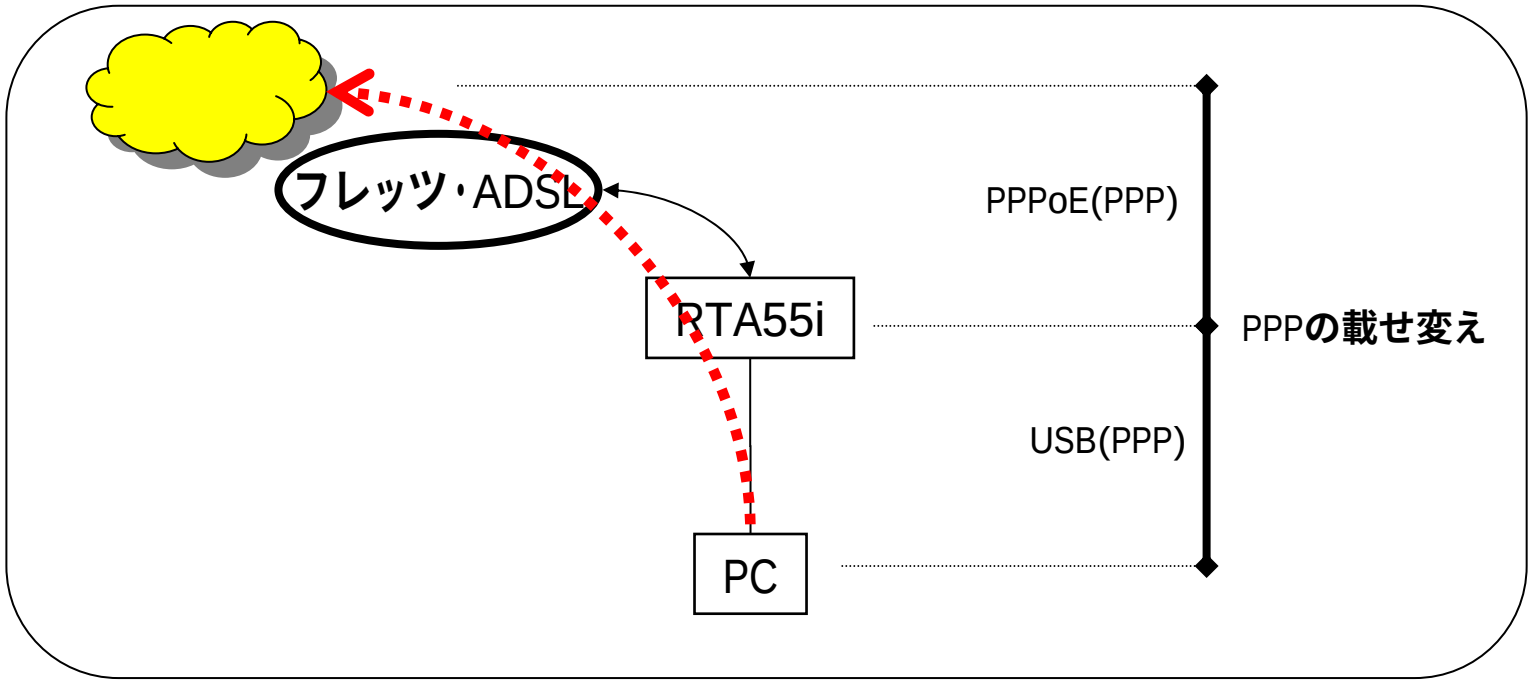
	RTA55i	RT56v
ISDNポート	OK	×



Microsoft社のWindows95やWindows98などの「Microsoft (R) VPN Adapter/マイクロソフト(R)仮想プライベートネットワーク」という機能を利用して、LAN上の端末(Windows)からISDN-TAやモデムなどと同等のPPP接続(PPP Adapter およびダイヤルアップネットワーク)が可能となる機能

ブロードバンドTA

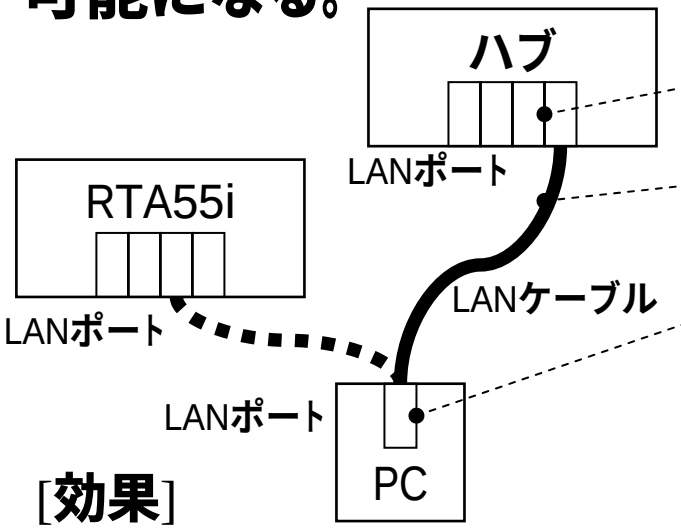
	RTA55i	RT56v
USBポート	OK	×



フレッツ・ADSLやBフレッツなどで利用されるPPPoEをISDN-TAやモデムなどと同等のPPP接続(PPP Adapterおよびダイヤルアップネットワーク)が可能となる機能

MDI/MDI-X自動判別機能

LANポート(内蔵L2スイッチングハブ)に接続されたケーブルや機器のMDIとMDI-X状態に依存しないで、常に適切な接続が可能になる。



条件					
	ハブ	=	X	=	X
	ケーブル	=	=	X	X
	PC	X	X	X	X
結果	通常	OK	NG	OK	NG
	自動判別	→ OK			

[効果]
- 配線がかんたん
- 配線ミスの軽減

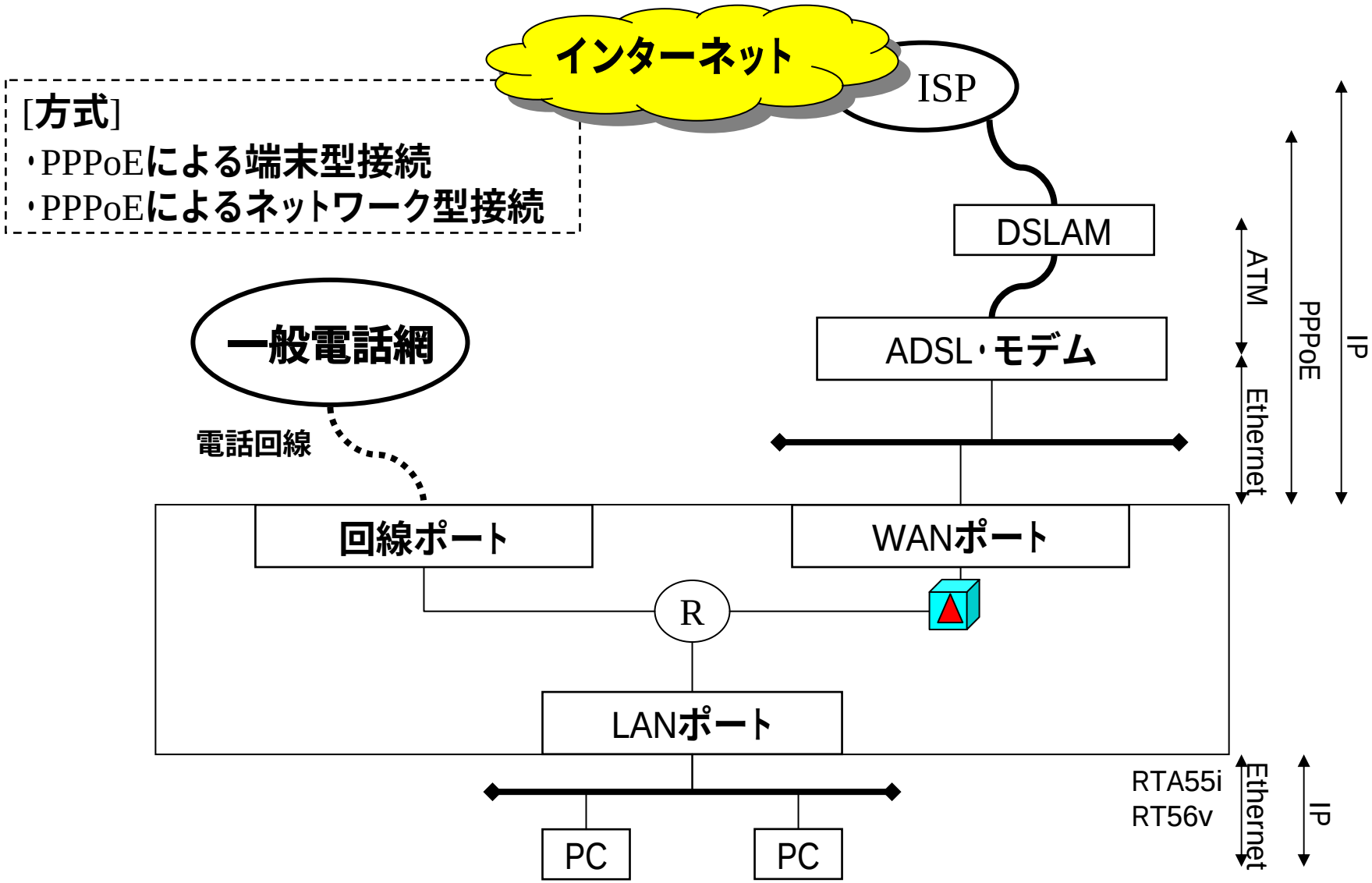
	RTA55i	RT56v
MDI/MDI-X	OK	OK

[ハブの記号の'='と'X']
- '=' : MDI　→端末に接続するポート
- 'X' : MDI-X→ハブに接続するポート(Uplink)

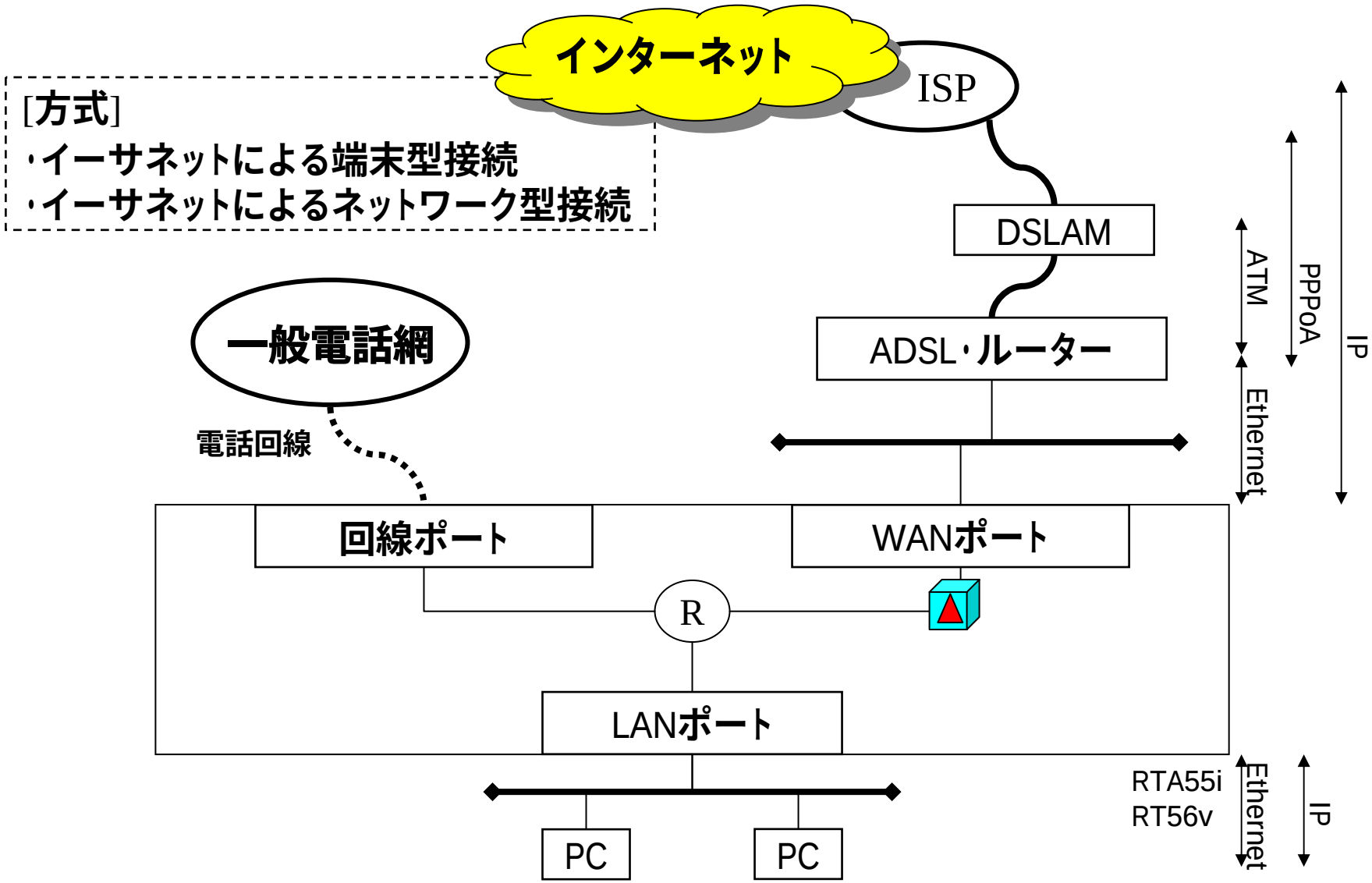
ネットボランチ RTA55i/RT56v インターネット接続

		RTA55i	RTW65i	RT56v
WAN ポート	・CATV ・ADSL/フレッツ・ADSL ・FTTH/Bフレッツ	OK	OK	OK
ISDN ポート	・ISDN/フレッツ・ISDN ・128kbps専用線 ・OCNエコノミー	OK	OK	×

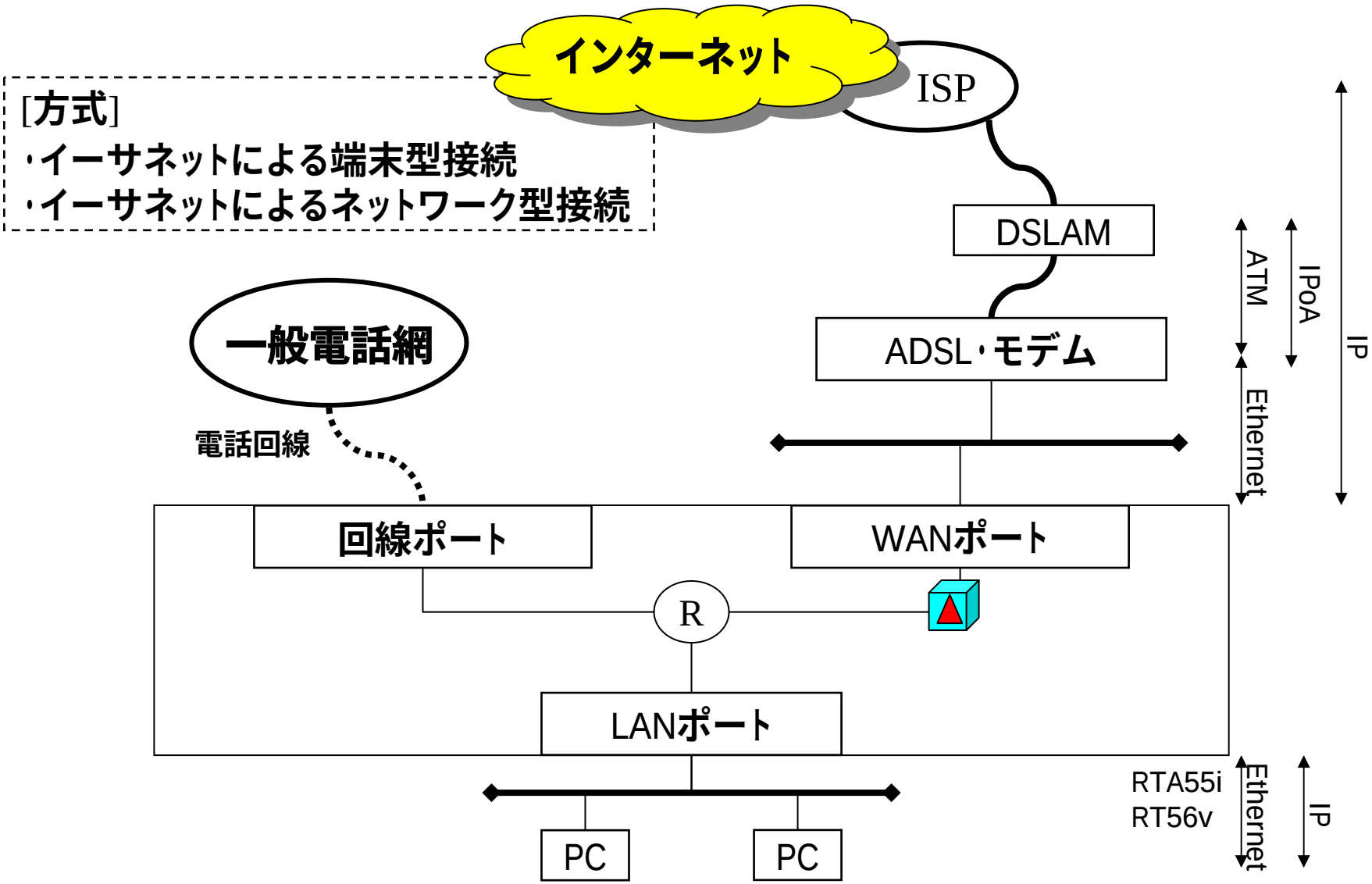
ADSLによるプロバイダ接続#1



ADSLによるプロバイダ接続#2

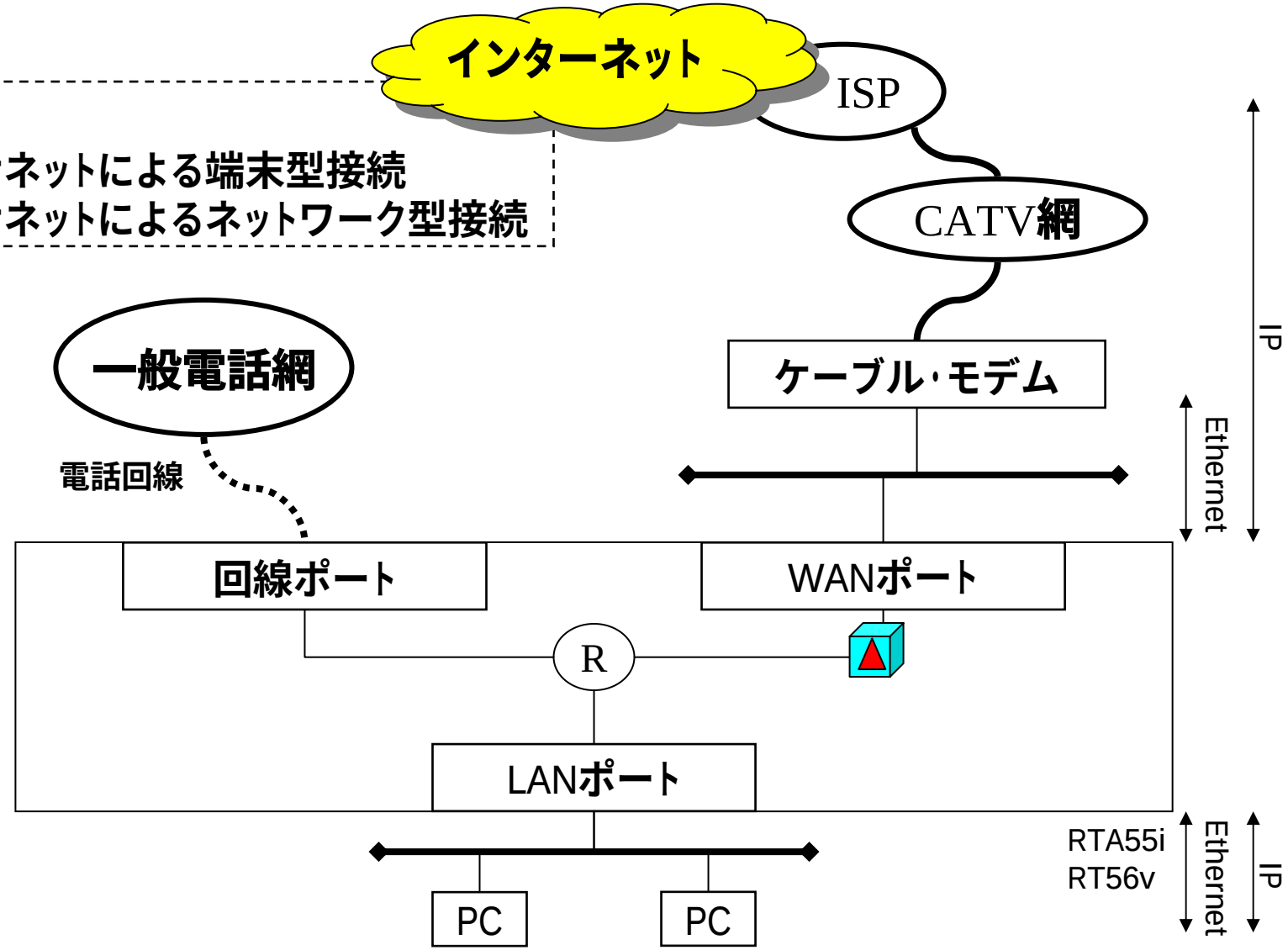


ADSLによるプロバイダ接続#3

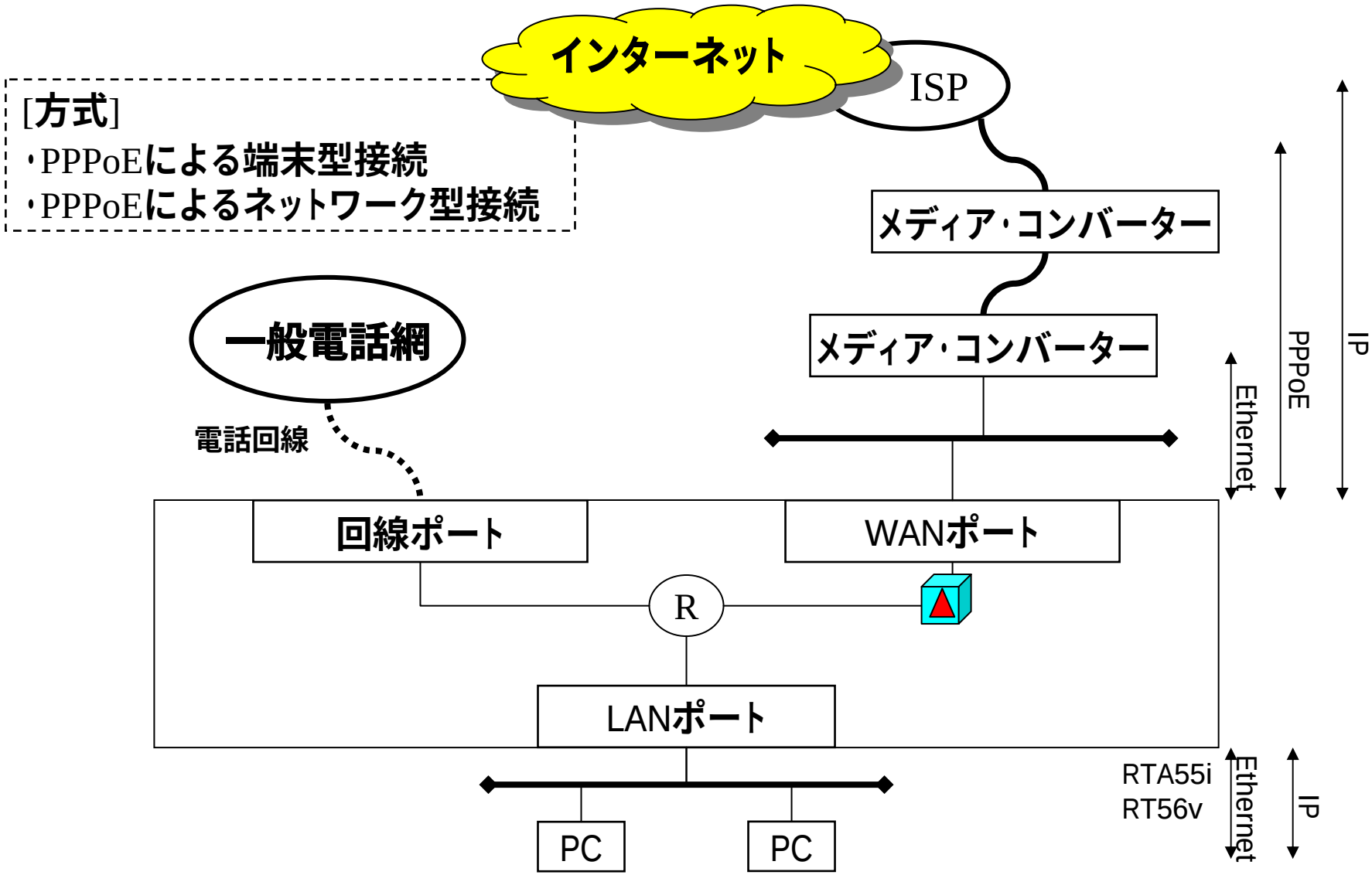


CATVによるプロバイダ接続

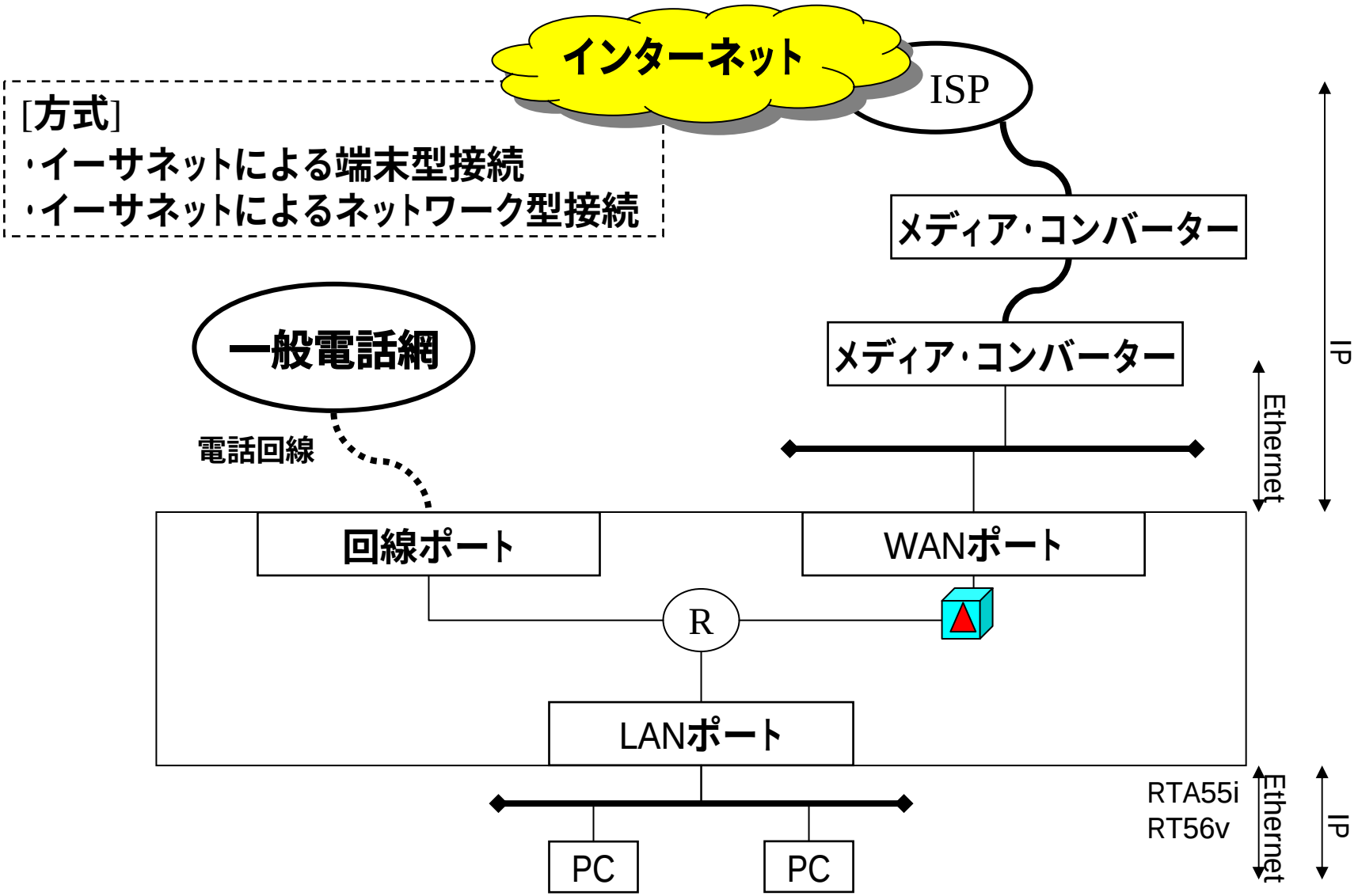
[方式]
・イーサネットによる端末型接続
・イーサネットによるネットワーク型接続



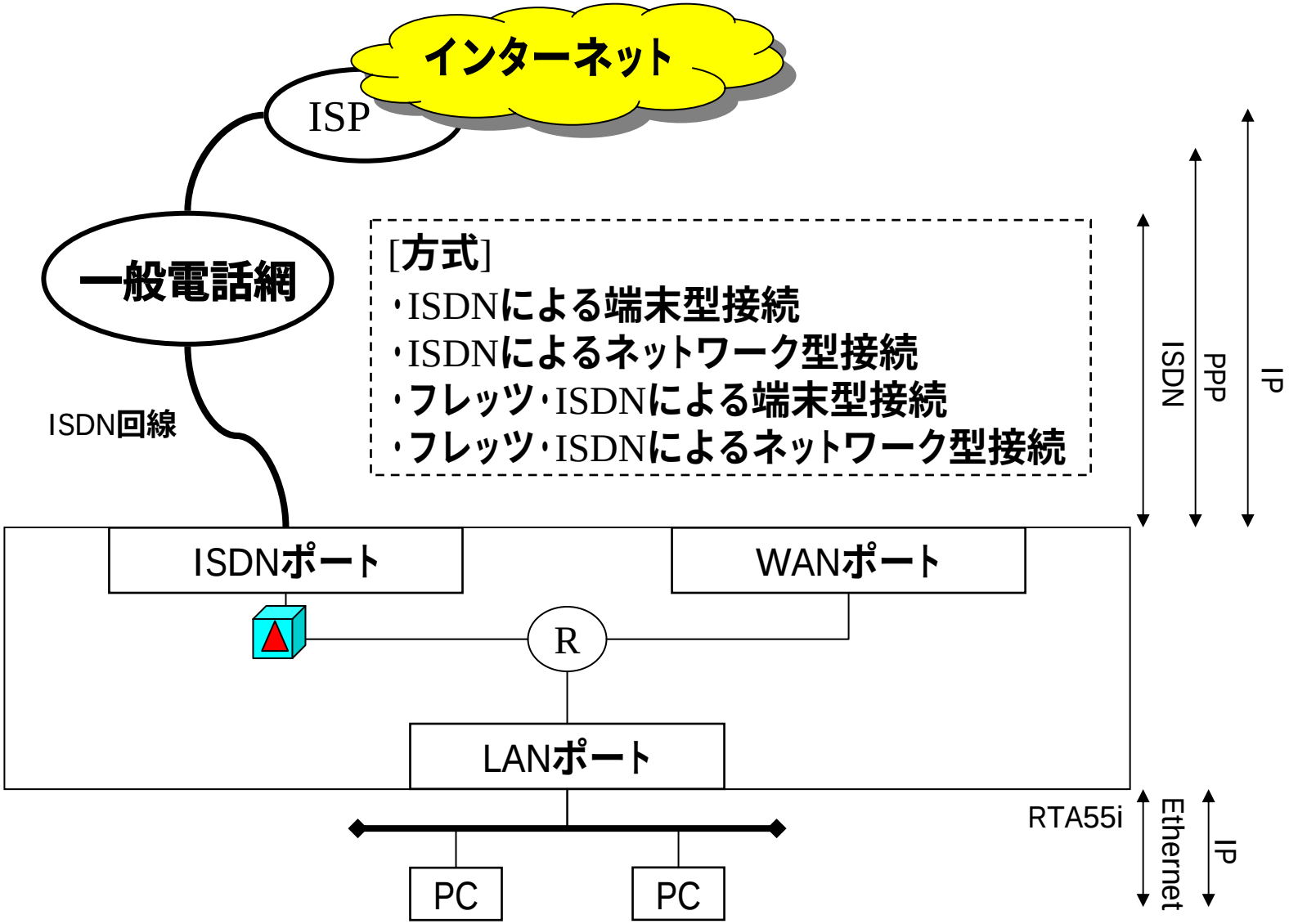
FTTHによるプロバイダ接続#1



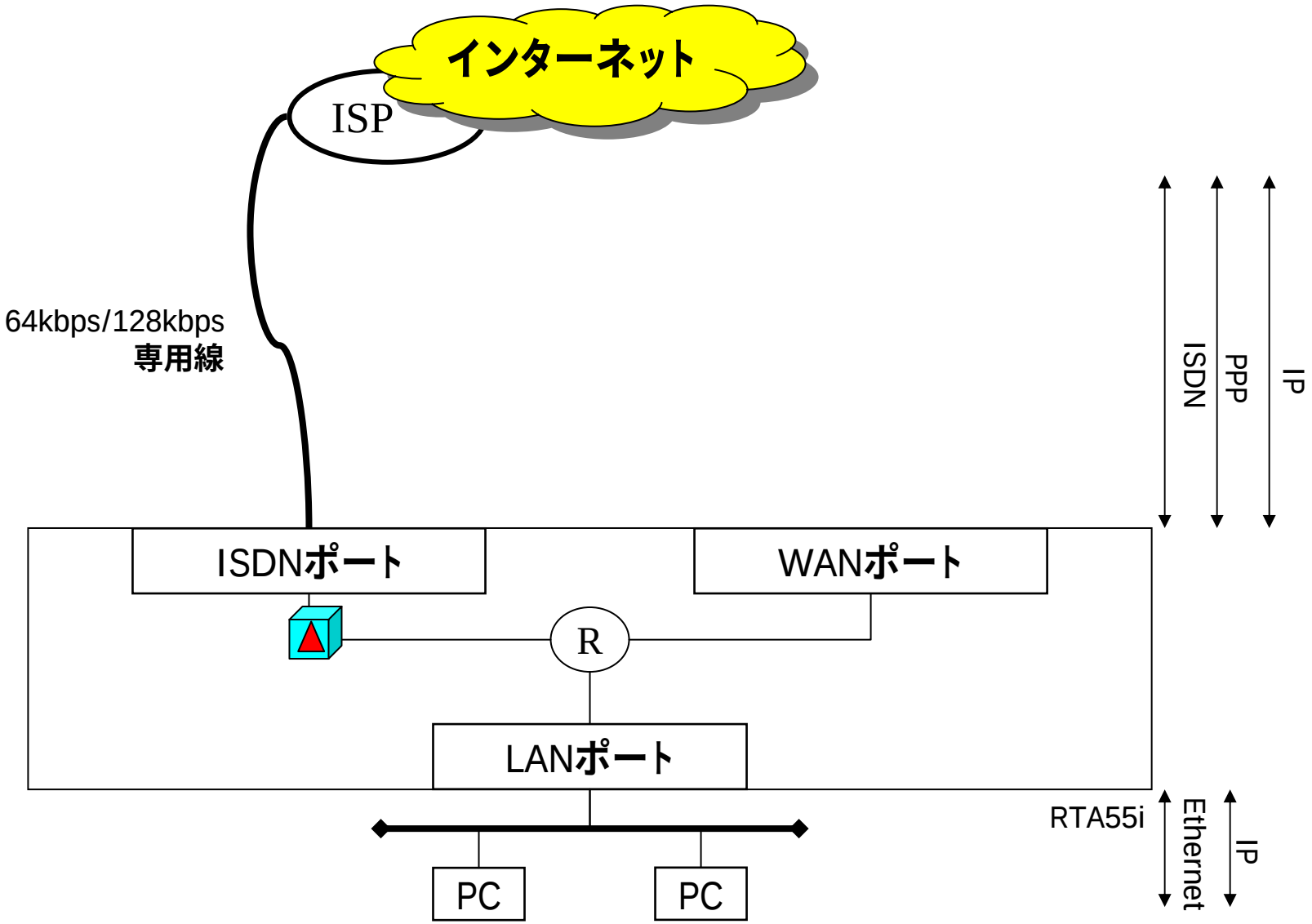
FTTHによるプロバイダ接続#2



ISDN回線によるプロバイダ接続



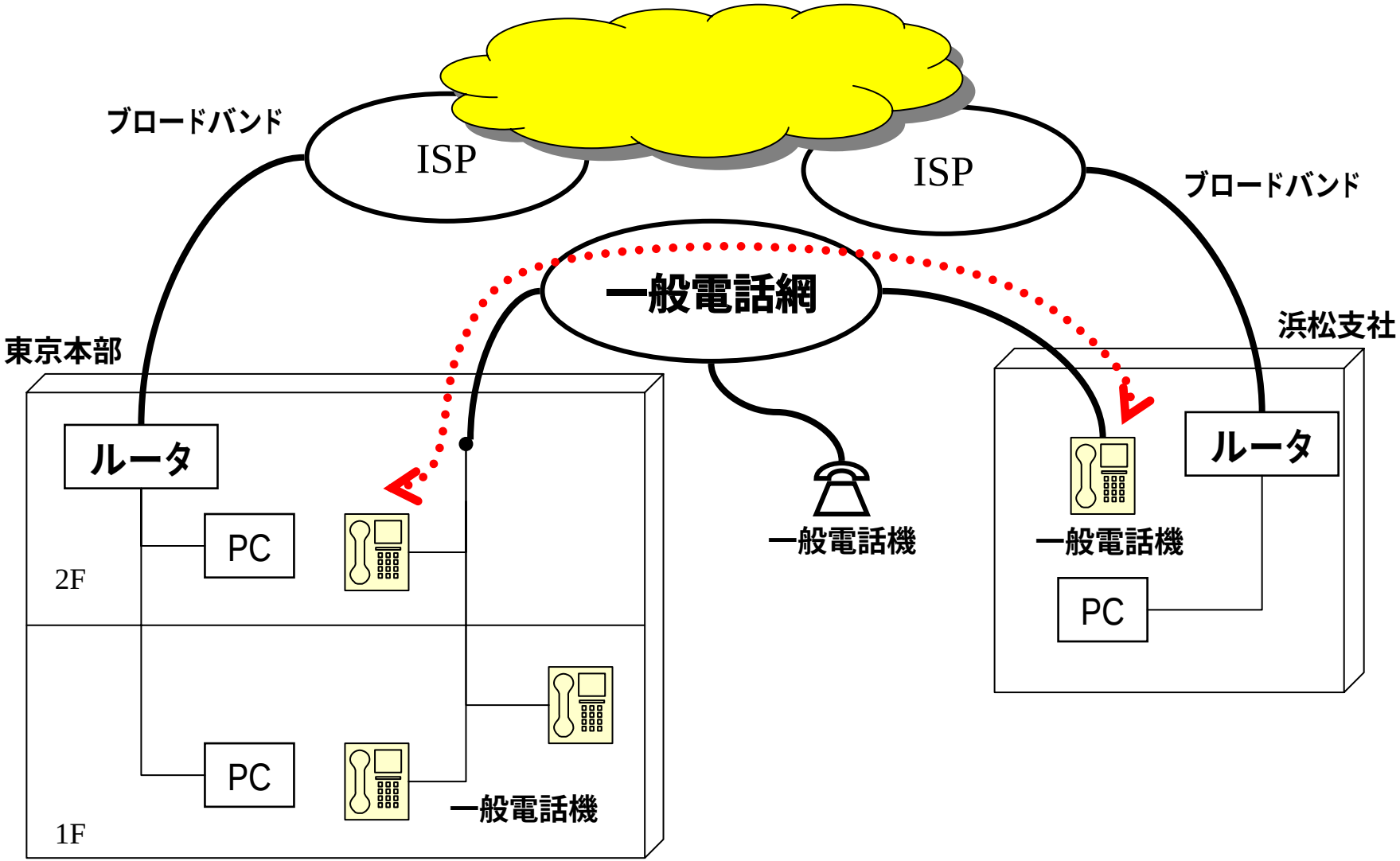
専用線によるプロバイダ接続



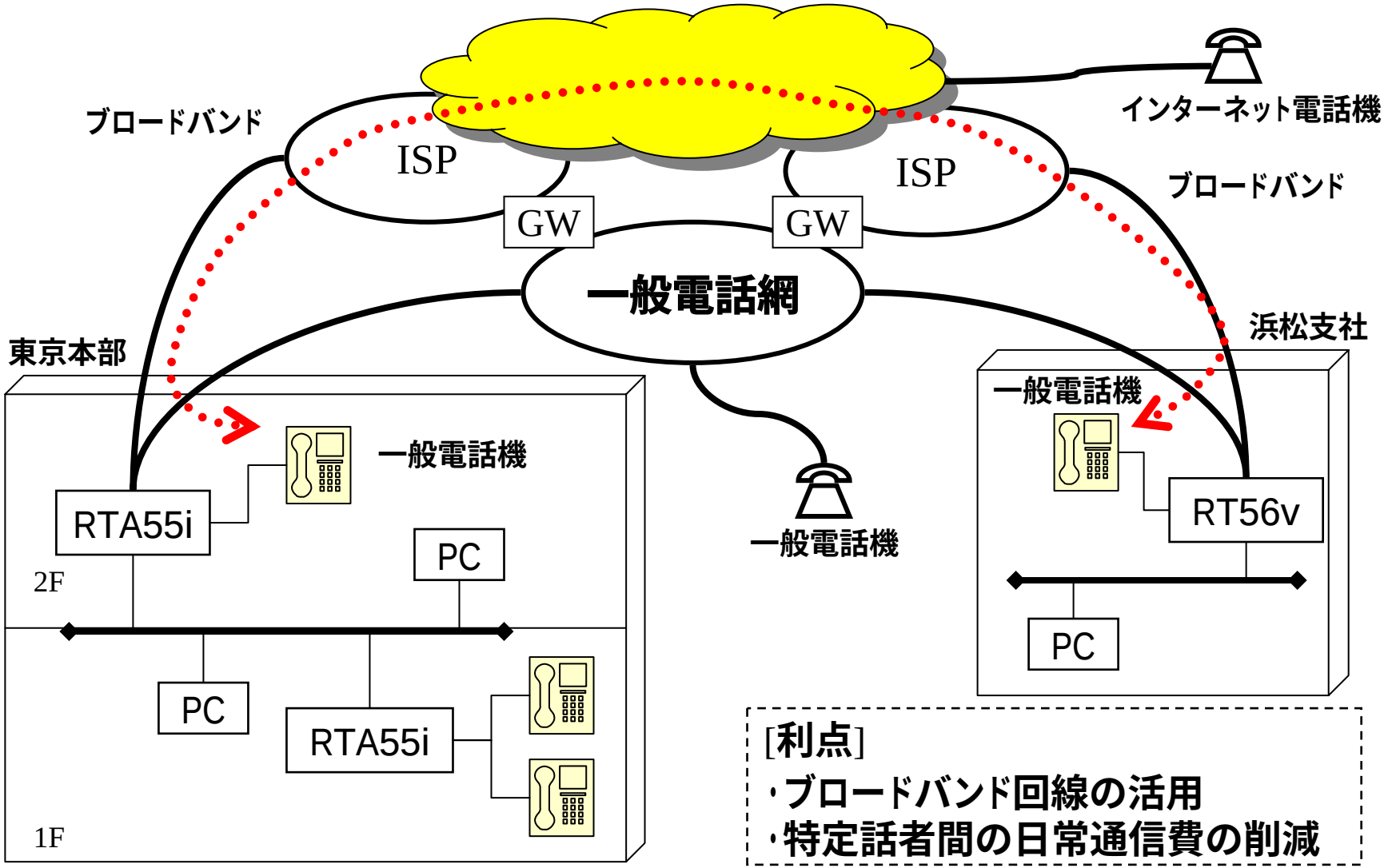
ネットボランチ RTA55i/RT56v
ビジネス用途
(VoIPソリューション)

	RTA55i	RTW65i	RT56v
ISDNポート	OK	OK	×
LINEポート	×	×	OK
TELポート	2	3	3

中小規模ブロードバンド・ネットワーク

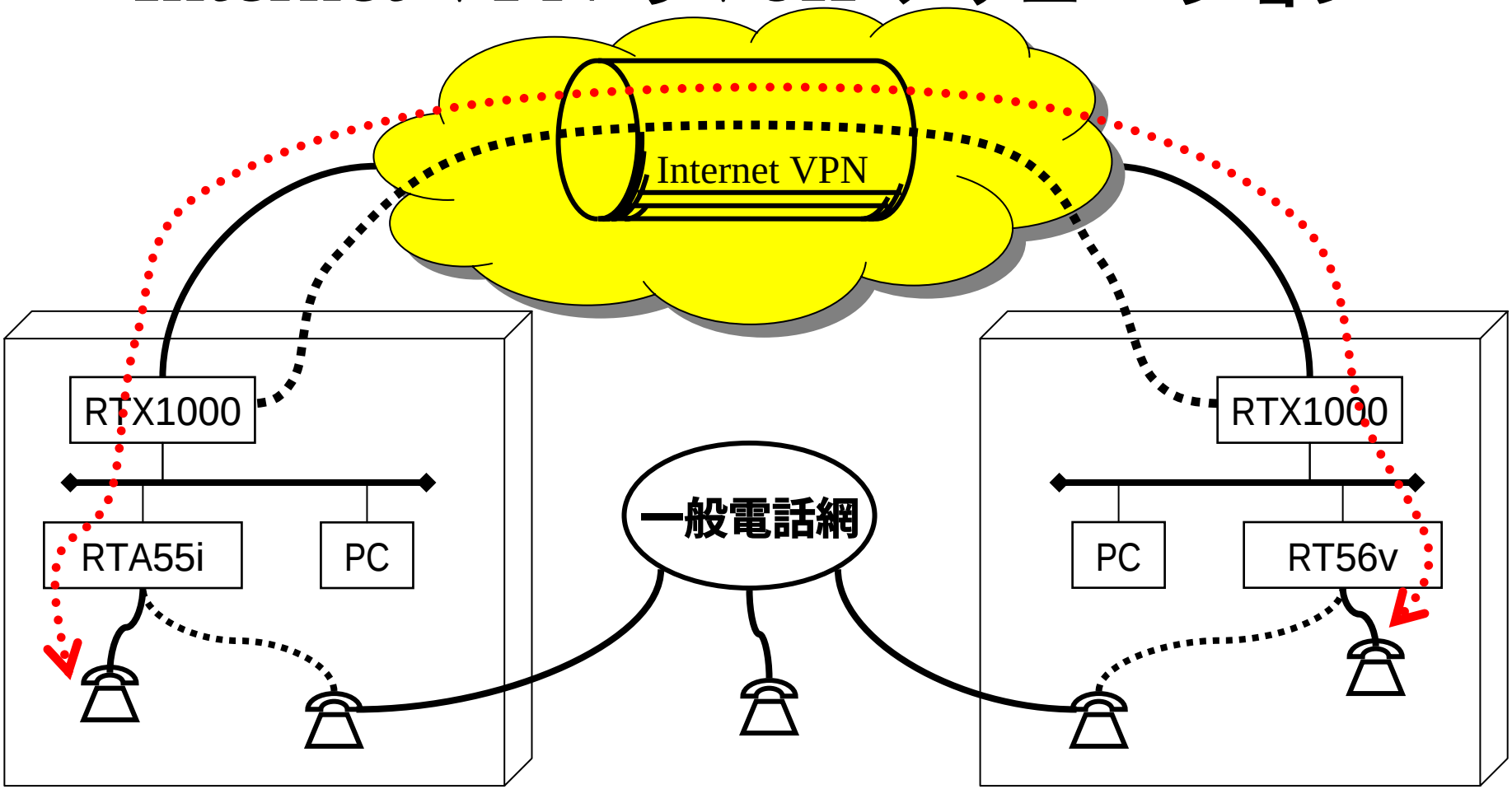


中小規模ネットワークのVoIP化



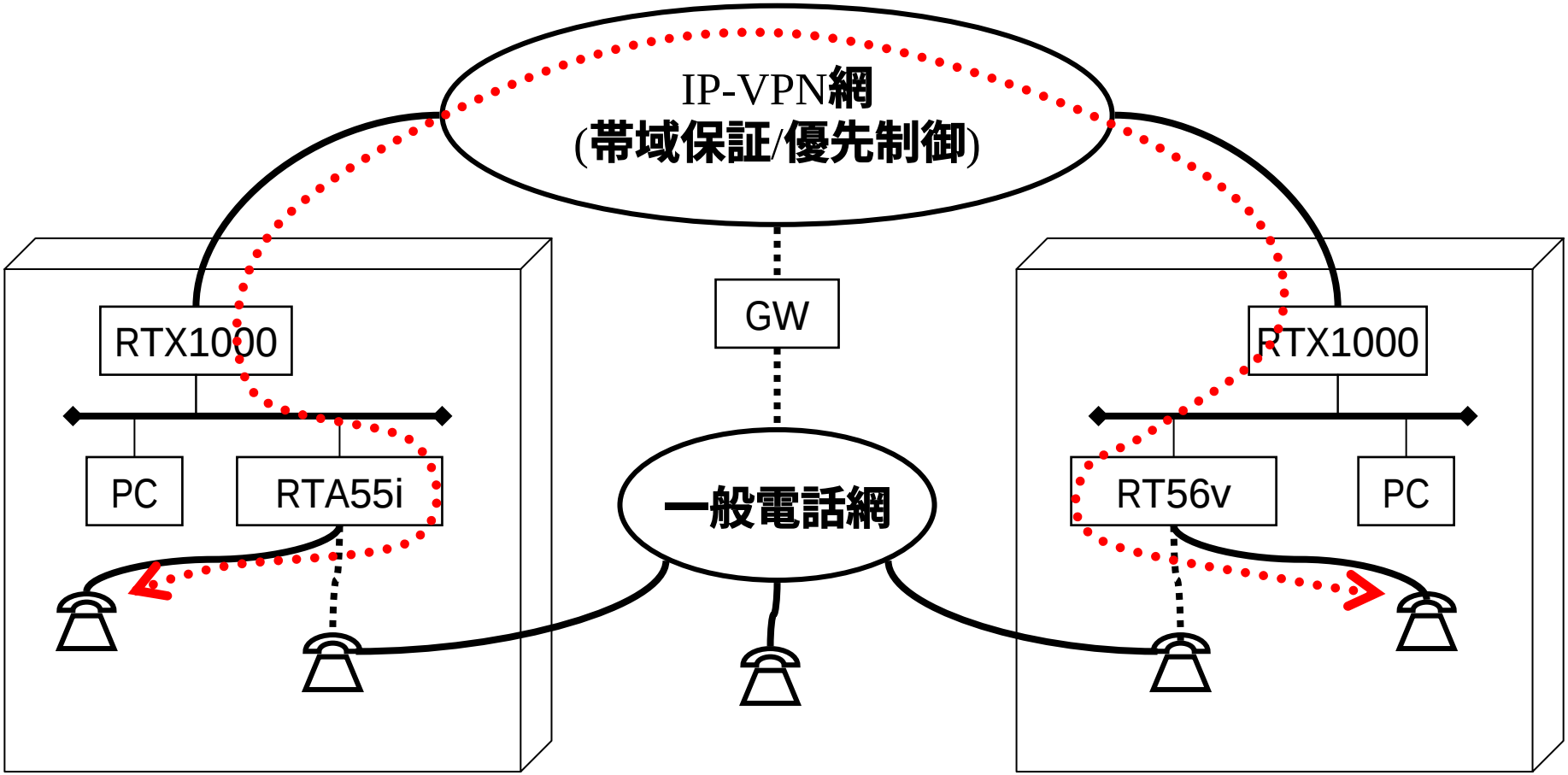
[利点]
・ブロードバンド回線の活用
・特定話者間の日常通信費の削減

Internet VPNのVoIPソリューション



- Internet VPNで拠点間通話(遠隔地との内線通話)のコスト削減
- 電話とデータの段階的統合

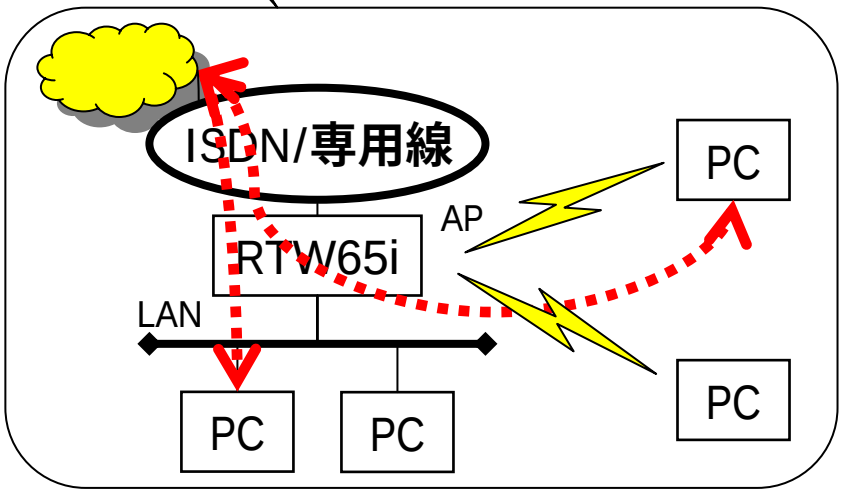
IP-VPNを活用したVoIPソリューション



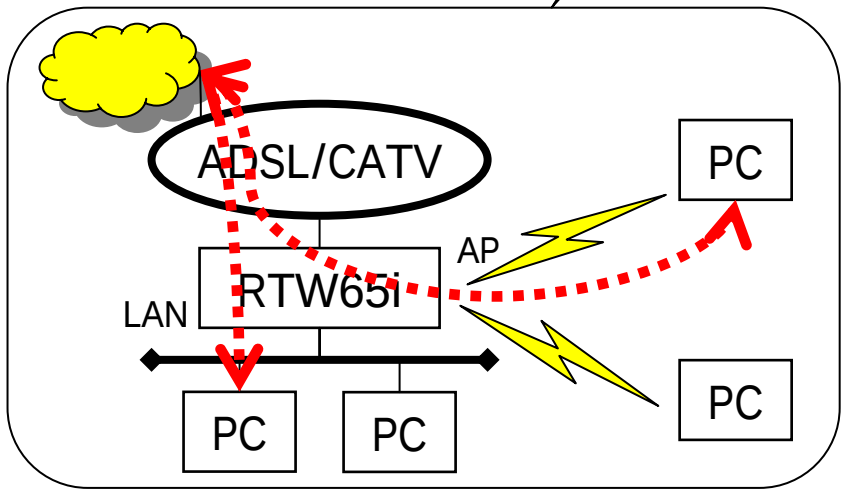
・Internet VPNとの差別化
・電話とデータの段階的統合

ネットボランチ
の
いろいろな機能や使い方
「無線LAN編」

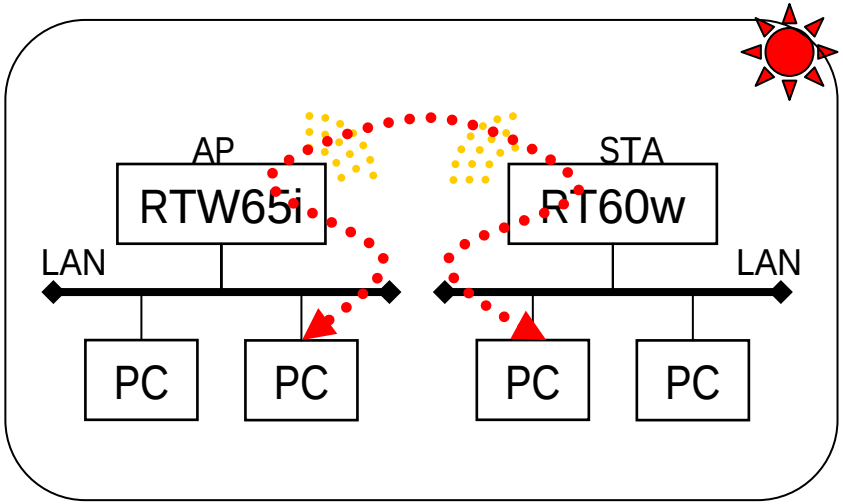
RTW65iの無線LAN機能



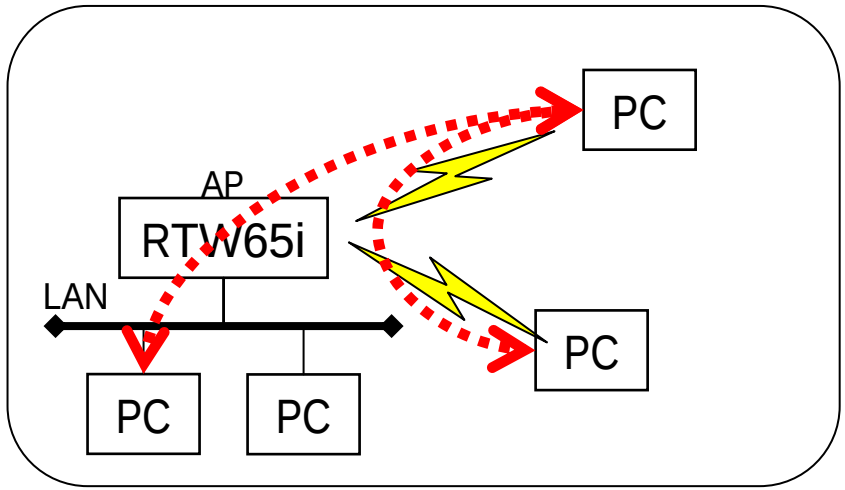
ISDN/専用線によるプロバイダ接続



ADSL/CATVによるプロバイダ接続

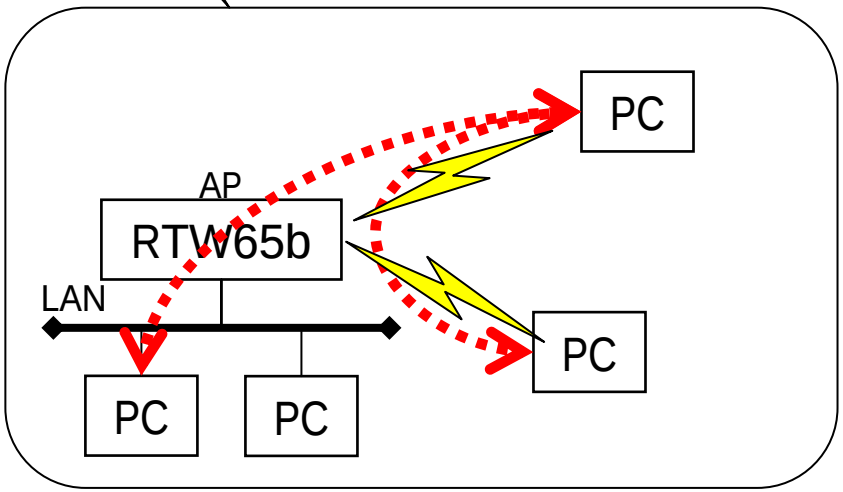


無線ブリッジ機能(離れた有線LAN間を接続)

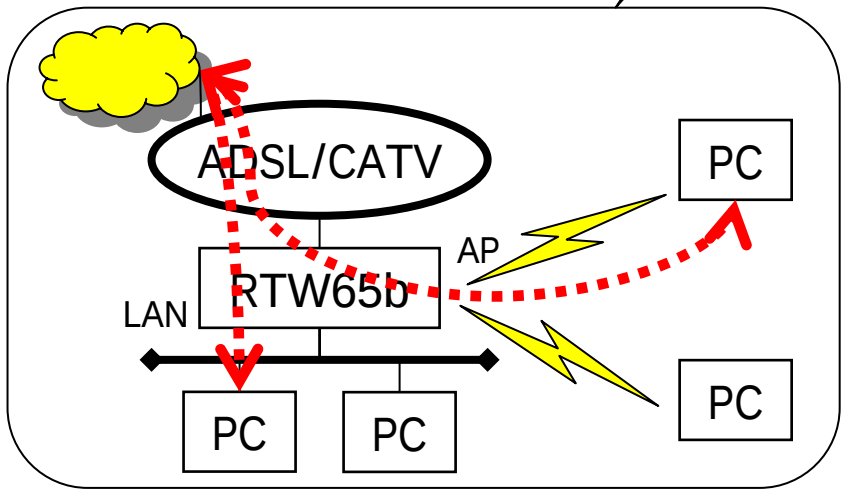


有線LANと無線LANのブリッジ機能

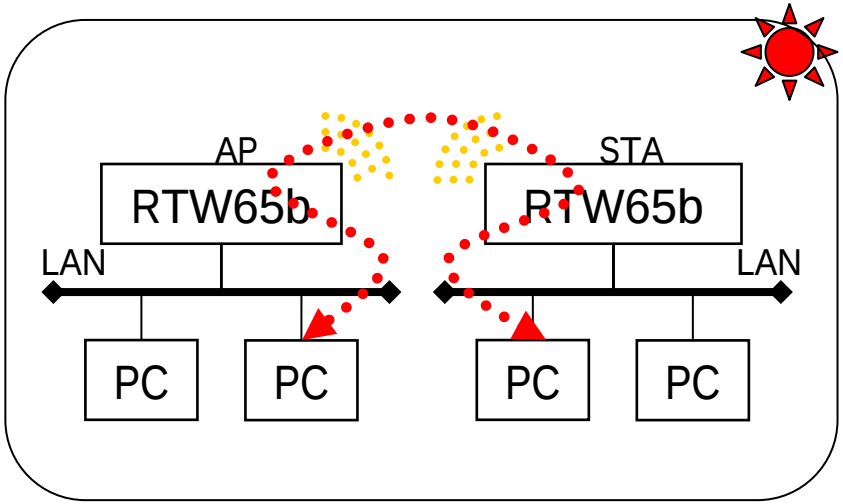
RTW65bの無線LAN機能



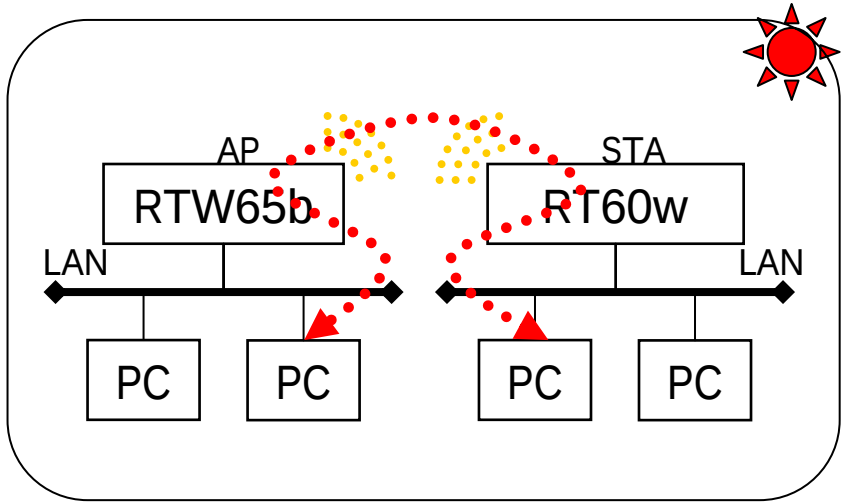
有線LANと無線LANのブリッジ機能



ADSL/CATVによるプロバイダ接続



無線ブリッジ機能(離れた有線LAN間を接続)



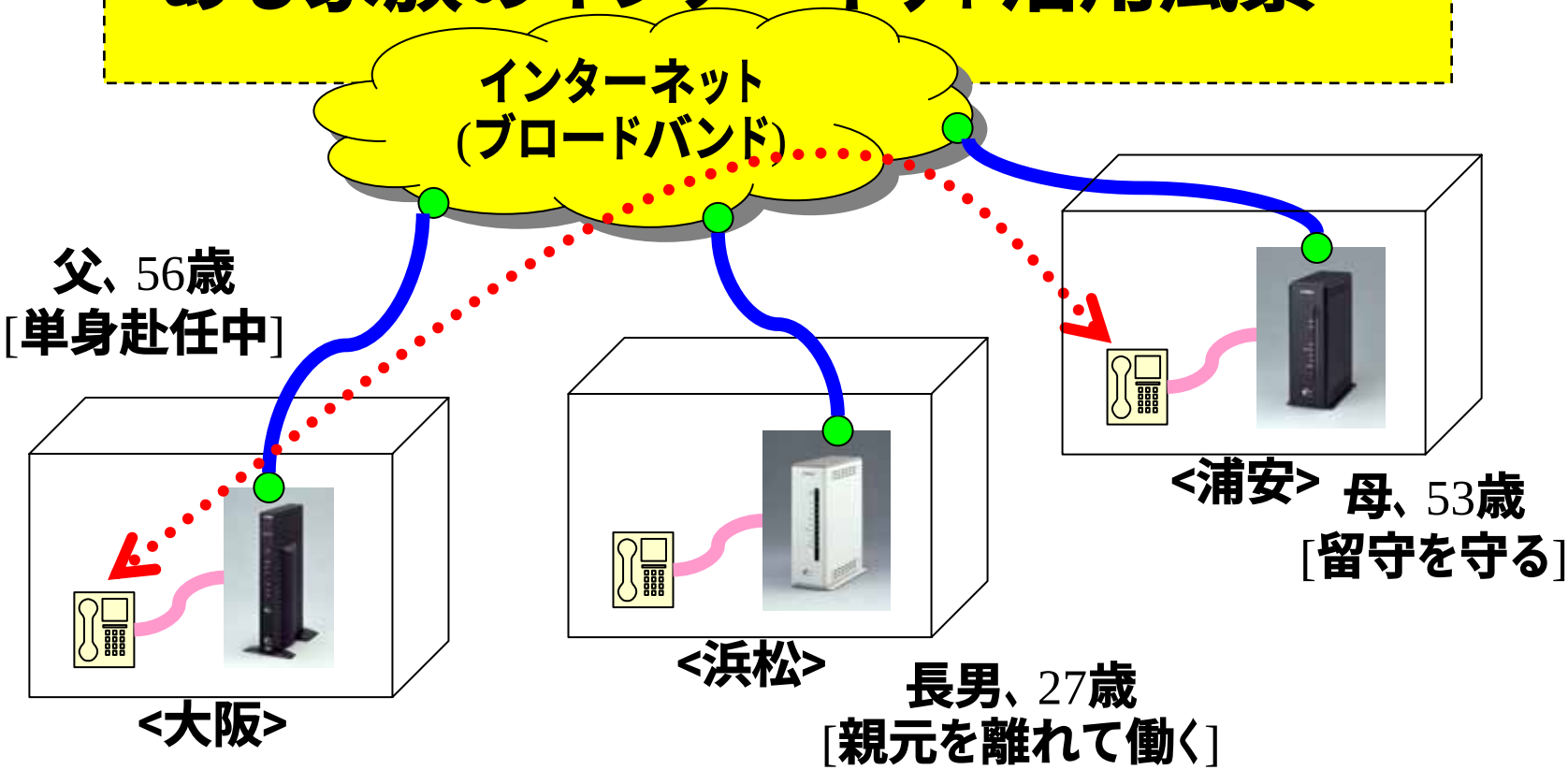
RT60wとの相互接続

ネットボランチ
～利用環境と実験環境～

Net Volante
ネットボランチ

インターネット電話を体験！

ある家族のインターネット活用風景・・



仮想ゲートウェイ

実験環境で、インタネット電話#1

(固定) 192.168.100.1

仮想インターネット

192.168.100.0/24

<大阪>

(固定) 192.168.100.2

192.168.2.0/24

PC

<浜松>

(固定) 192.168.100.3

192.168.3.0/24

PC

<浦安>

(固定) 192.168.100.4

192.168.4.0/24

浜松	9#3#

大阪	9#2#

実験環境

[方式]
・イーサネットによる端末型接続

(固定) 192.168.100.1

仮想インターネット

192.168.100.0/24

<大阪>

(固定) 192.168.100.2

192.168.2.0/24

PC

<浜松>

(固定) 192.168.100.3

192.168.3.0/24

①インターネット接続設定

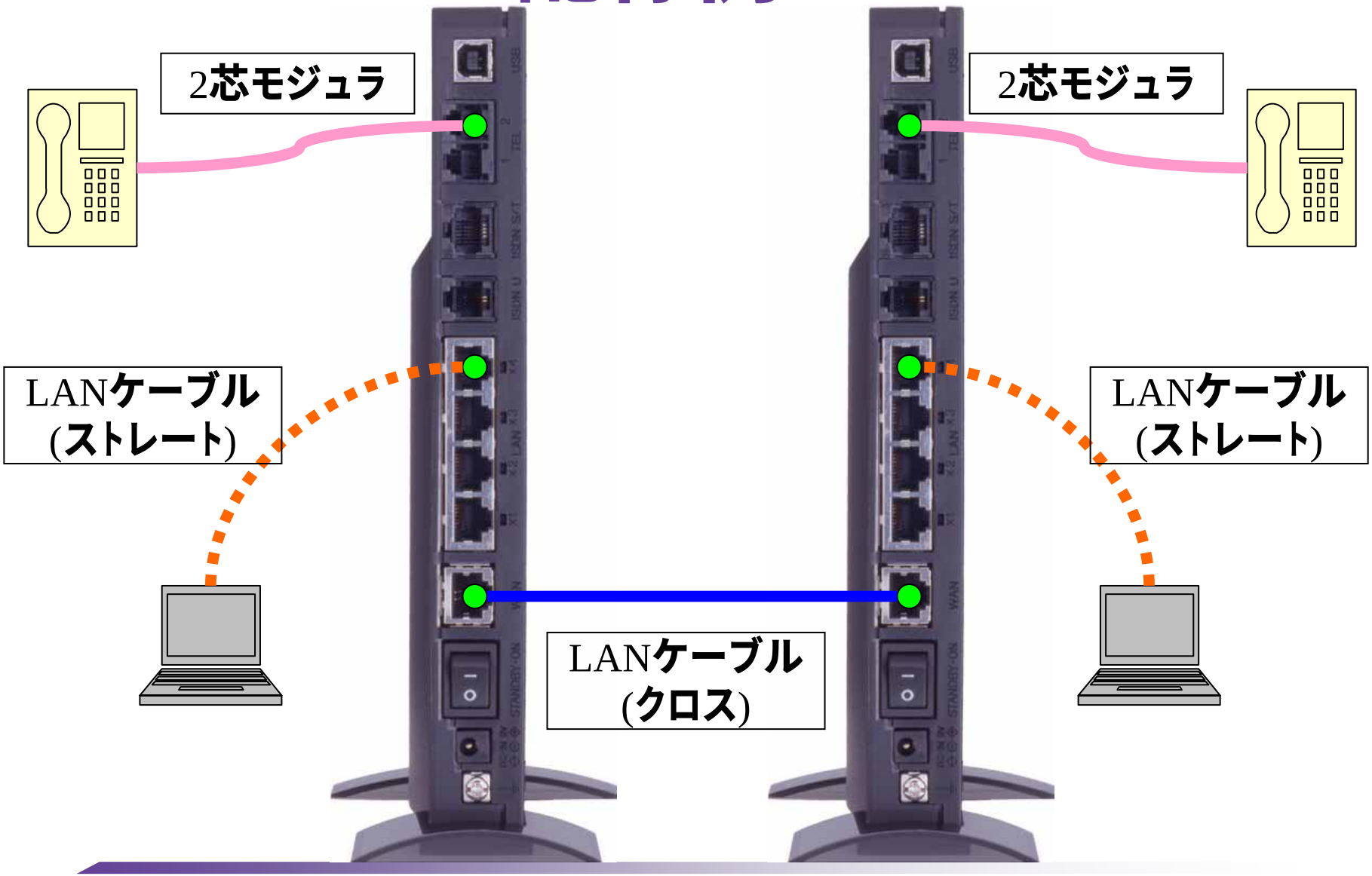
②インターネット電話設定

③電話帳設定

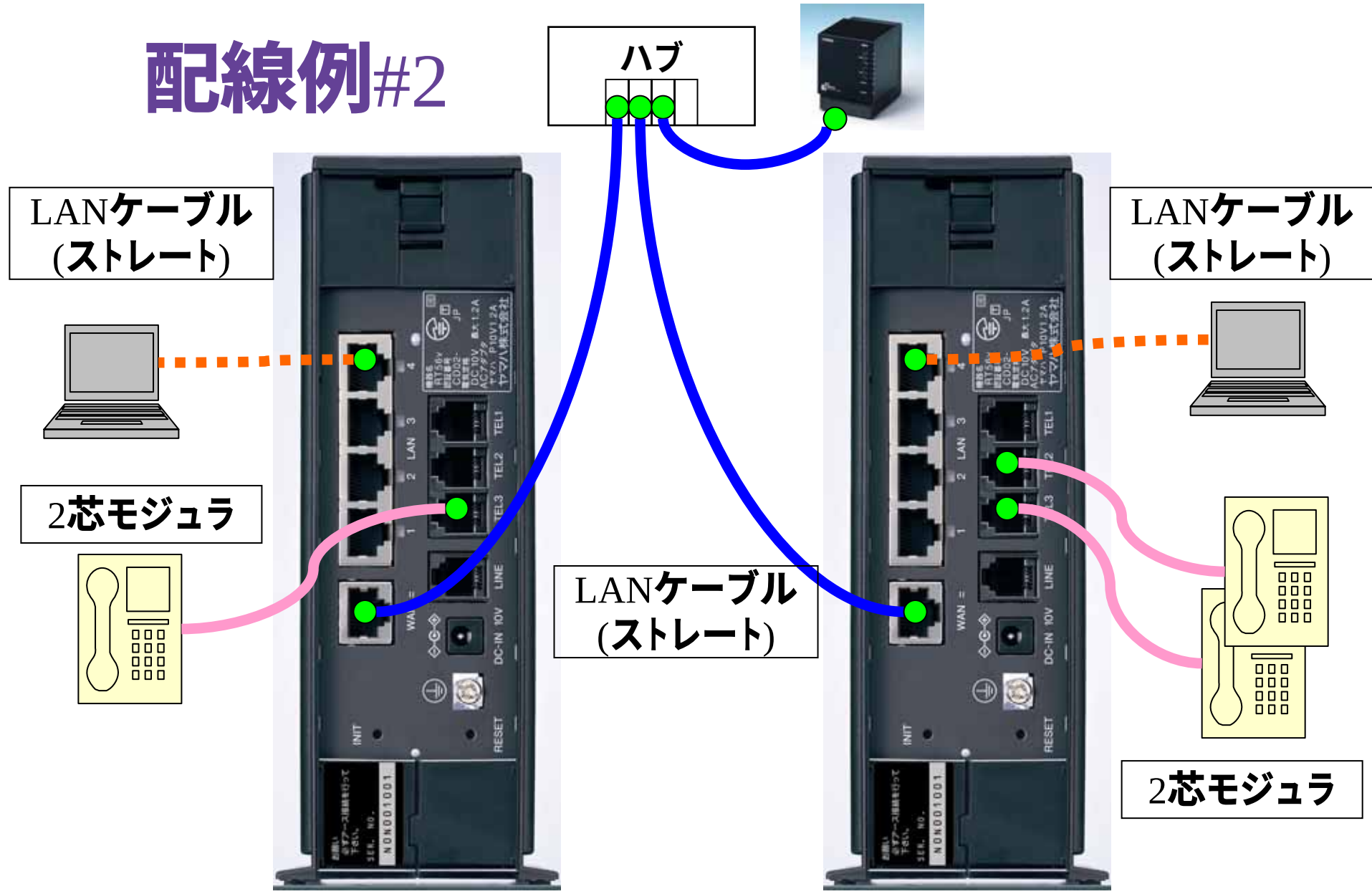
浜松	9#3#

大阪	9#2#

配線例#1

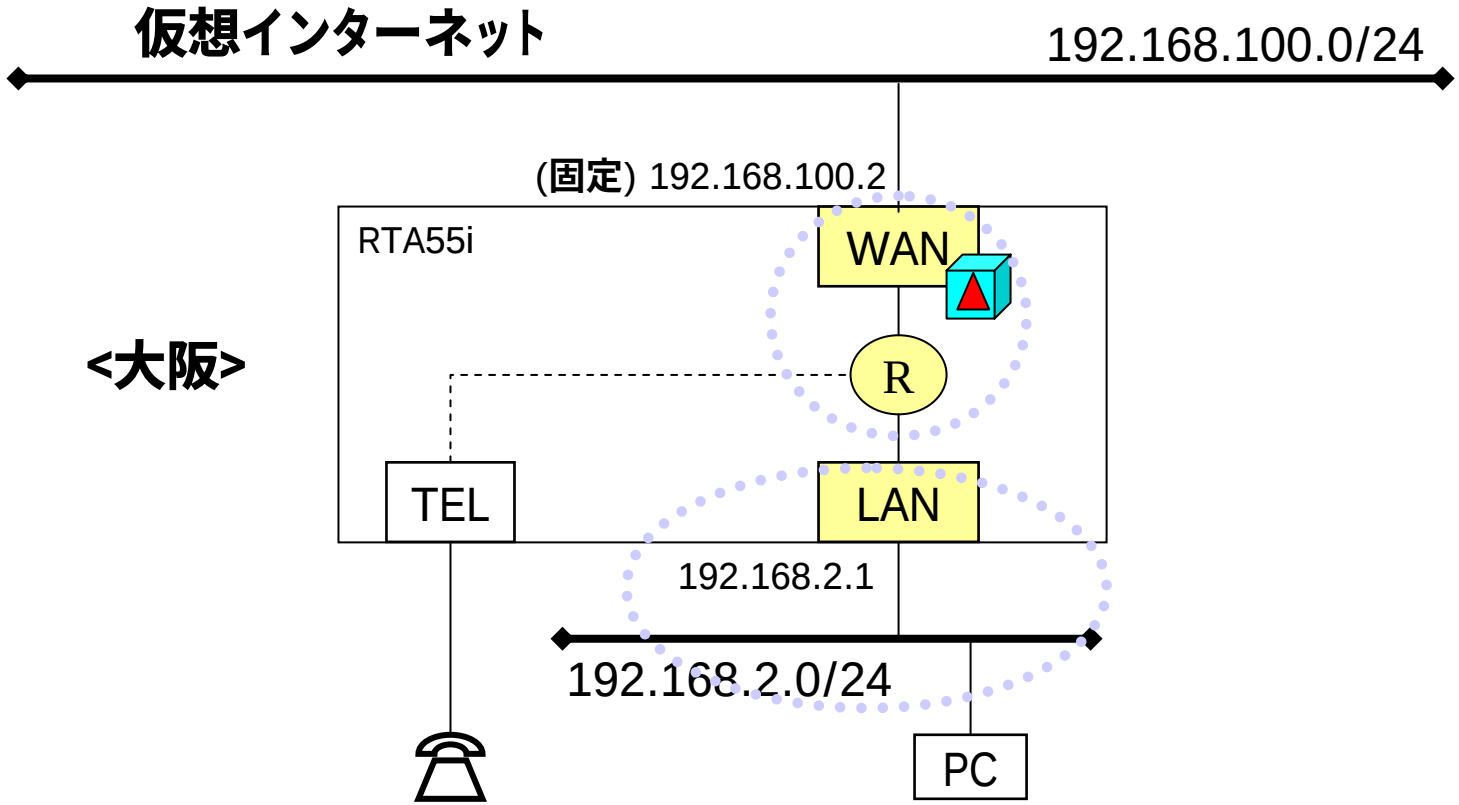


配線例#2



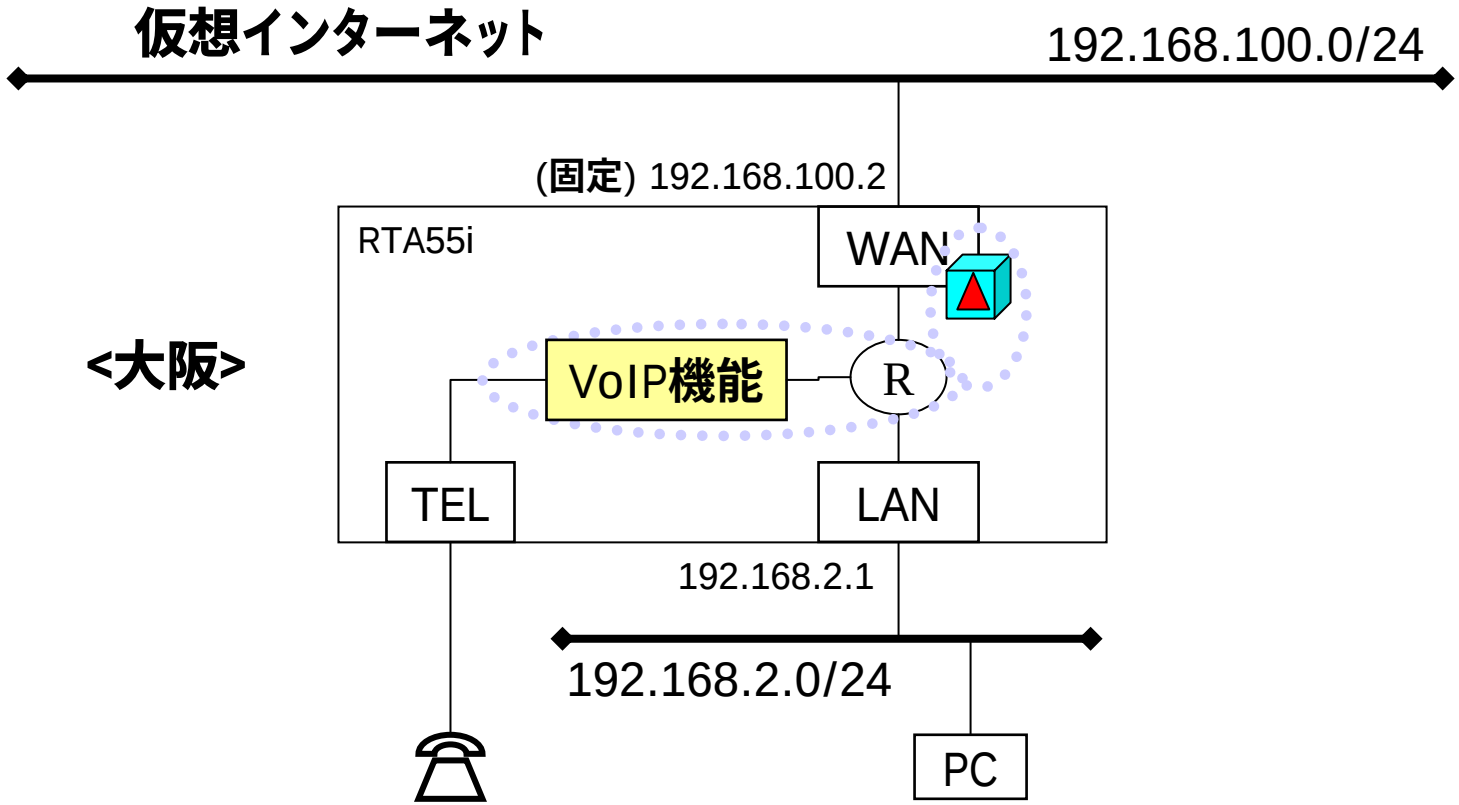
インターネット接続の設定

[方式]
・イーサネットによる端末型接続

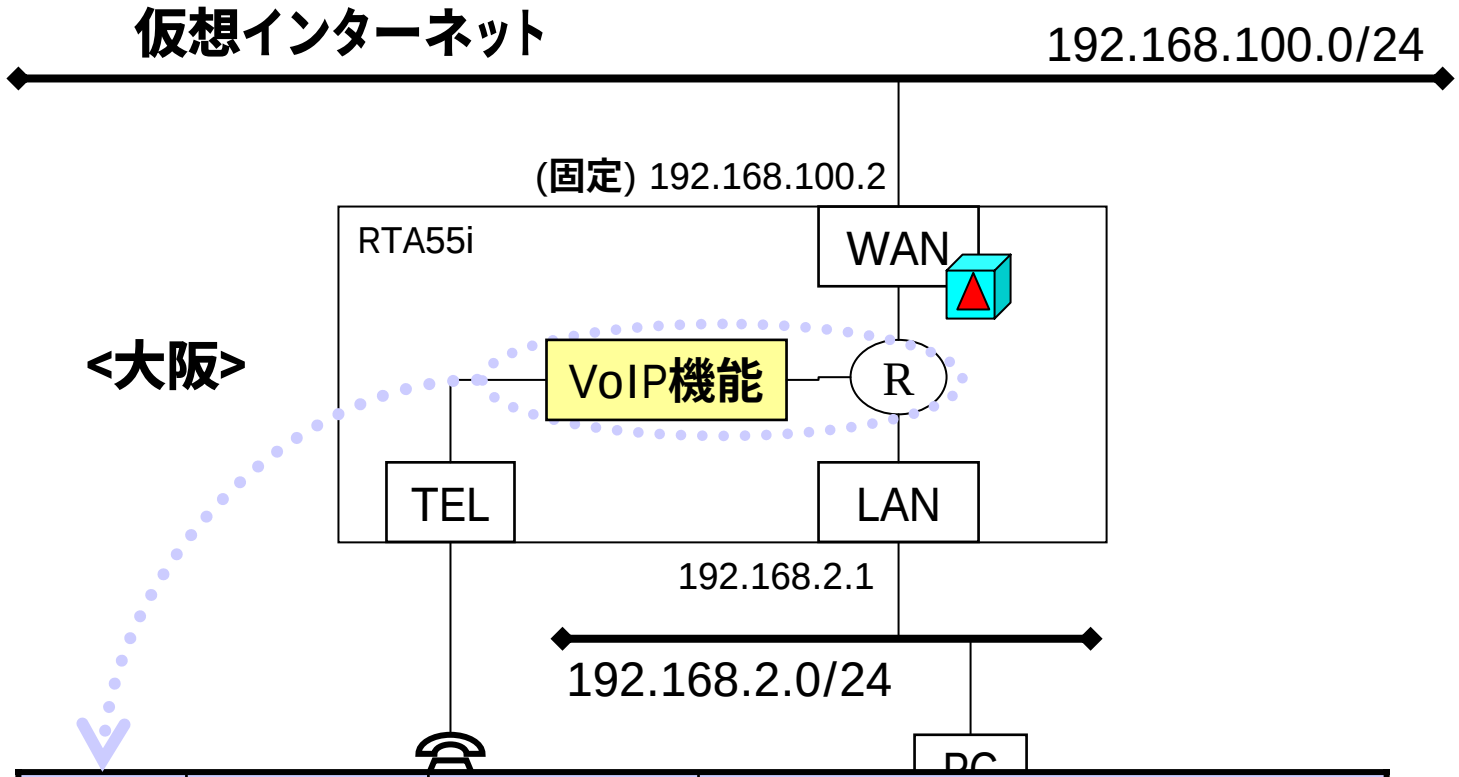


インターネット電話の設定

[方式]
・イーサネットによる端末型接続

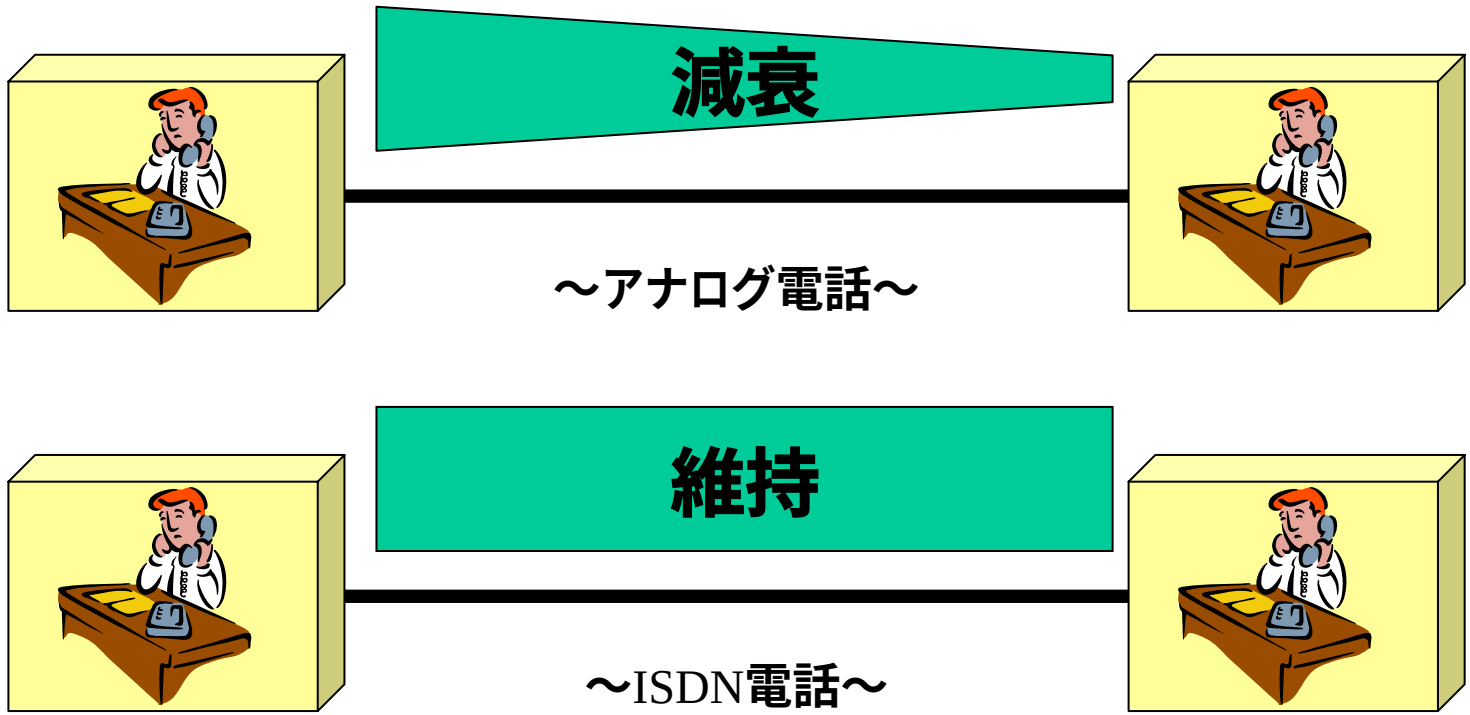


インターネット電話帳の設定



宛先	ダイヤル	登録番号	sipアドレス
浜松	9#3#	3	sip:rta55i@192.168.100.3
浦安	9#4#	4	sip:rt56v@192.168.100.4

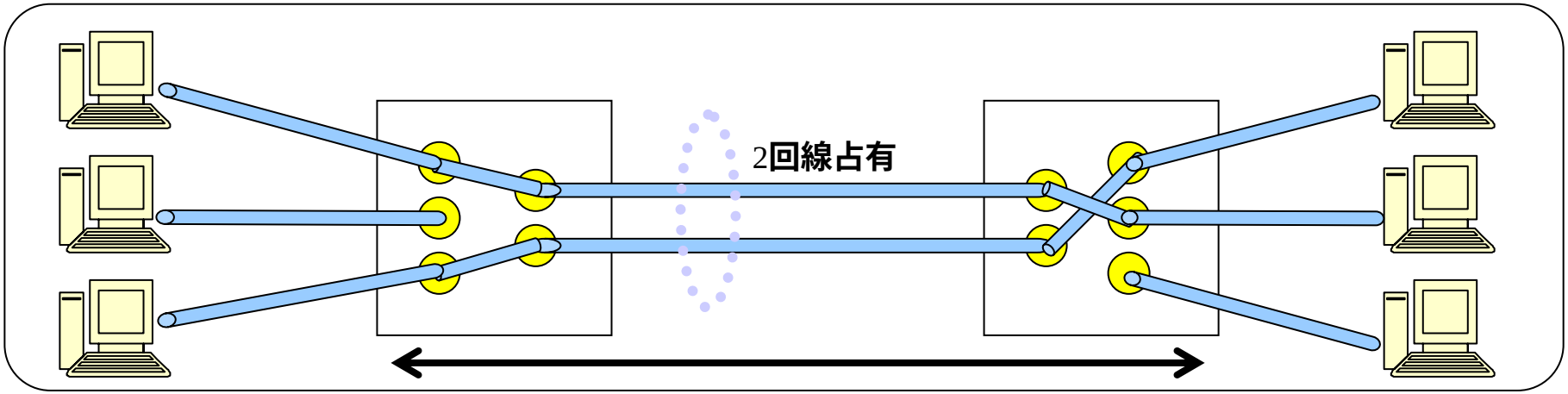
アナログ電話とデジタル電話(デジタル)



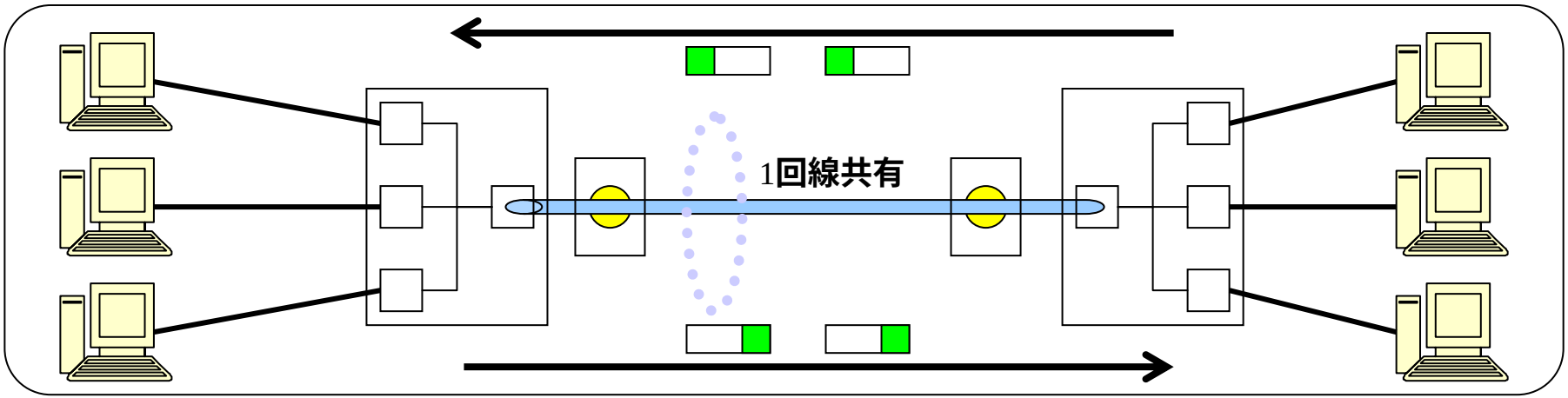
[距離による音質の差]
・劣化の可能性
・遅れの可能性

回線交換とパケット交換

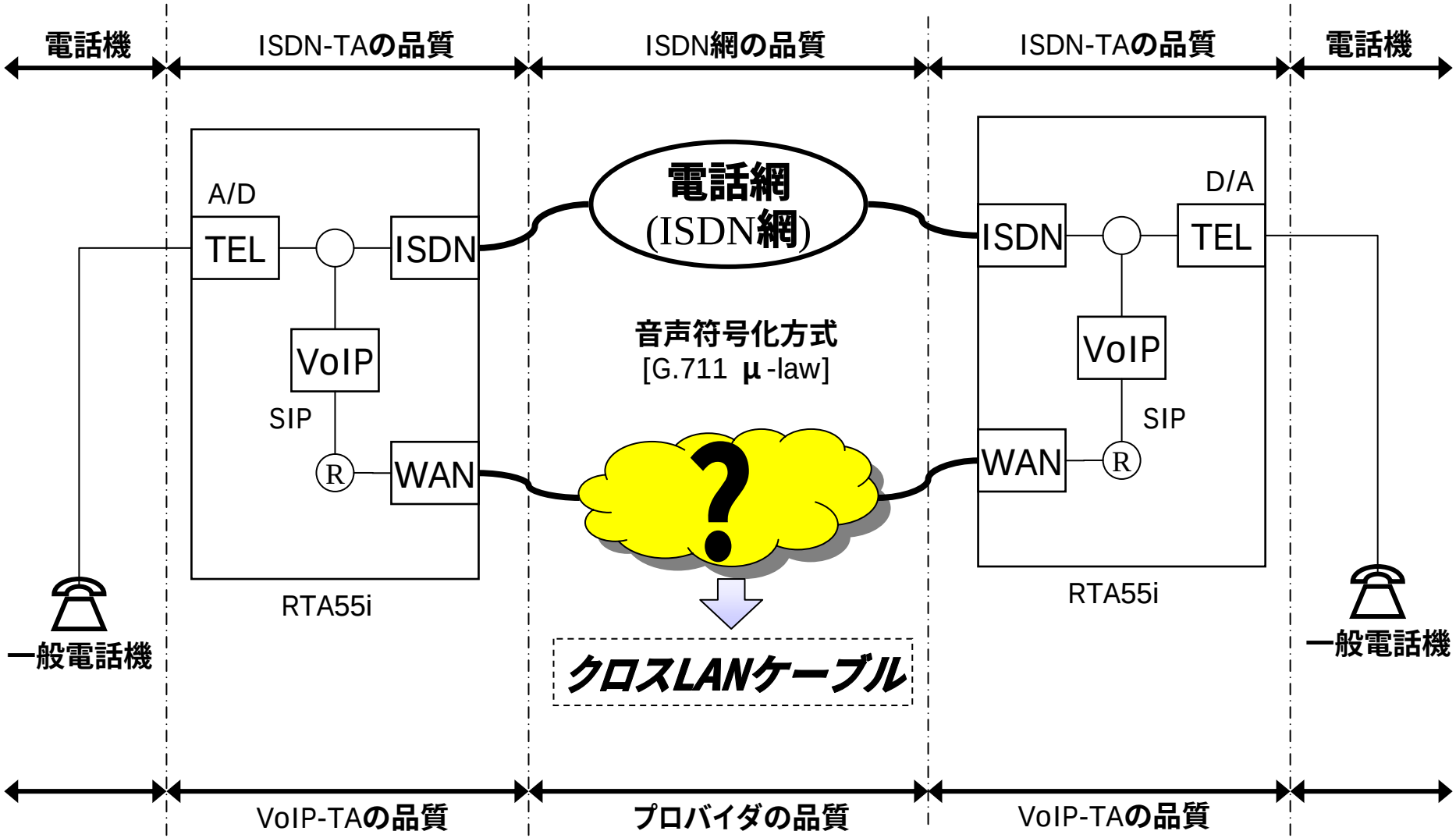
回線交換…つまり、電話回線



パケット交換…IP通信(ブロードバンド回線、常時接続回線)

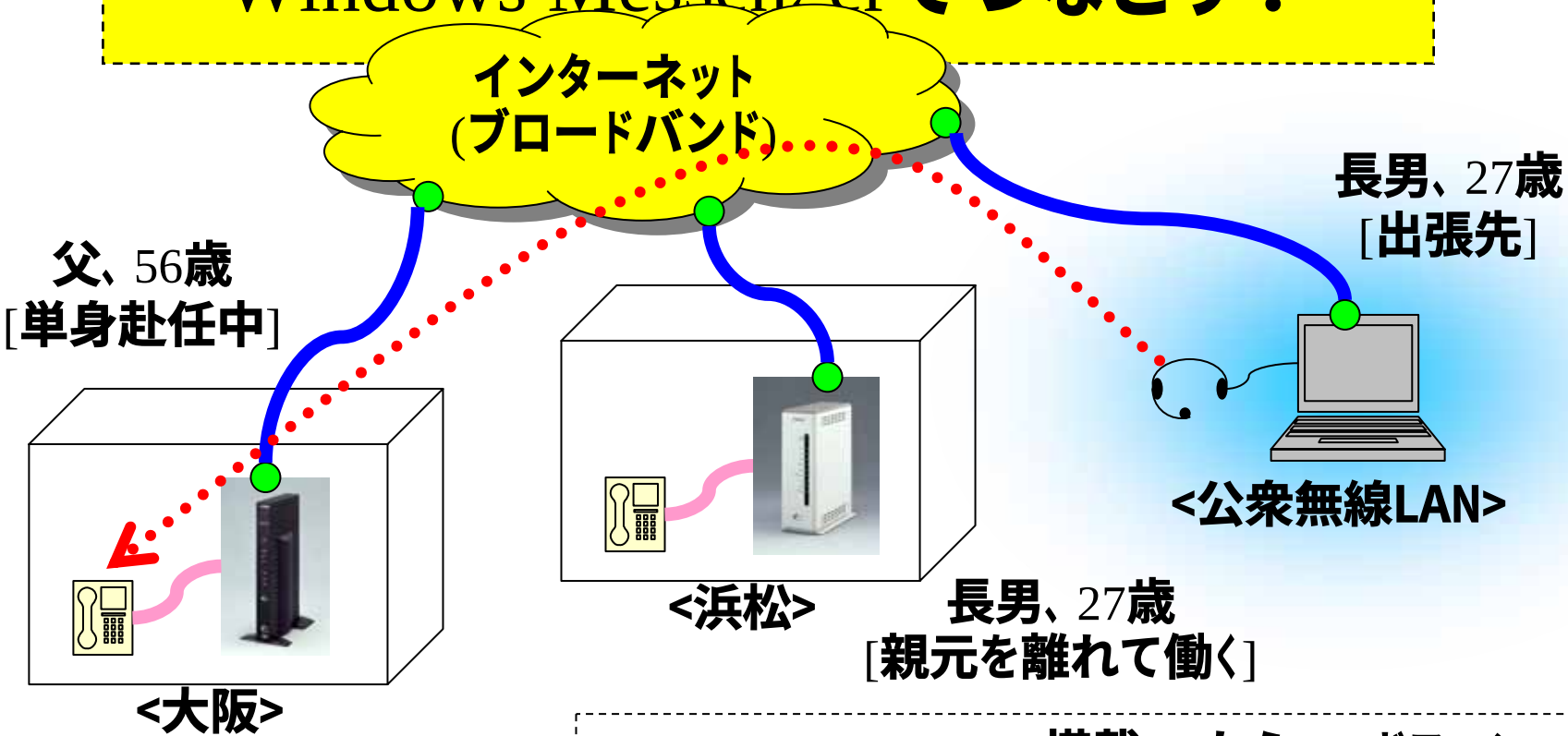


究極のプロバイダ



インターネット電話を体験！

Windows Messengerでつなごう！



Windows Messenger搭載PCからヘッドフォンセットを使って大阪へ電話をします！

実験環境で、インターネット電話#2

(固定) 192.168.100.1

仮想インターネット

192.168.100.0/24

<大阪>

(固定) 192.168.100.2

192.168.2.0/24

PC

<浜松>

(固定) 192.168.100.3

192.168.3.0/24

PC

<浦安>

(固定) 192.168.100.4

192.168.4.0/24

PC
Windows
Messenger

<出張先>

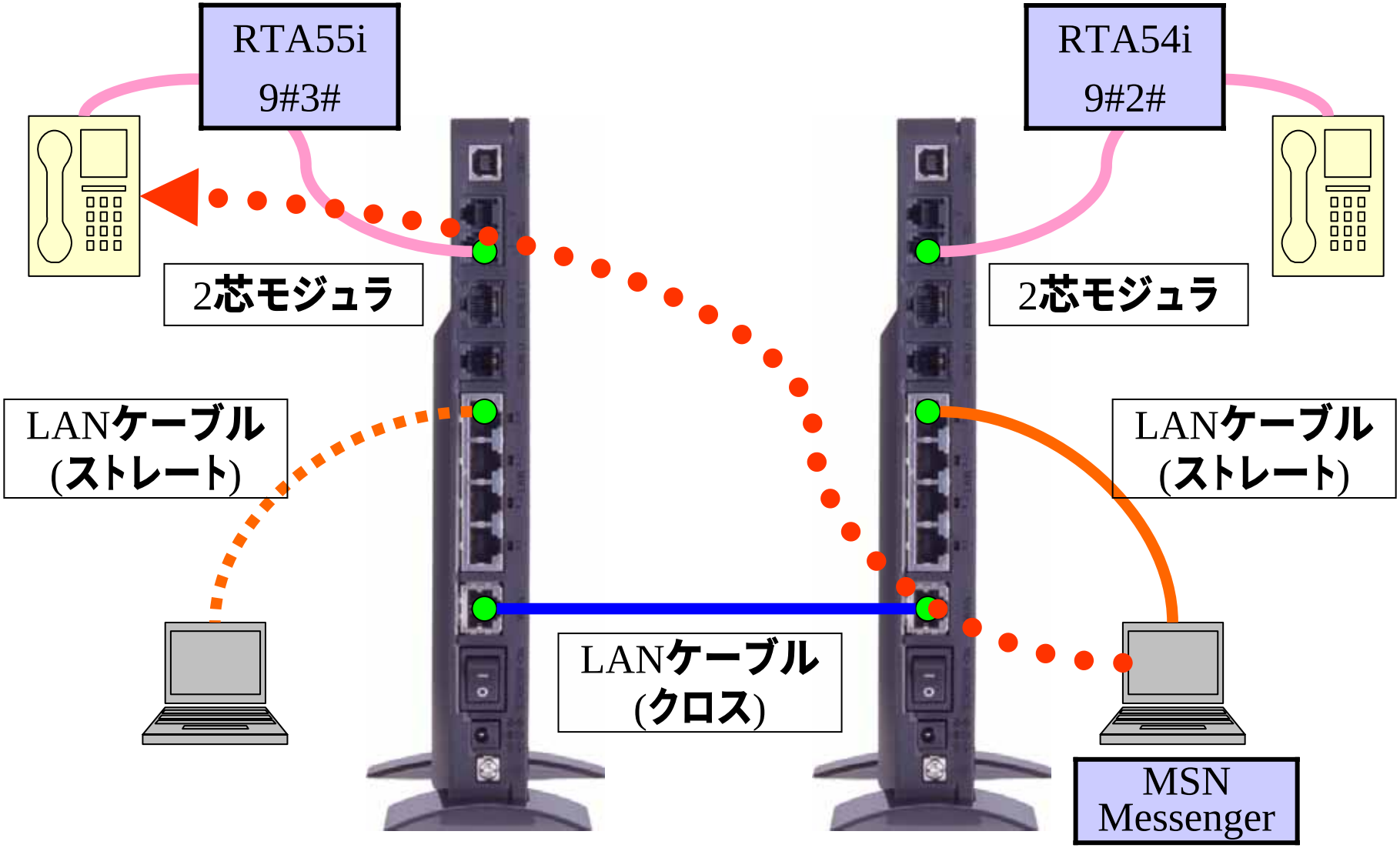
浜松	9#3
浦安	9#4

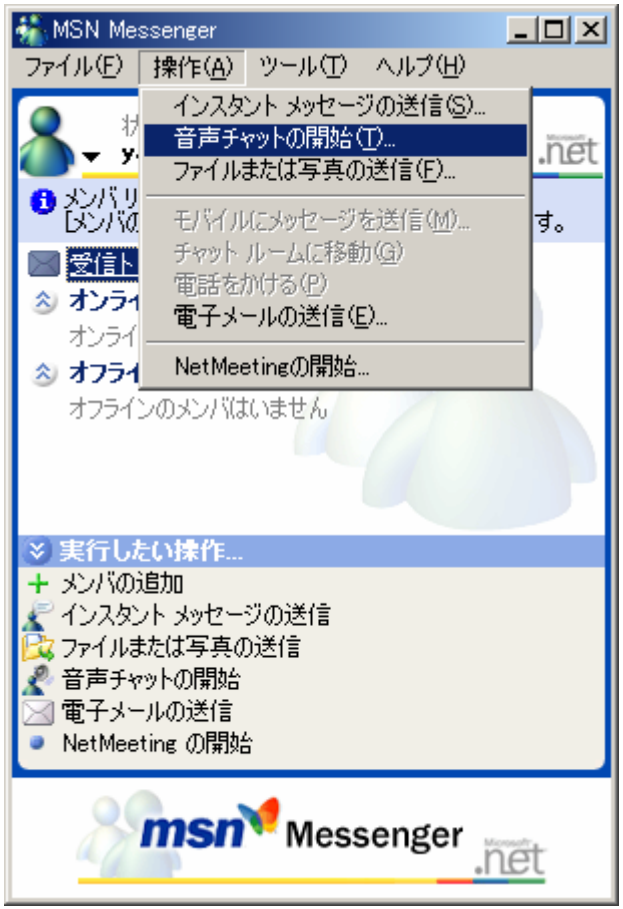
大阪	9#2
浦安	9#4

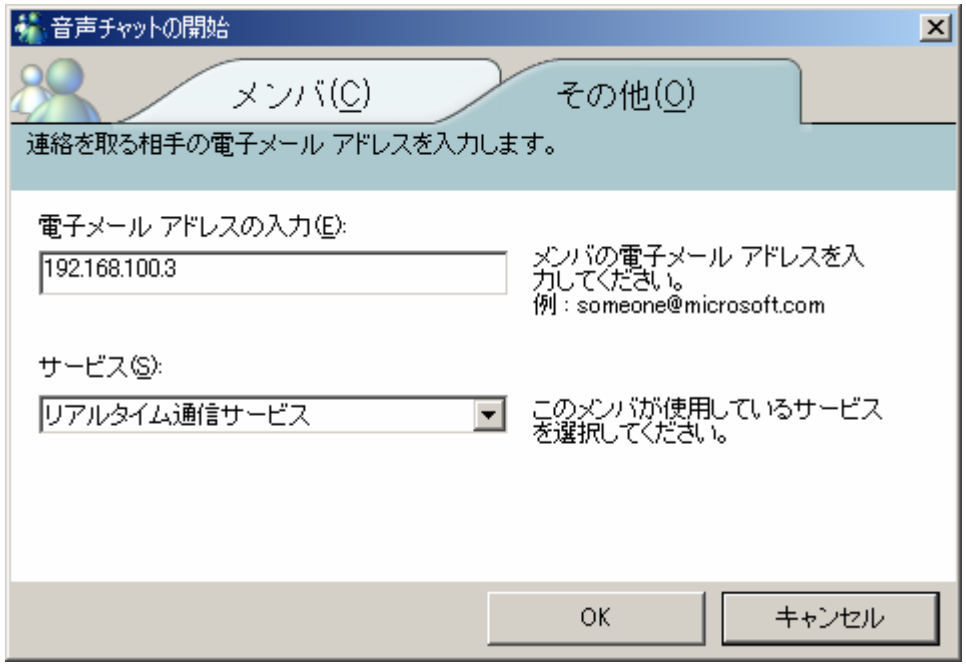
大阪	9#2
浜松	9#3

http://www.rtpro.yamaha.co.jp/RT/FAQ/VoIP/WinMsg/messenger.html

配線例



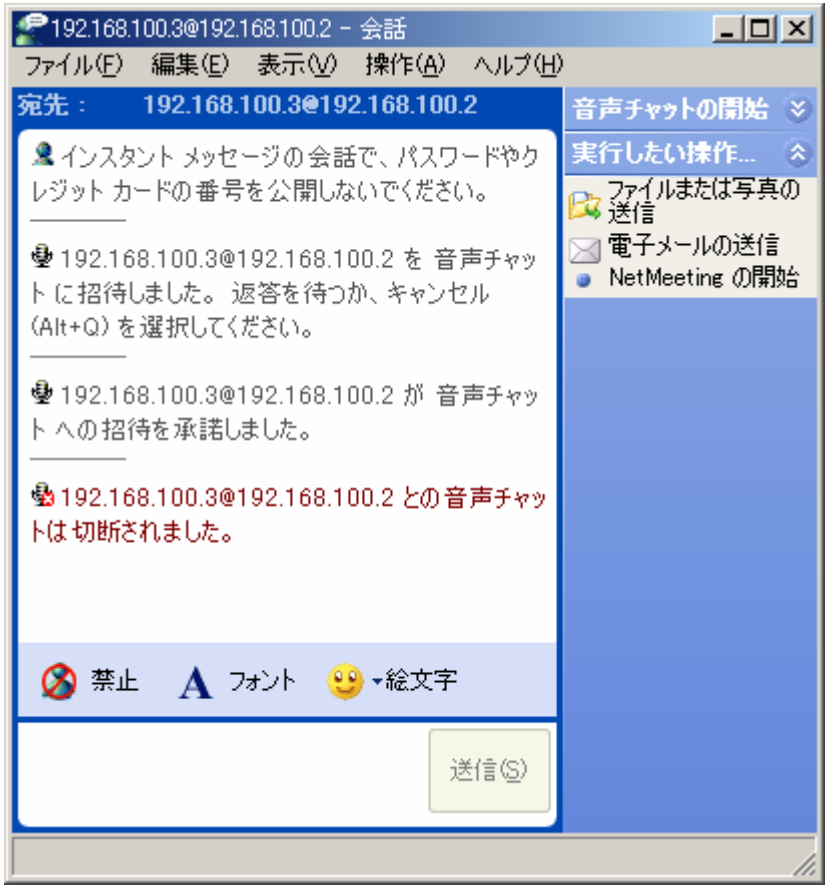


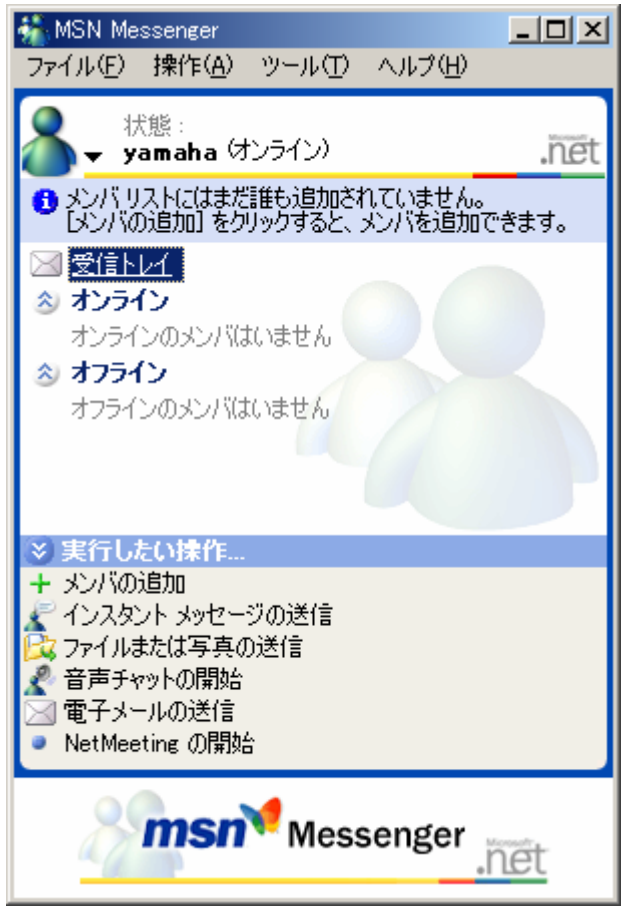


http://messenger.msn.co.jp/

※「リアルタイム通信サービス」**の利用できる版が必要です。**

例) 4.6.0082

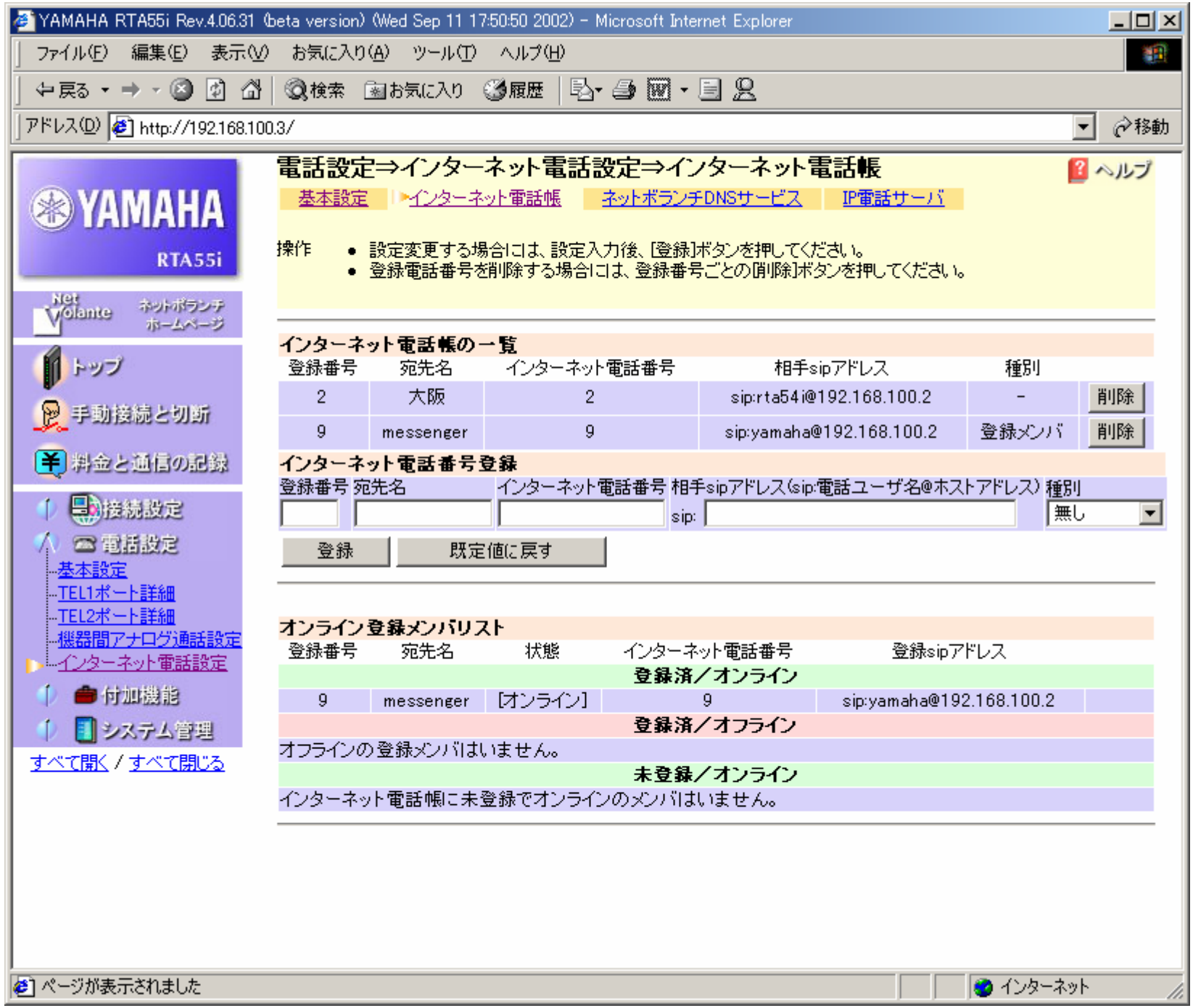




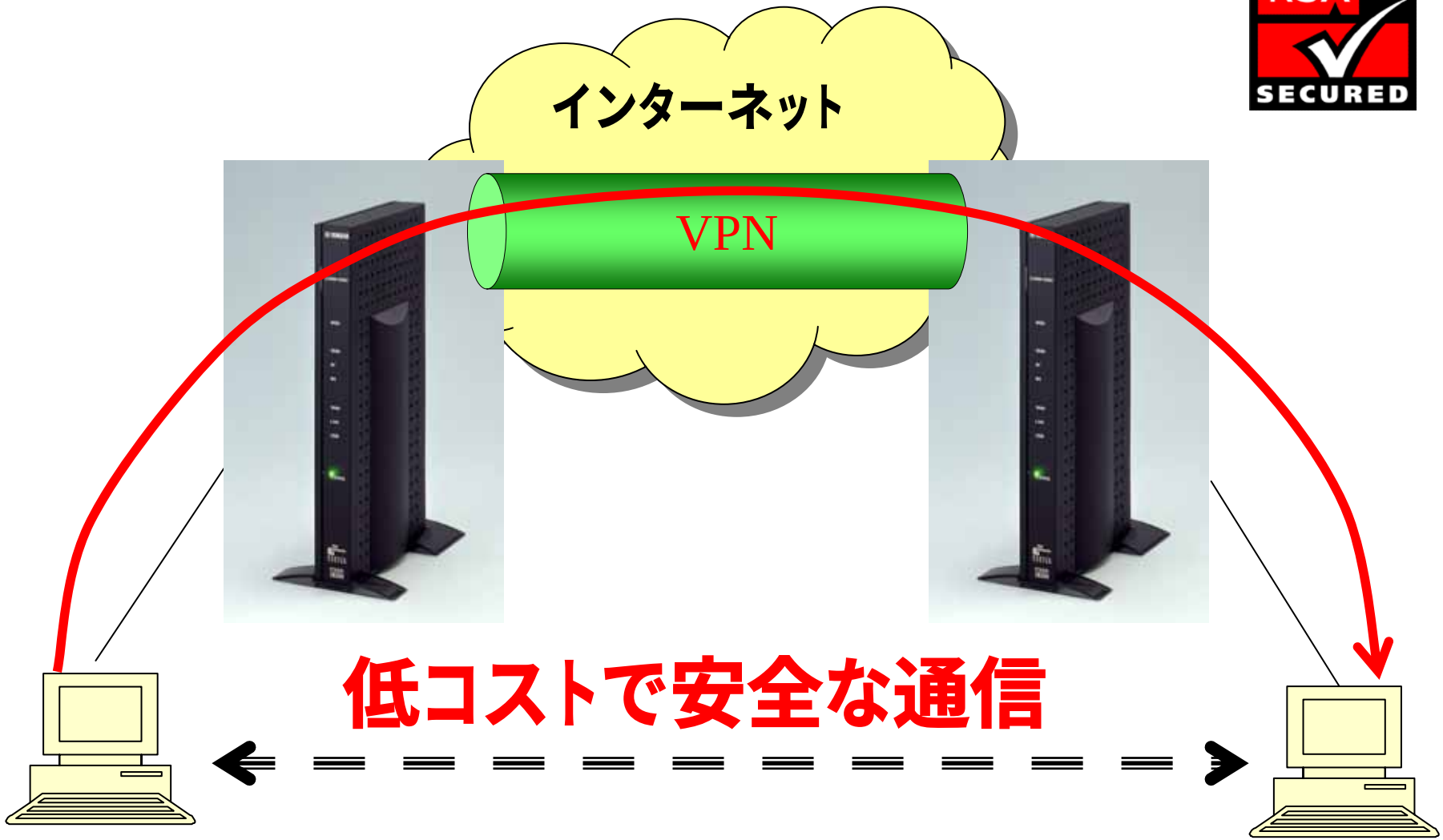
http://messenger.msn.co.jp/

※「リアルタイム通信サービス」の利用できる版が必要です。

例) 4.6.0082


YAMAHA RTA55i Rev.4.06.31 (beta version) (Wed Sep 11 17:50:50 2002) - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る 検索 お気に入り 履歴
アドレス(D) http://192.168.100.3/
移動
YAMAHA
RTA55i
Net Volante ネットボランチ ホームページ
トップ
手動接続と切断
料金と通信の記録
接続設定
電話設定
基本設定
TEL1ポート詳細
TEL2ポート詳細
機器間アナログ通話設定
インターネット電話設定
付加機能
システム管理
すべて開く / すべて閉じる
電話設定⇒インターネット電話設定⇒インターネット電話帳
ヘルプ
基本設定 インターネット電話帳 ネットボランチDNSサービス IP電話サーバ
操作
• 設定変更する場合には、設定入力後、[登録]ボタンを押してください。
• 登録電話番号を削除する場合には、登録番号ごとの[削除]ボタンを押してください。
インターネット電話帳の一覧
登録番号 宛先名 インターネット電話番号 相手sipアドレス 種別
2 大阪 2 sip:rta54i@192.168.100.2 - 削除
9 messenger 9 sip:yamaha@192.168.100.2 登録メンバ 削除
インターネット電話番号登録
登録番号 宛先名 インターネット電話番号 相手sipアドレス(sip:電話ユーザ名@ホストアドレス) 種別
sip:
無し
登録 既定値に戻す
オンライン登録メンバリスト
登録番号 宛先名 状態 インターネット電話番号 登録sipアドレス
登録済／オンライン
9 messenger [オンライン] 9 sip:yamaha@192.168.100.2
登録済／オフライン
オフラインの登録メンバはいません。
未登録／オンライン
インターネット電話帳に未登録でオンラインのメンバはいません。
ページが表示されました
インターネット

VPN(仮想専用線)



実験環境で、LAN間接続VPN

(固定) 192.168.100.1

仮想インターネット

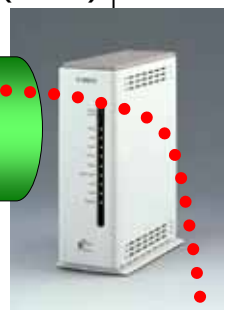
192.168.100.0/24

(固定) 192.168.100.2

(固定) 192.168.100.3

(固定) 192.168.100.4

VPN



192.168.2.0/24

192.168.3.0/24

192.168.4.0/24

PC

PC

<大阪>

<浜松>

<浦安>

YAMAHA

実験環境で、リモートアクセスVPN

(固定) 192.168.100.1

仮想インターネット

192.168.100.0/24

(固定) 192.168.100.2

(固定) 192.168.100.3

(固定) 192.168.100.4

VPN

PC
Microsoft
VPN Adapter

192.168.2.0/24

192.168.3.0/24

192.168.4.0/24

PC

PC

<大阪>

<浜松>

<浦安>

<出張先>

Windows Messenger 対応

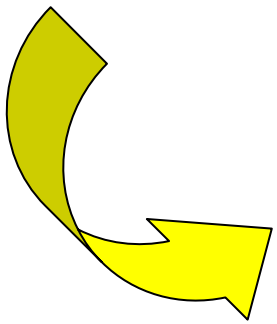
RSA SECURED

ヤマハ ルーター
ファイアウォール機能
～説明資料～

- ヤマハルーターの構造とフレキシビリティ
- アドレス変換
- フィルタリング

ファイアウォールの要素

[必須]
- 高度な静的フィルタリング
- アドレス変換



[ヤマハルータ]
- フィルタ定義数
- VPNへの適用
- 高度な動的フィルタリング
- 不正アクセス検知機能
- IPv6対応

ファイアウォール機能の特徴

- **デフォルトの高いセキュリティポリシー**

  [ネットボランチ]

  a) 常時接続の設定を選択した場合には、セキュリティフィルタが自動適用される。

  b) 7段階のセキュリティレベルの選択によって、誰もかんたんに安全性が得られる。

  c) 安全性を考慮して、パスワード管理の習慣を持ってもらう。

  ⇒WWW設定機能では、最初にパスワードを設定してもらう。

- **常時接続を想定した高度なフィルタリング機能**

  a) 動的フィルタリング

  静的フィルタリングの弱点を補強し、高度なセキュリティとセキュリティフィルタの扱い易さを提供する。⇒利便性とセキュリティの両立

  b) 不正アクセス検知

  侵入(Intrusion)や攻撃(attack)を目的とするパケットを受信したときに、それを検出してユーザに通知(ログ、ブザー、メール)

- **フレキシビリティ**

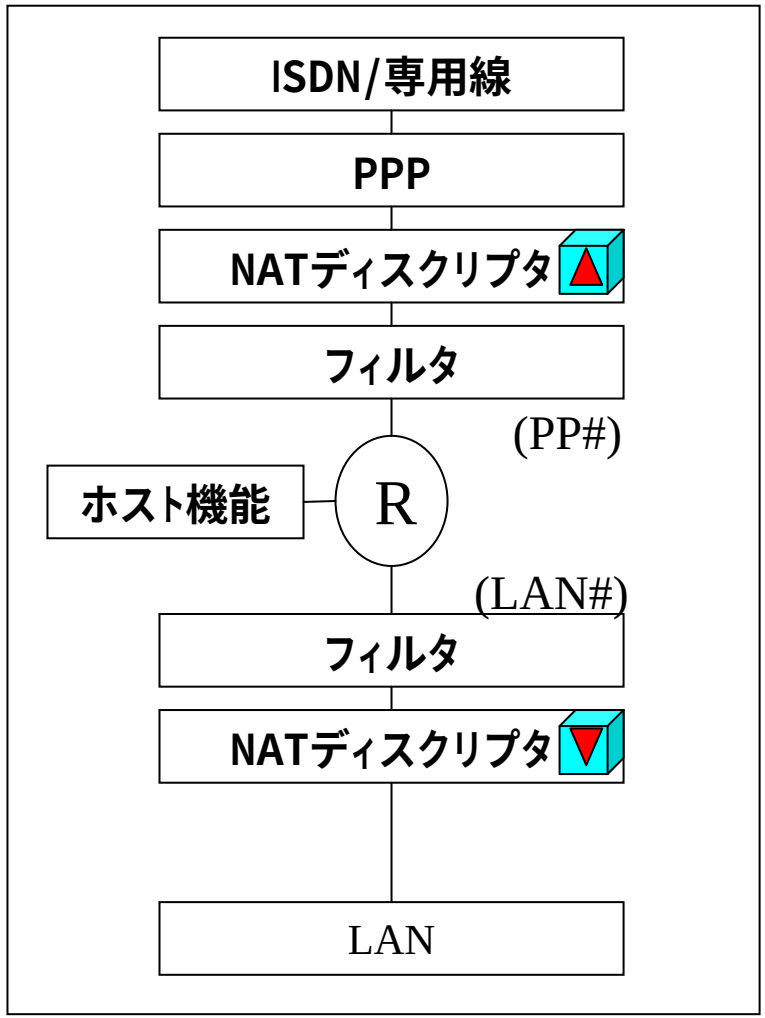
  a) フィルタ定義数の制限緩和

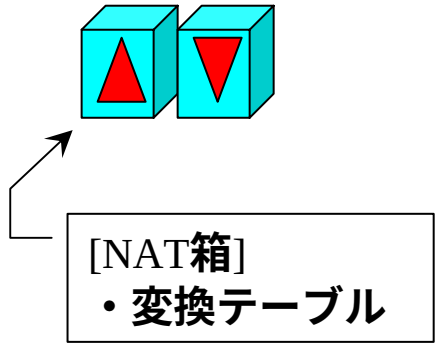
構造#1(PPP)

RT140i

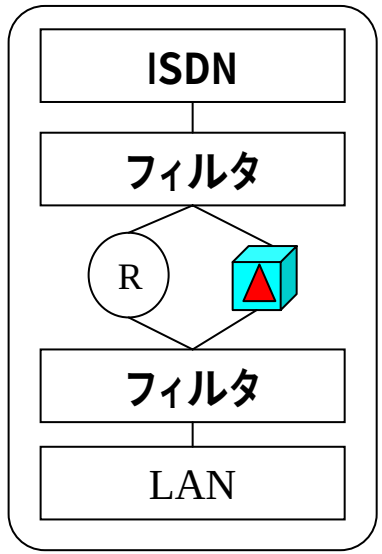
RT105i

RTA52i





比較構成例

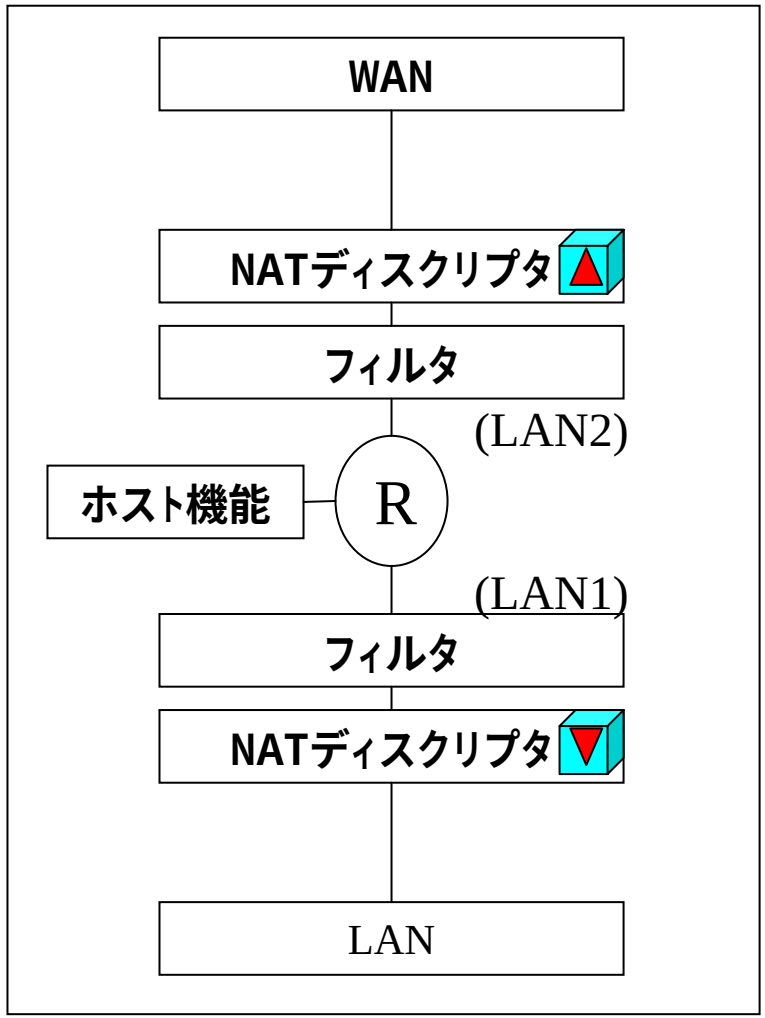


構造#2(ローカルルータ)

RT300i

RT140e

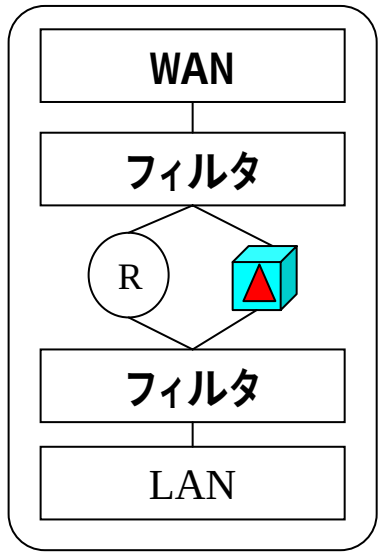
RT105e



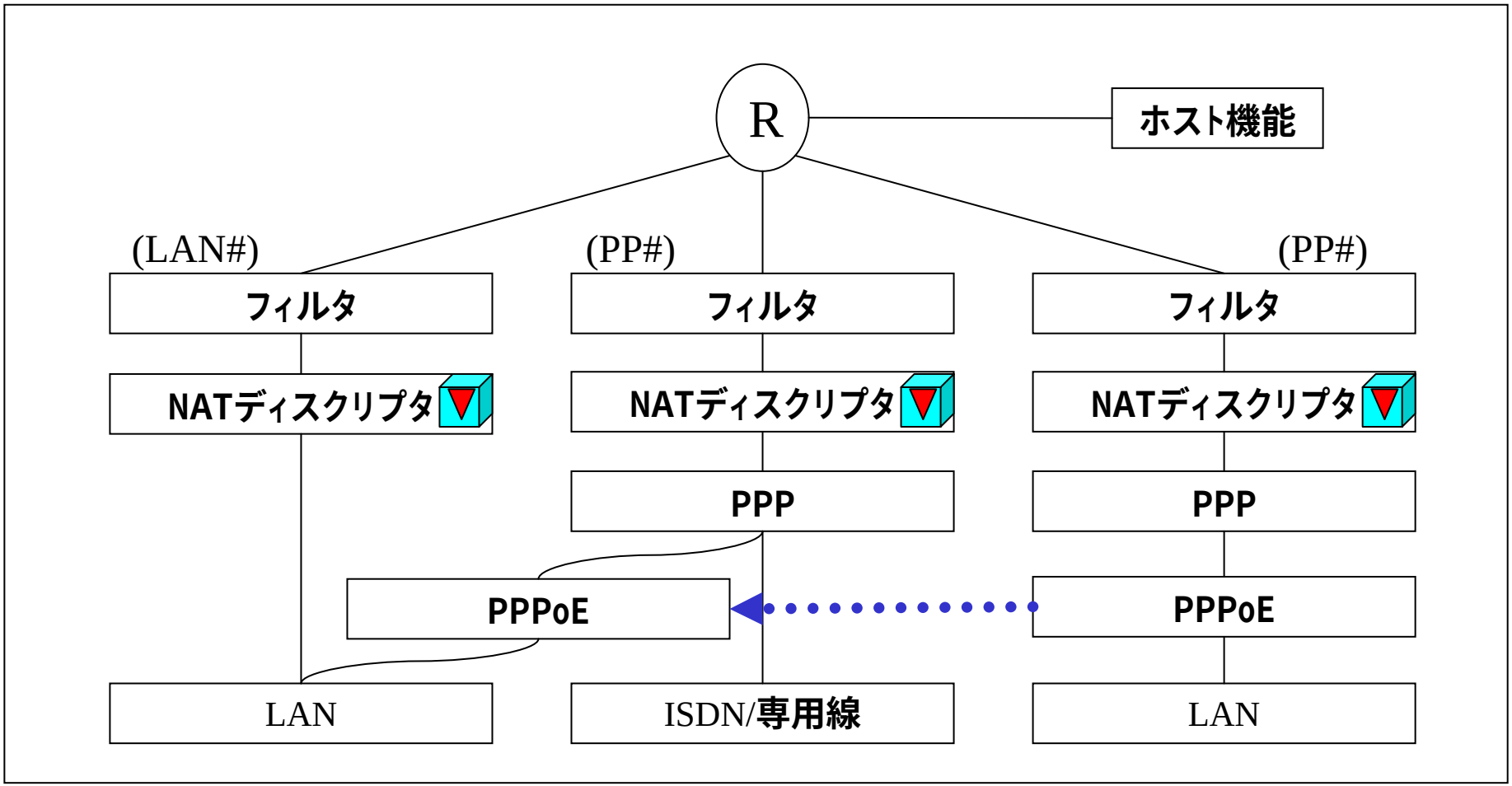
RTW65b

RTA55i

比較構成例



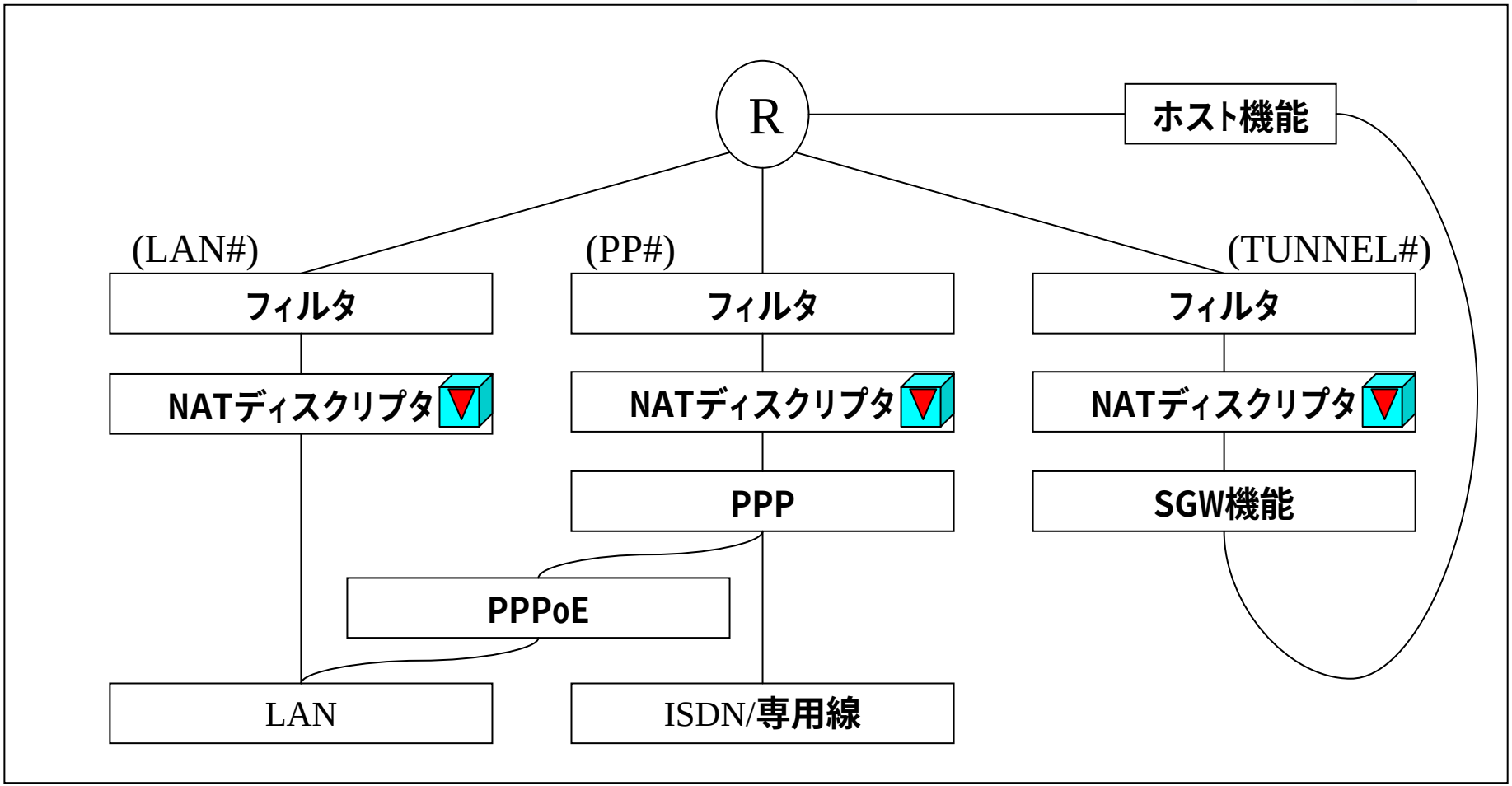
構造#3(PPPoE)



RT300i

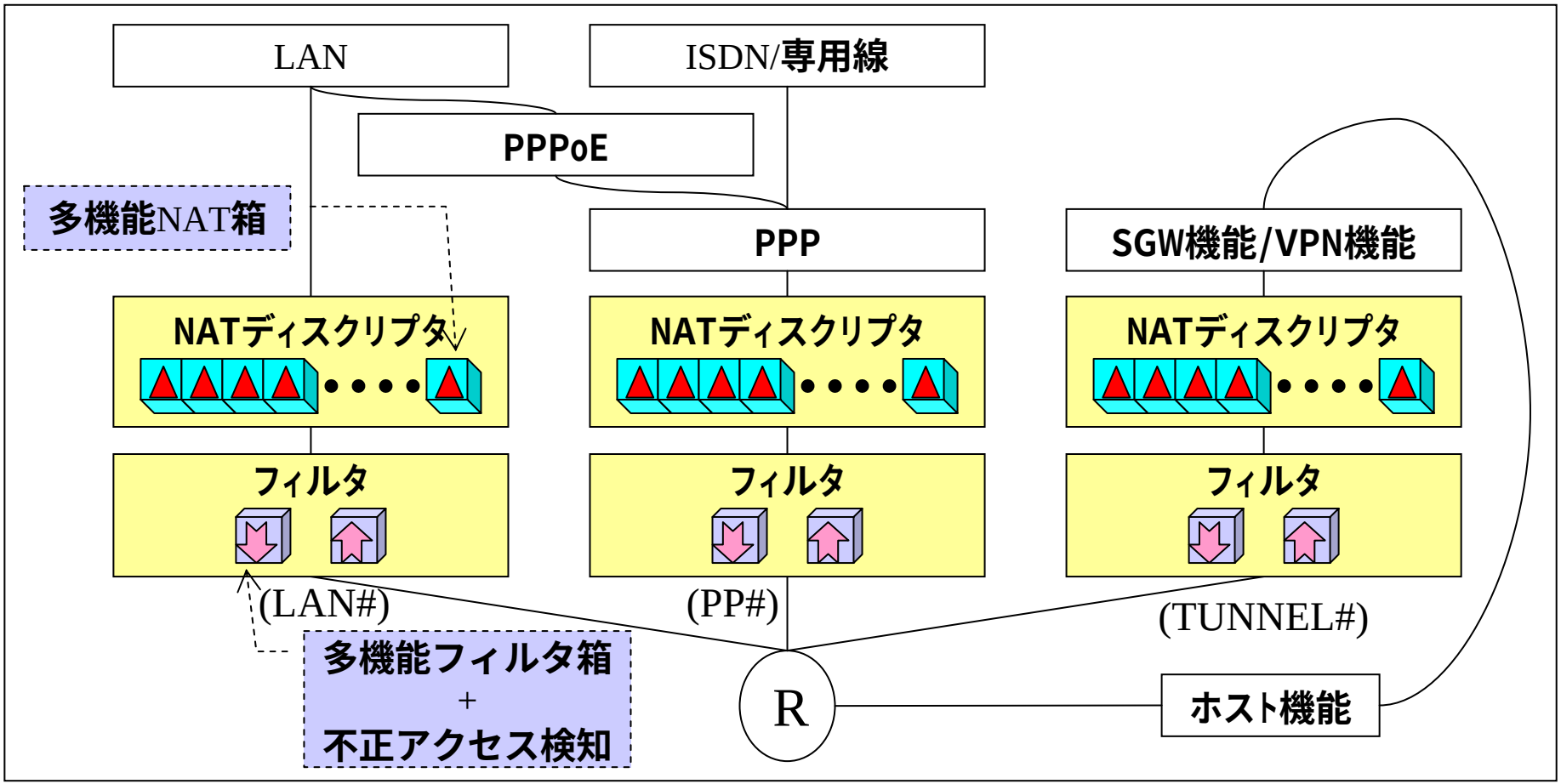
構造#4(VPN)

RT105シリーズ



ファイアウォールのフレキシビリティ

ファイアウォール機能を自由自在に利用できるしくみ



アドレス変換(NATディスクリプタ)

- NATディスクリプタの特徴
- 応用例#1,#2
- IPマスカレードの処理選択
  - incoming/unconvertible/range
- IPマスカレードのアプリケーション対応
  - ping/traceroute/FTP/CU-SeeMe
  - VPNパススルー機能
  - PPTPのマルチセッション対応
  - NetMeeting 3.0対応
- UPnP対応、WindowsMessenger対応

NATディスクリプタの目的･用途
(NATからNATディスクリプタへ)

[NATの経緯]
･1995年にRT100iを発売した。
･インターネット接続の普及が進むと、構築済みのIPネットワークから
インターネット接続を行うためにNAT技術が必要とされた。
･1996年にNAT(Basic NAT)、1997年にIPマスカレード(NAPT)を実装した。
･主な用途は、インターネット接続用であった。
[課題]
･インターネット接続の普及と平行して、IPによる拠点間接続が増えたことに
より、色々なアドレスが重複して、直接通信ができない問題が発覚した。
[NATディスクリプタの開発目的]
･IPアドレス問題に関する問題解決手段を提供すること。
･LAN間通信でNAT/IPマスカレードを利用可能にすること。
･NAT/IPマスカレードをインタフェースに依存しない使い方に統一すること。

アドレス変換機能(NAT)への取り組み

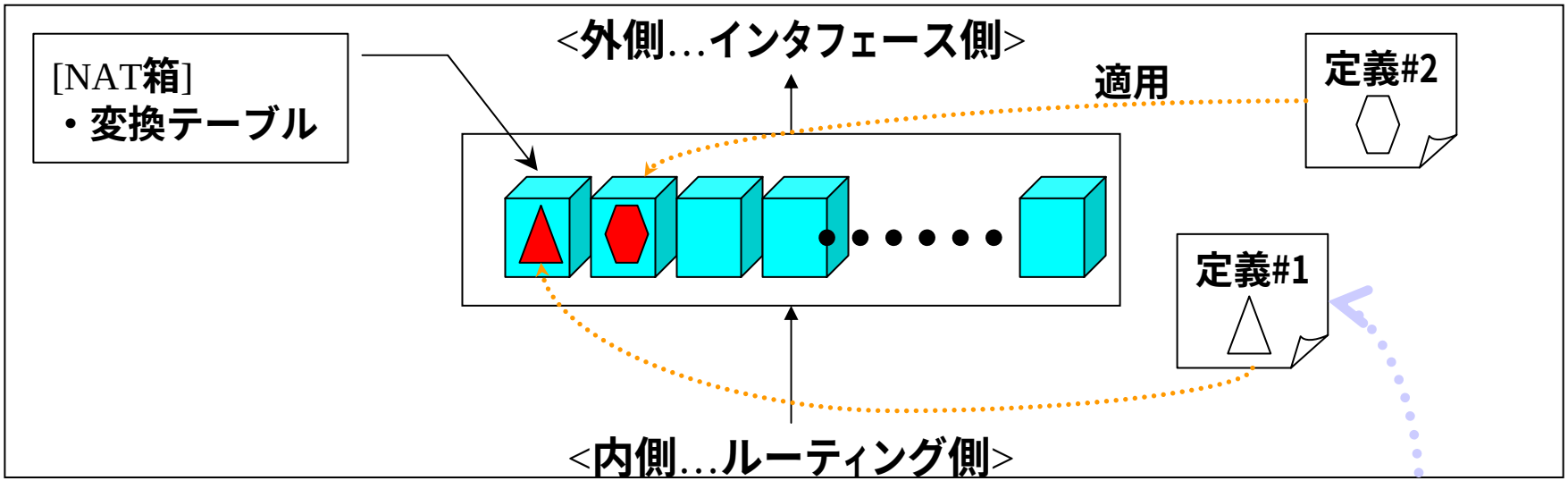
日付	Revision	内容
1996年6月	Rev.1.06.08	・NAT機能
1996年11月	Rev.1.06.22	・IPマスカレード機能
1997年10月	Rev.2.02.15	・静的IPマスカレード機能
1999年 1月	Rev.4.00.02	・NATディスクリプタ機能(機能統合、多重適用、PP側適用、LAN側適用)
1999年4月	Rev.4.00.07	・TUNNELインタフェースへのNATディスクリプタ適用
1999年 8月	Rev.4.00.13	・ping./traceroute対応 ・IPマスカレード管理テーブルの仕様変更
2000年7月	Rev.4.00.39	・VPNパススルー(静的IPマスカレードの制限緩和)
2001年7月	Rev.6.02.07	・IPマスカレードにおける破棄パケットのログ
2002年1月	Rev.6.02.16	・DMZホスト機能 ・NetMeeting 3.0対応変換機能
2002年3月	Rev.6.02.18	・PPTPのマルチセッション対応処理 ・IPマスカレードのポート割り当て方式の指定 (常時変換、必要時変換) ・IPマスカレードのポーと割り当て範囲の指定 ・NAT/IPマスカレードのFTP監視ポートの指定

旧NAT機能(Rev.1系〜Rev.3系)からの主な違い

- LANインタフェースに対応
  - LANのprimary⇔secondaryの変換が可能
- TUNNELインタフェースに対応
  - VPNで変換が可能
- 3つの変換タイプ
  - NAT形式
  - IPマスカレード形式
  - NAT + IPマスカレード形式
- 機能統合、制限の緩和
  - 複数の変換規則を並列的に適用可能
    (ひとつのインタフェースに16組)

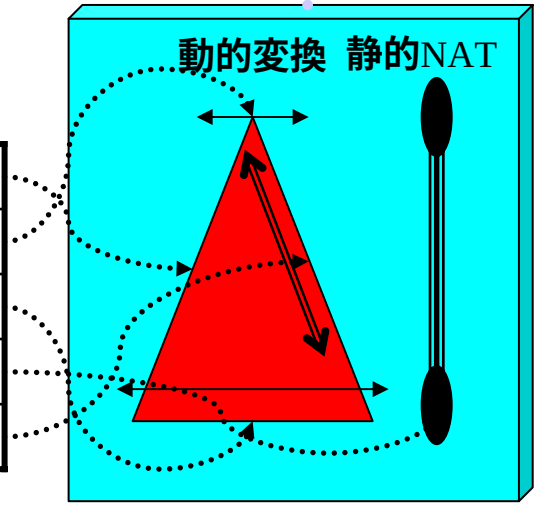
http://www.rtpro.yamaha.co.jp/RT/docs/nat-descriptor/index.html

NATディスクリプタの構造



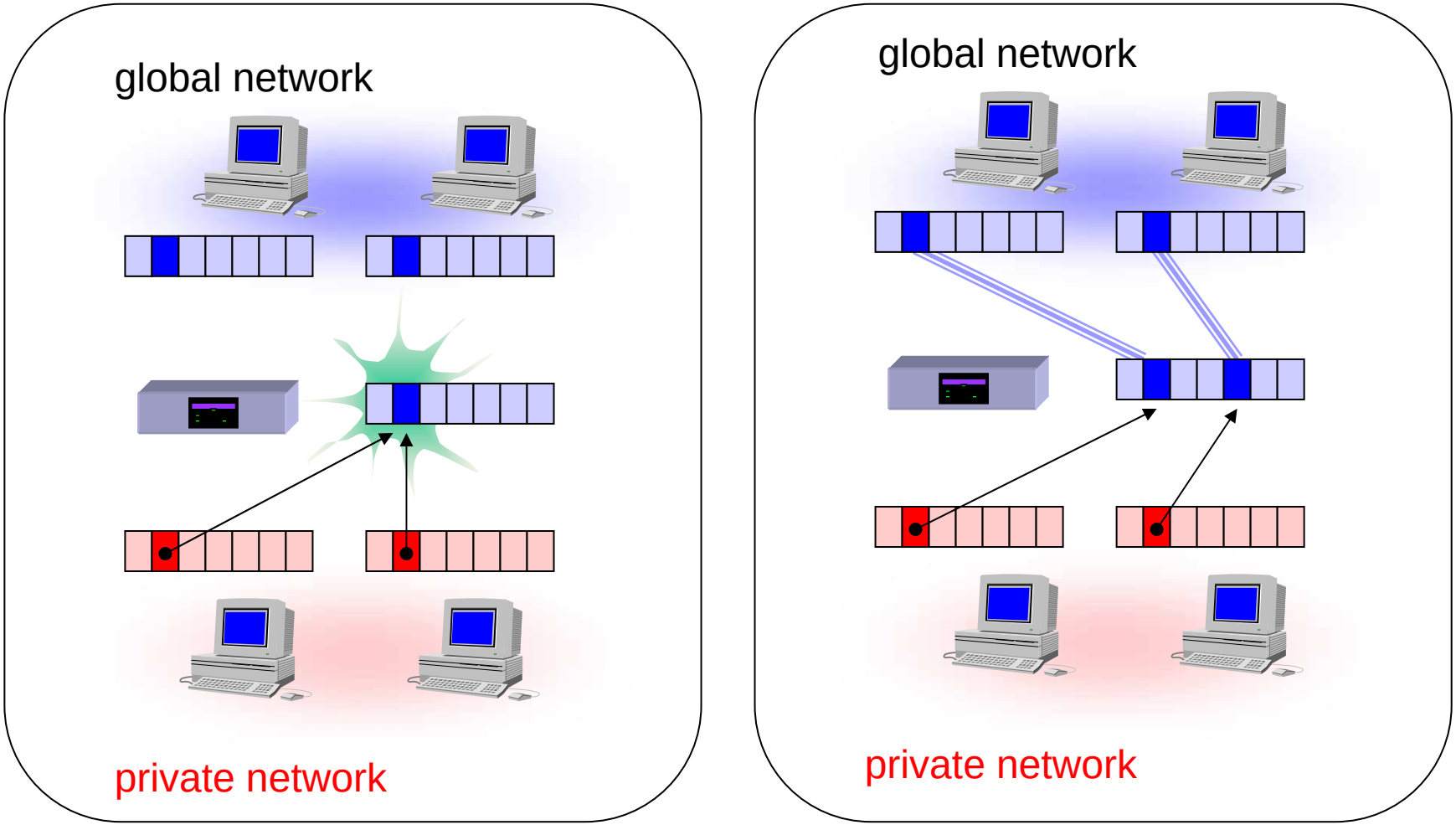
[定義→アドレス変換の設計図]

変換タイプ	動的なアドレス変換形式
外側アドレス範囲	動的アドレス変換に使用される範囲
内側アドレス範囲	動的アドレス変換の対象となる範囲
静的NAT	固定的なアドレス変換の組み合わせ
静的IPマスカレード	固定的なIPマスカレード変換



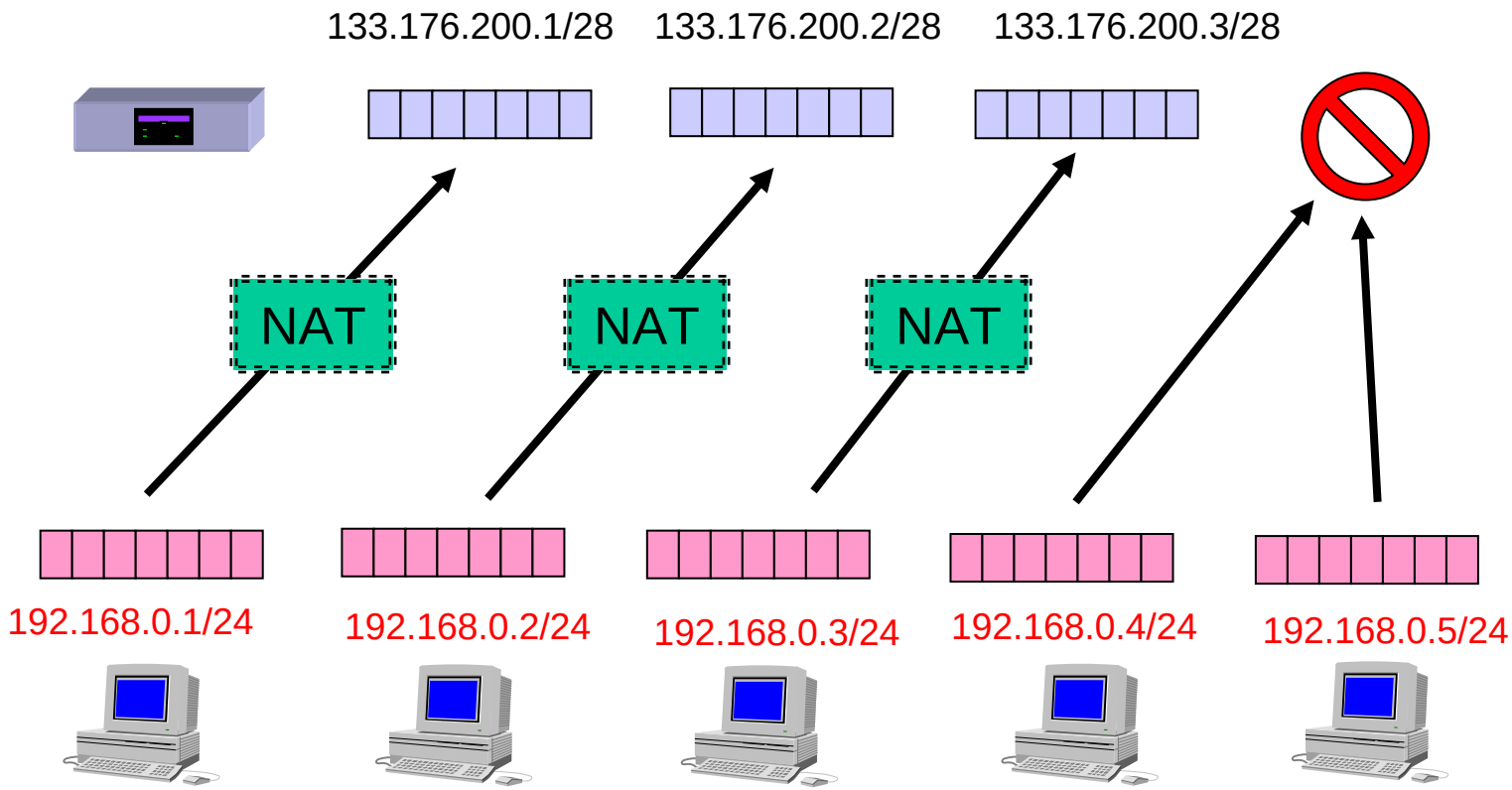
IPマスカレード(IP Masquerade)

nat descriptor type <NATディスクリプタ番号> masquerade



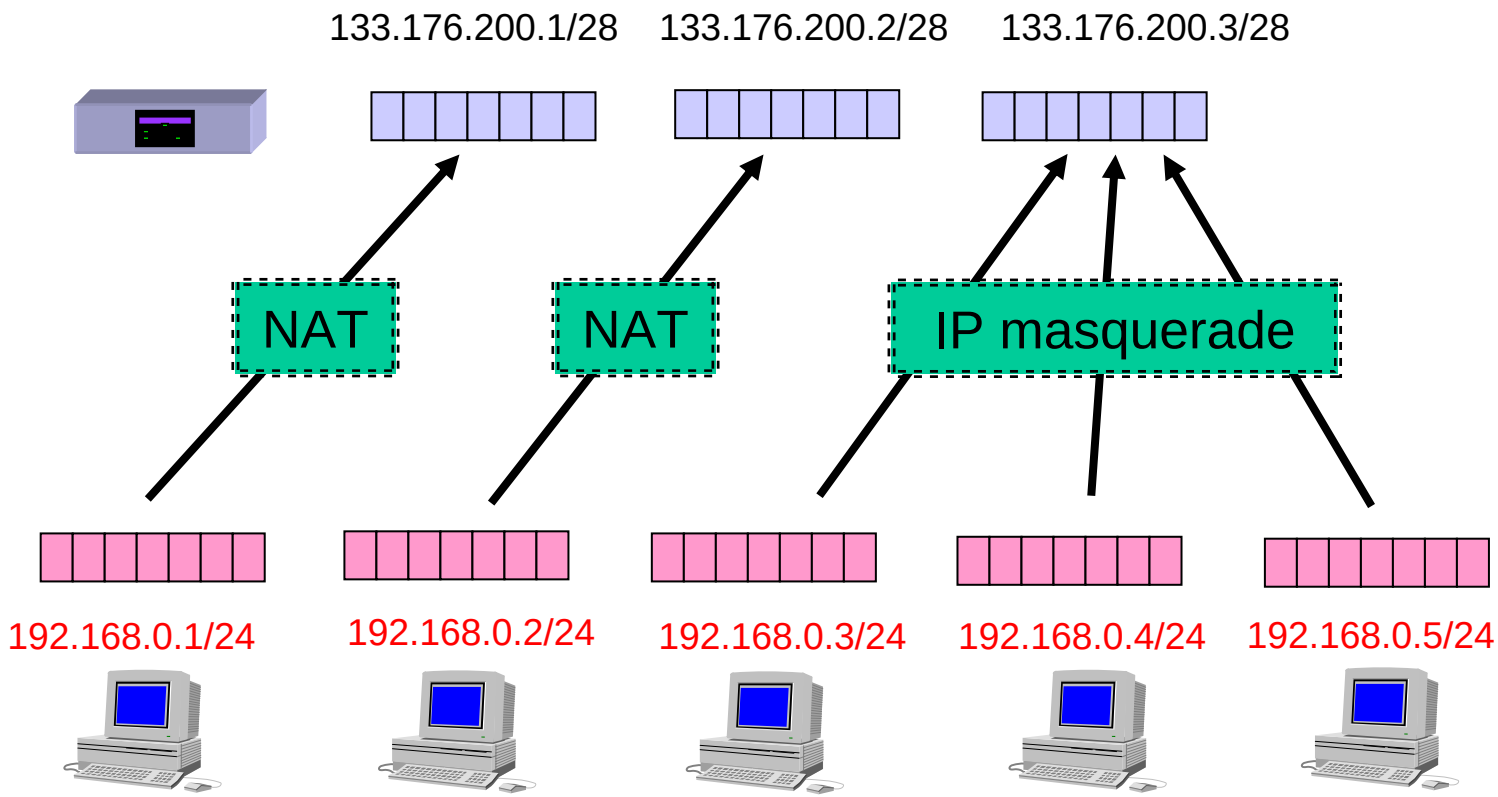
NAT (Network Address Translation)

nat descriptor type <NATディスクリプタ番号> nat

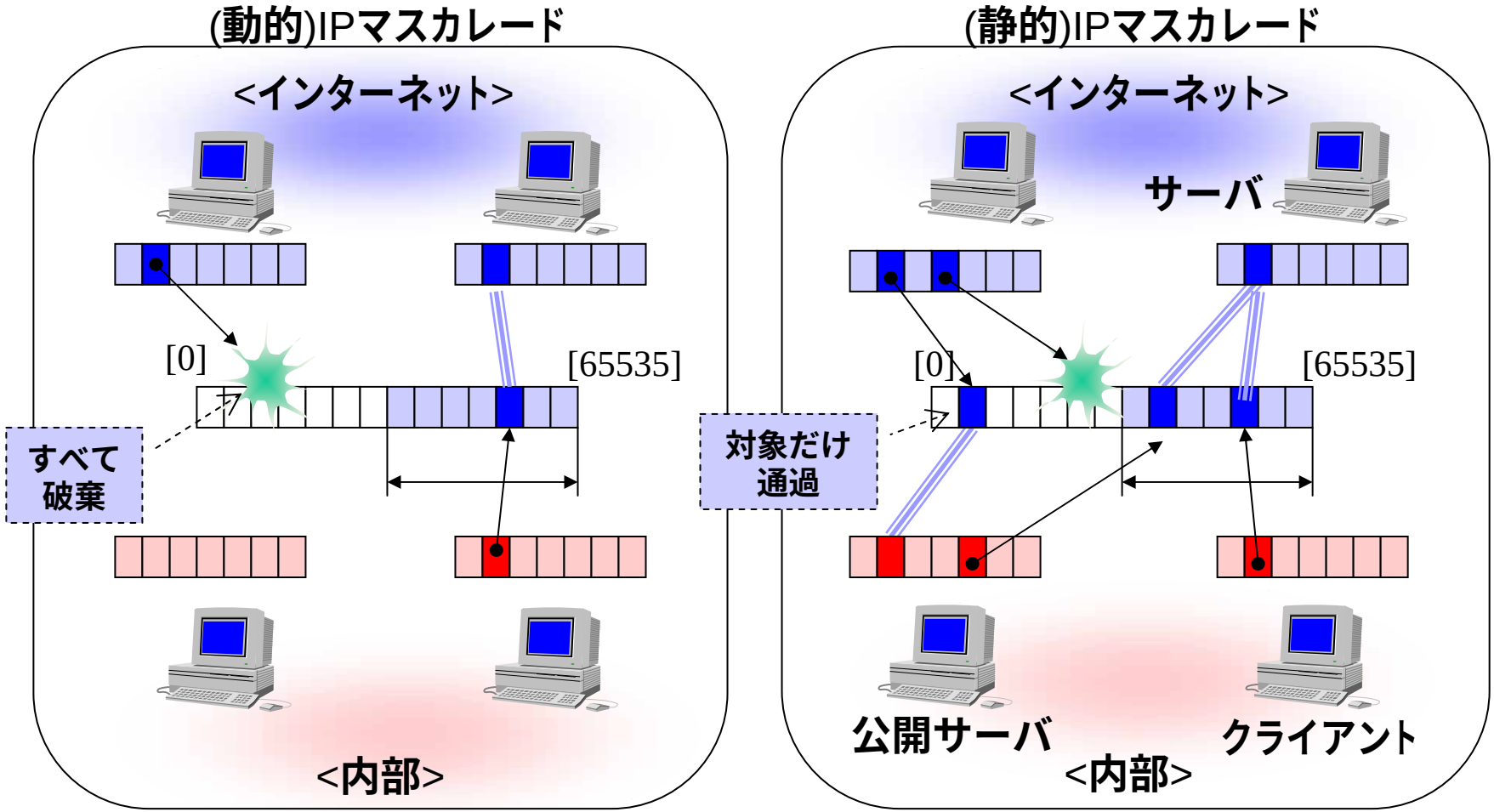


NAT + IPマスカレード形式

nat descriptor type <NATディスクリプタ番号> nat-masquerade



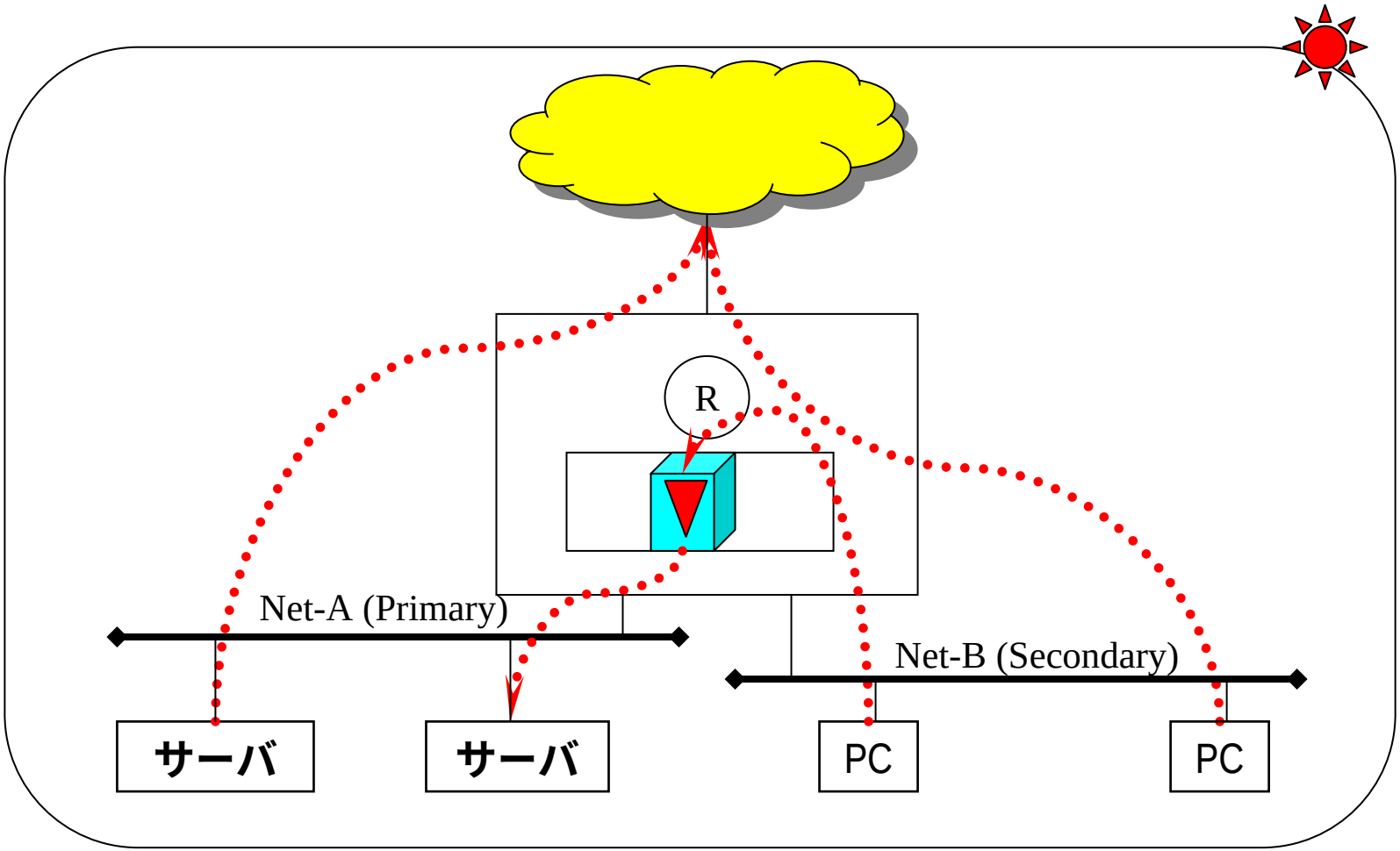
静的IPマスカレード



(静的IPマスカレード)

特定の通信だけ固定して、公開する。

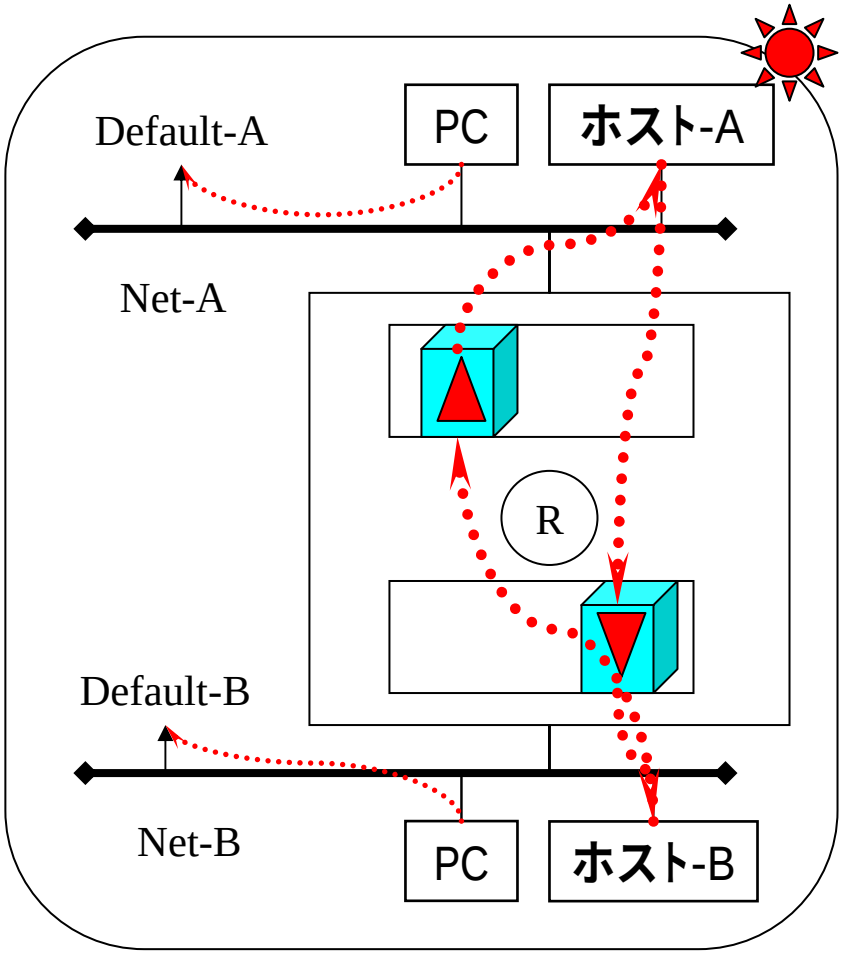
NATディスクリプタの応用例#1



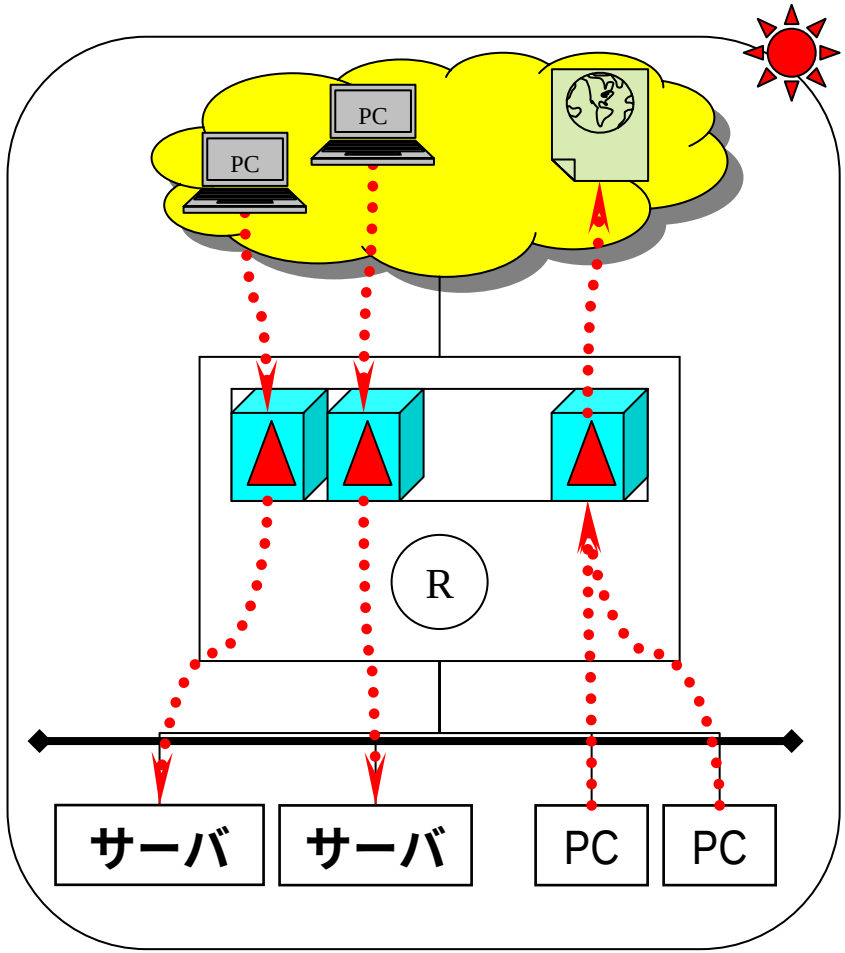
primary⇔secondary間のIPマスカレード (逆マスカレード)

http://www.rtpro.yamaha.co.jp/RT/docs/nat-descriptor/example/index.html

NATディスクリプタの応用例#2



2つの隔離されたネット間での通信(hot line)



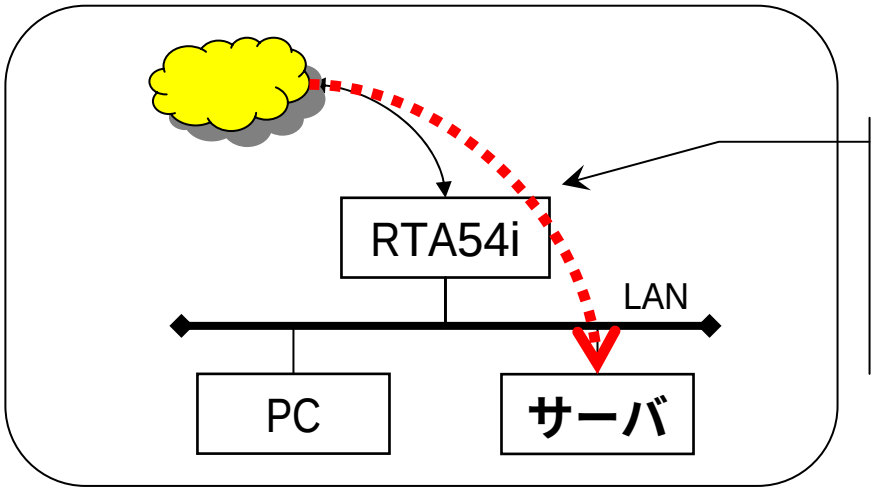
公開サーバにIPマスカレード適用

http://www.rtpro.yamaha.co.jp/RT/docs/nat-descriptor/example/index.html

IPマスカレードの機能選択

- **外来パケット処理選択**(incoming)
  - **変換しないで、通過**(through)
  - **破棄** (reject,discard)
  - **特定のアドレスに変換** (forward…DMZ**ホスト機能**)
- **ポート割り当て方式の選択**(unconvertible port)
  - **必ずポート番号変換する処理**
  - **可能な限りポート番号変換しない処理**
- **ポート割り当て範囲の選択**(port range)
  - **ポート番号変換の割り当て範囲の変更**

DMZホスト機能



ISDN/ADSL/CATVプロバイダ接続(LAN)

[IPマスカレードの処理選択]
- through … 変換せずに通す
- reject …. 破棄して、TCPの場合はRSTを返す
- discard … 破棄して、何も返さない
- forward … 指定されたホストに転送する

・ネットアプリ対応/ネットゲーム対応の機能
IPマスカレード機能を利用してインターネット接続を共有しているとき、インターネット側からの接続要求を特定のサーバ/ホストに転送する機能。
※セキュリティホールの側面

DMZホスト機能
～コマンド仕様～

IPマスカレードで、外側から受信したパケットに該当する変換テーブルが存在しないときに、そのパケットを特定のホストに転送できるようにした。このほかにも、破棄や通過などの動作を選択することができる。

○IPマスカレードで外側から受信したパケットに該当する変換テーブルが存在しないときの動作の設定

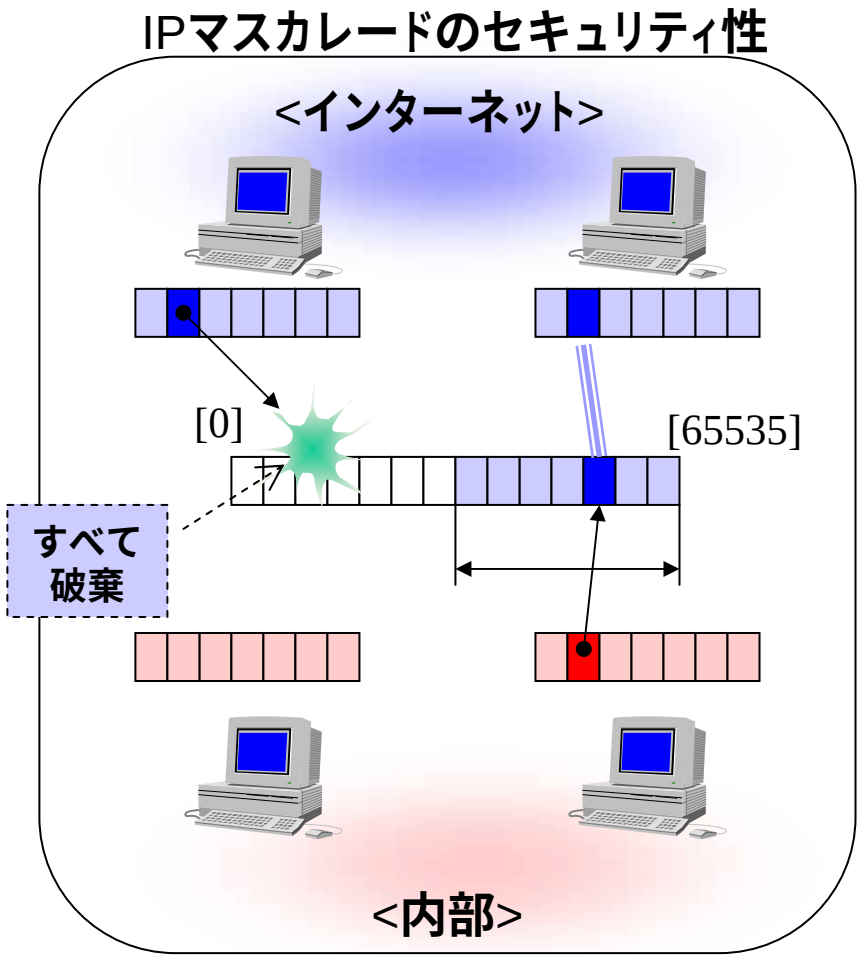
[入力形式] nat descriptor masquerade incoming DESC_ID ACTION [IP_ADDRESS]

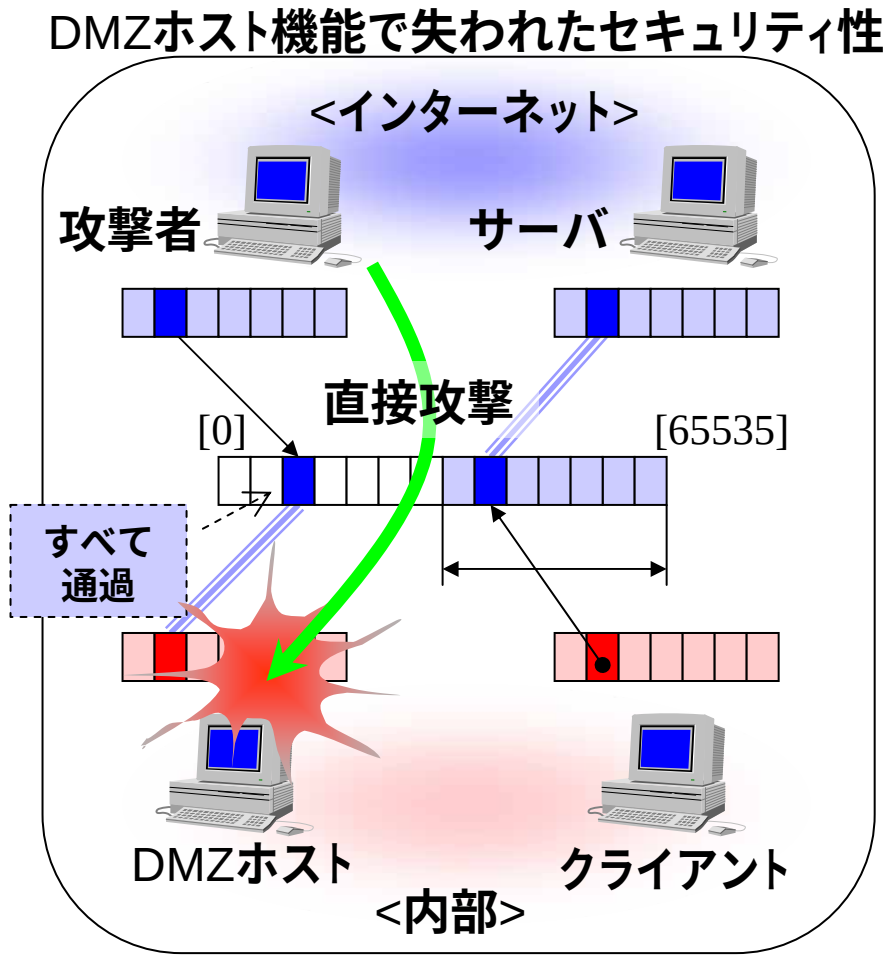
[パラメータ] - DESC_ID ..... NATディスクリプタ番号
- ACTION ..... 動作
  - through ... 変換せずに通す
  - reject .... 破棄して、TCPの場合はRSTを返す
  - discard ... 破棄して、何も返さない
  - forward ... 指定されたホストに転送する
- IP_ADDRESS ... 転送先のIPアドレス

[説明] IPマスカレードで外側から受信したパケットに該当する変換テーブルが存在しないときの動作を設定する。ACTIONがforwardのときにはIP_ADDRESSを設定する必要がある。

[デフォルト値] reject

DMZホスト機能の脆弱性

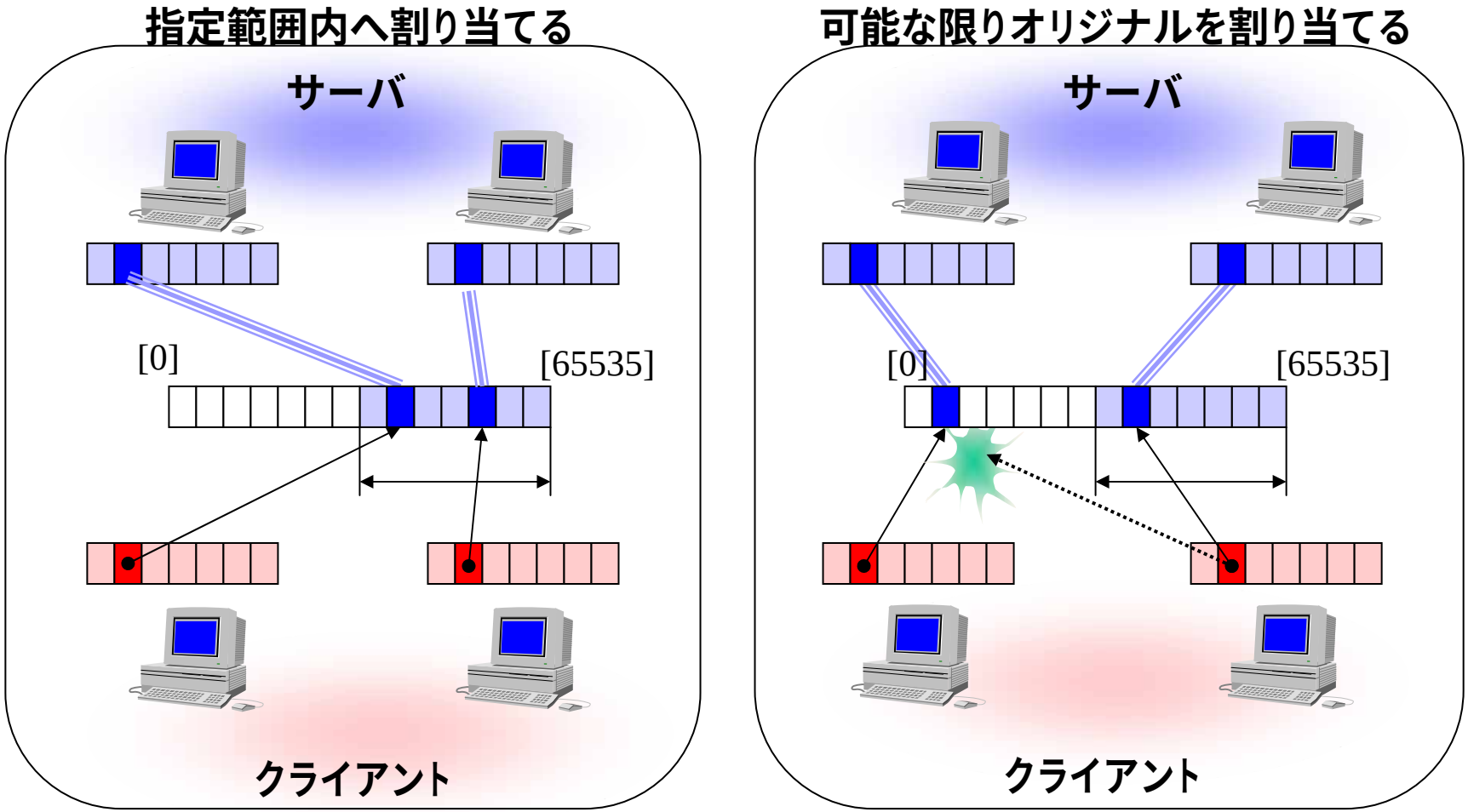




(利便性とセキュリティ性のトレードオフ)

アドレス変換の苦手なアプリケーションが便利になるが、セキュリティ性は低下する。

ポート割当方式指定機能



ポート番号変換を苦手とするアプリケーションの通信をできる限り救う。.

ポート割当方式指定機能
～コマンド仕様～

IPマスカレードで可能な限りポート番号変換を行わない方式を選択可能にした。これにより、アドレス変換を苦手とするアプリケーションを救えるようになる。

○IPマスカレードで、特定のポート番号は変換せずにそのまま外部に転送できる機能
を実装した。

[入力形式]

```
nat descriptor masquerade unconvertible port DESC if-possible
nat descriptor masquerade unconvertible port DESC PROTOCOL PORT
```

[パラメータ]

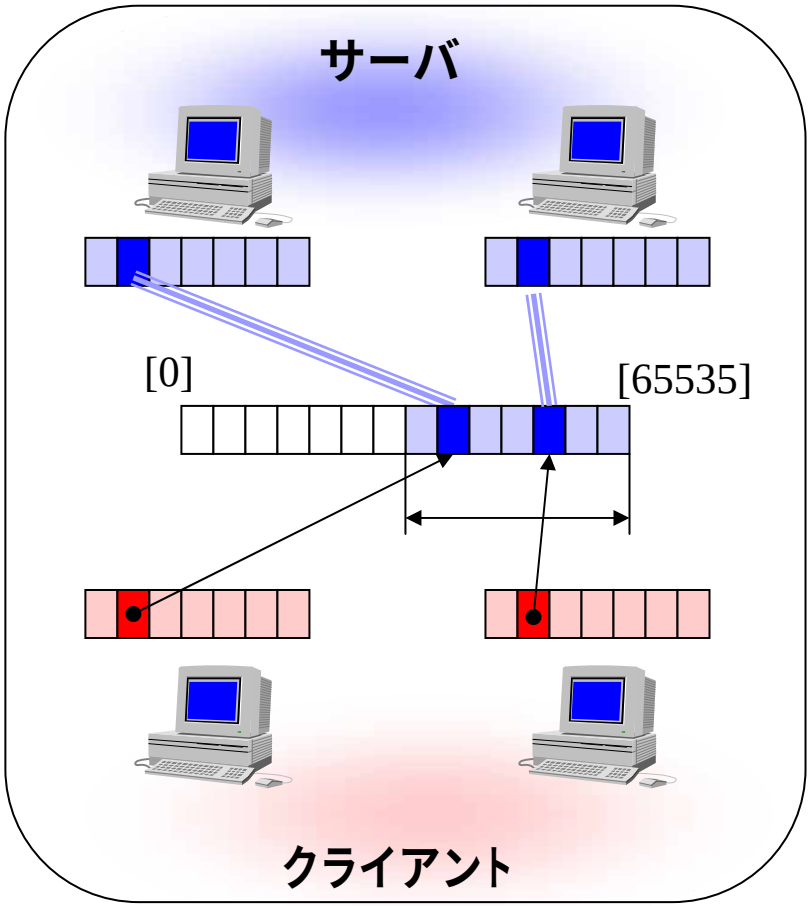
DESC ... ディスクリプタ番号
PROTOCOL ... プロトコル、'tcp'もしくは'udp'
PORT ... ポート番号の範囲

[説明]

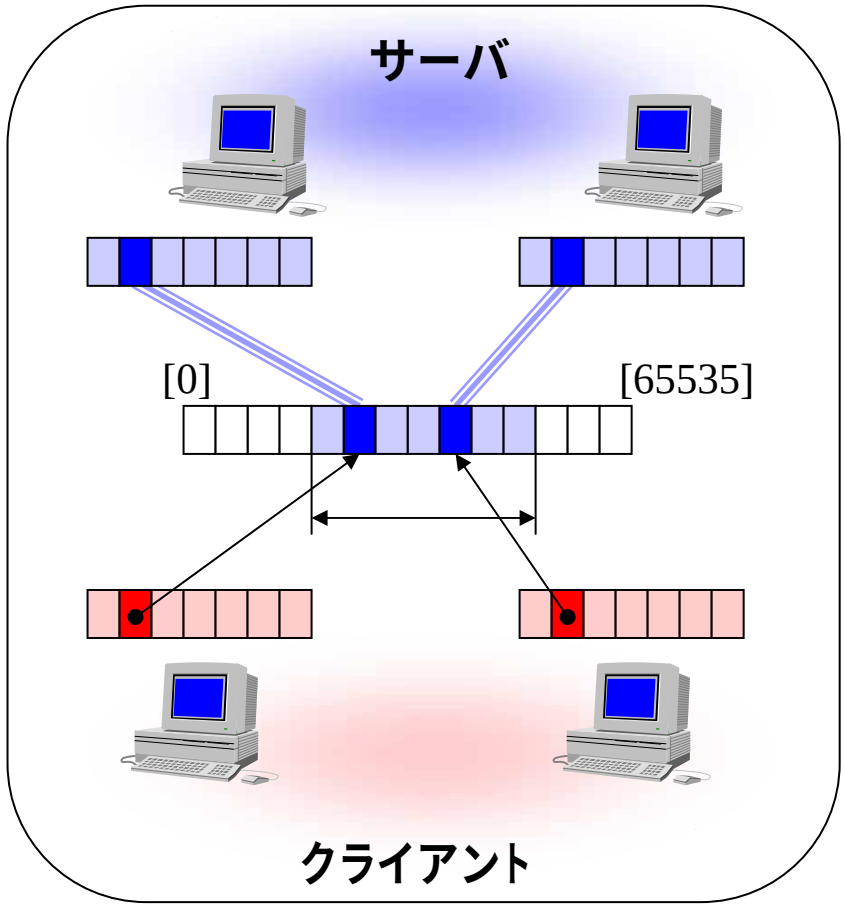
IPマスカレードで変換しないポート番号の範囲を設定する。
if-possibleが指定されている時には、処理しようとするポート番号が他の通信で使われていない場合には値を変換せずそのまま利用する。

ポート割り当ての範囲指定機能

通常の割り当て範囲



割り当て範囲を変更



IPマスカレードで使用しているポート割り当て範囲(60000～64095)を他のアプリケーションで利用することができる。

ポート割り当ての範囲指定機能
～コマンド仕様～

IPマスカレードで使用するポート割り当て範囲(60000～64095)を変更することができるようになった。これにより、この範囲を他のアプリケーションで利用することができるようになる。

○IPマスカレードで利用するポートの範囲を設定できるようにした。

[入力形式]

```
nat descriptor masquerade port range DESC START [NUM]
```

[パラメータ]

DESC ... ディスクリプタ番号
START ... 開始ポート番号、1024～65534
NUM ... ポート数、1～4096、省略時は4096

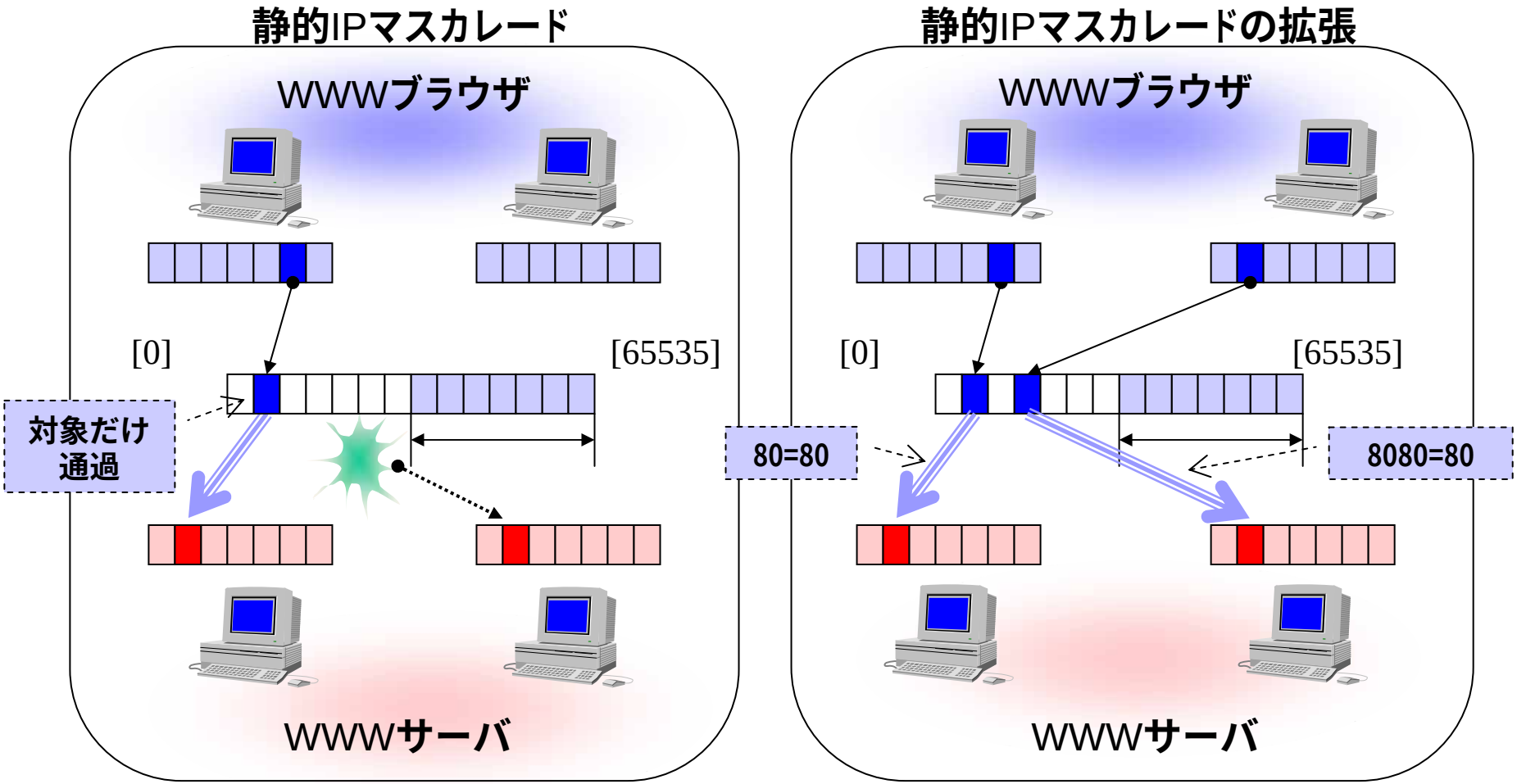
[説明]

IPマスカレードで利用するポート番号の範囲を設定する。STARTとNUMの和が65535以下(START + NUM ≦ 65535)でなくてはいけない。

[デフォルト]

60000 4096

静的IPマスカレードの内側と外側の関連付け



IPマスカレードのポート番号変換を固定(外側=内側、外側!=内側)する。.

静的IPマスカレードの内側と外側の関連付け

～コマンド仕様～

従来、静的IPマスカレード機能は、外側と内側のポート番号を同固定すものだった。外側と内側で異なるポート番号を関連付けできるように拡張した。

○静的IPマスカレード機能を拡張し、外側ポートと 内側ポートを変換できるようにした。

[入力形式]

```
nat descriptor masquerade static DESC ID INNER_IP PROTOCOL
        OUTER_PORT=INNER_PORT
```

[パラメータ]

DESC ... ディスクリプタ番号
ID ... 識別情報
INNER_IP ... 内側で使用するアドレス
PROTOCOL ... プロトコル、‘tcp‘、’udp‘、’icmp’、プロトコル番号
OUTER_PORT ... 外側で使用するポート番号
INNER_PORT ... 内側で使用するポート番号

[説明]

IPマスカレードによる通信でポート番号変換をしないように固定する。
また、外側ポートと内側ポートの関連付けも可能。

IPマスカレードのアプリケーション対応

●FTP対応

FTP/アプリケーション対応の必要性

FTPセッション保持機能

FTP監視ポート指定機能

●NetMeeting 3.0対応

可能な限りポート番号変換しない処理

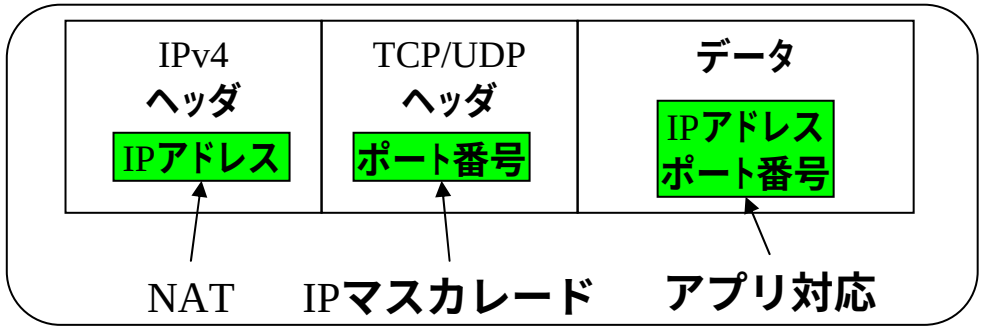
●VPNパススルー機能

同時1セッション、静的IPマスカレードの制限緩和

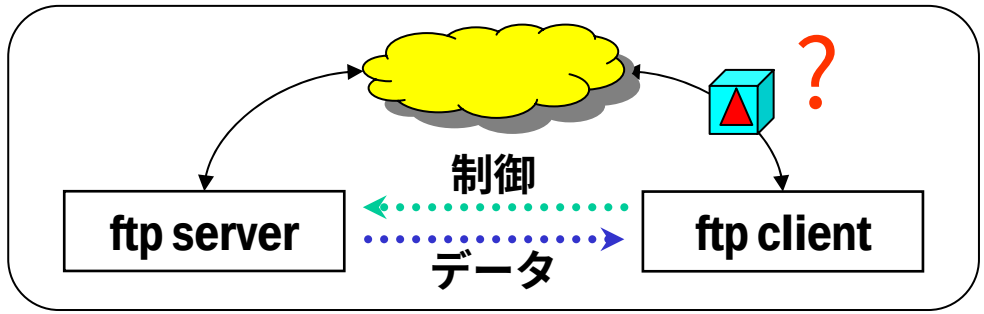
●PPTPのマルチセッション対応

アプリケーション対応の概要#1

①パケット内にIPアドレスやポート番号を記述

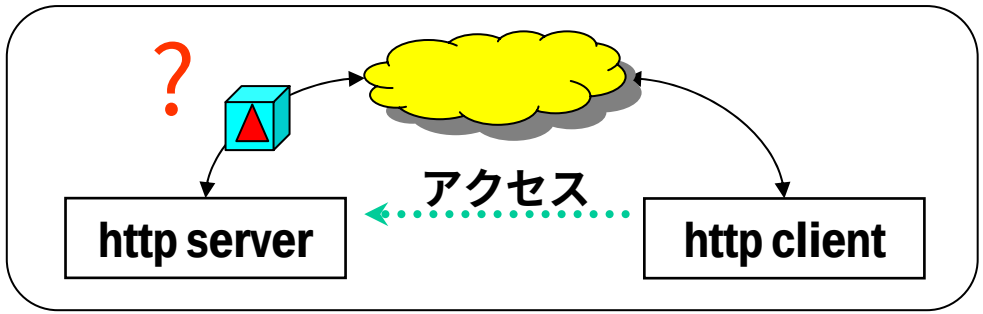


②複数のコネクションが利用される(異なる方向)



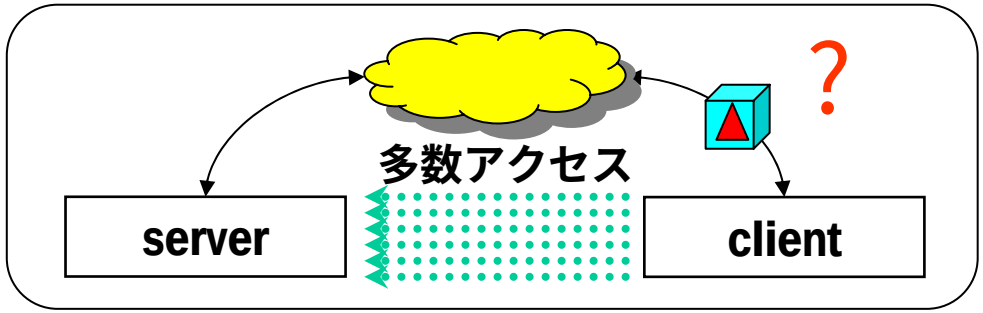
ftpのアクティブ転送(PORTコマンド)

③サーバ公開(サービス公開)

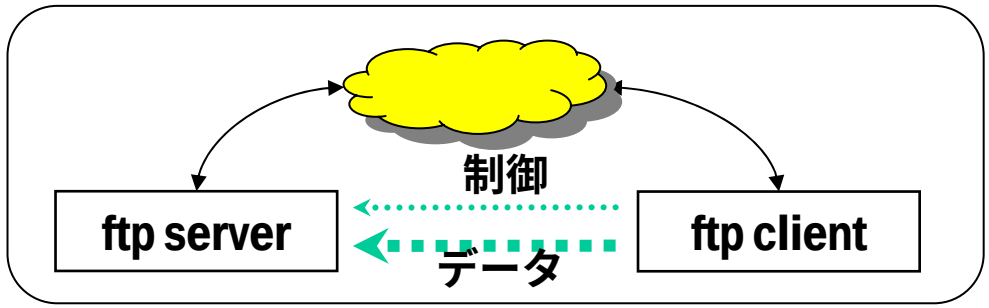


アプリケーション対応の概要#2

④同時多数接続を行うアプリケーション

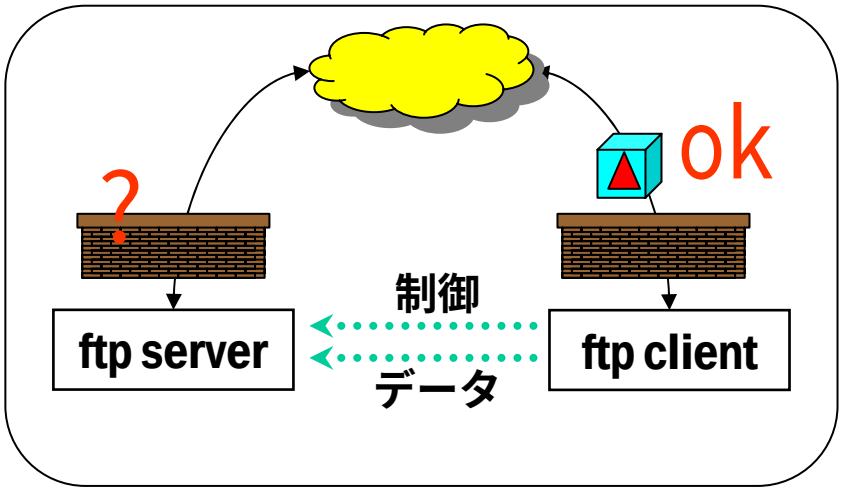


⑤複数のコネクションが利用される
(利用状態が不均一)

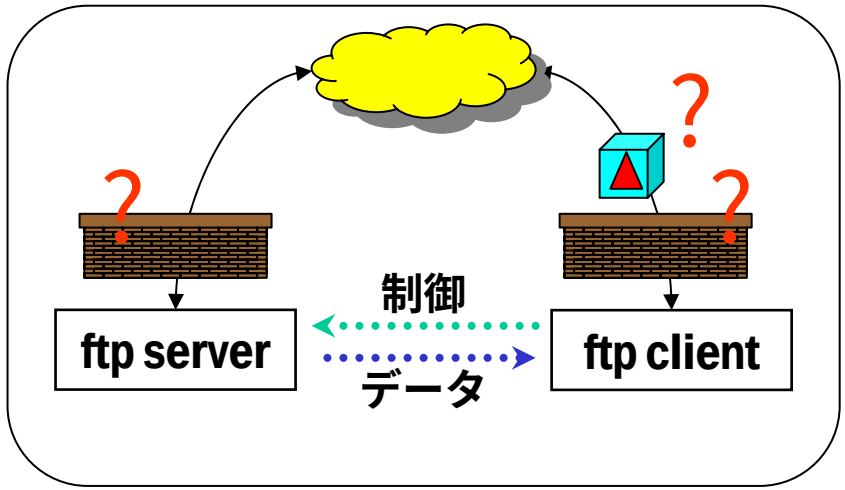


ftpのパッシブ転送(PASVコマンド)

FTP/アプリケーション対応の必要性



ftpのパッシブ転送(PASVコマンド)



ftpのアクティブ転送(PORTコマンド)

[状況]

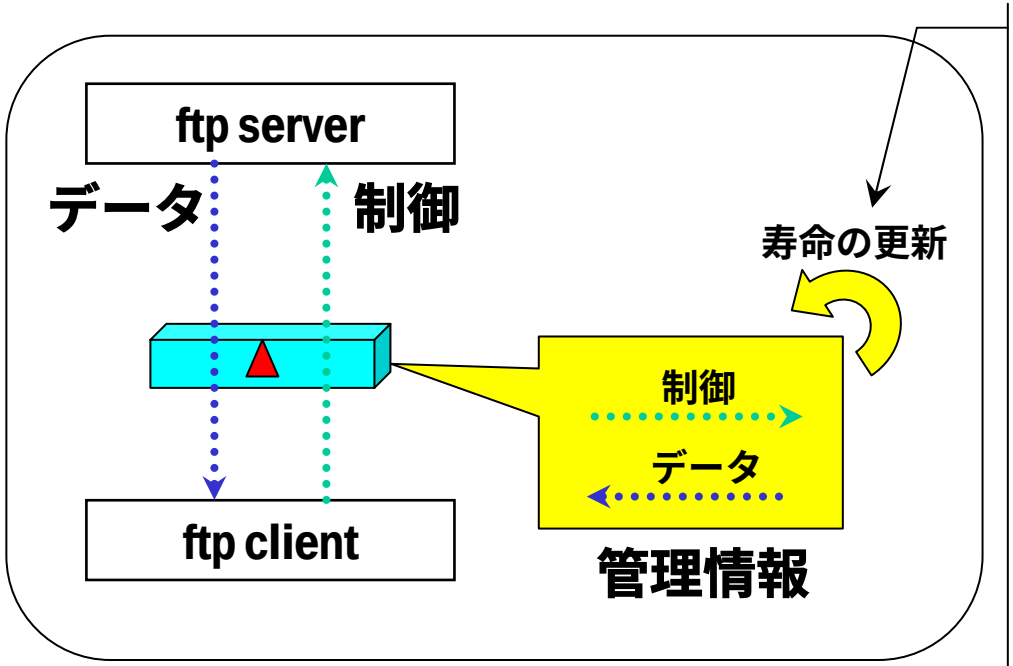
- アプリ/機能を実現するために複数のコネクションが必要
- 双方向通信が必要なのに、片方向の通信環境での運用

[例外処理を必要とする通信]

- FTP,CU-SeeMe,NetMeeting Version 3.0, …

http://www.rtpro.yamaha.co.jp/RT/FAQ/TCPIP/ftp-passive-mode.html

FTPセッション保持機能



(通常の寿命更新)
　一定時間の寿命により管理情報から削除される。(接続が切れる)
(FTPセッション保持機能)
　ftpに連動したtcpの寿命延長

[FTPセッション保持機能の選択]
　FTPセッション保持機能における寿命延長対象の選択
- all … すべてのtcp
- ftp …. ftpの制御チャネルのみ

・大量のファイル転送が行われていると、通信に時間がかかり、制御チャネルのtcpコネクションが管理情報から削除されてしまう。
・ftp通信の制御チャネルを救うため、単純に寿命を長くすると、管理情報が溢れてしまう。

⇒効率的運用ノウハウ
　ftpの制御チャネルをtcpコネクションのみを寿命延長対象とする。

FTPセッション保持機能の管理対象選択
～コマンド仕様～

このコマンドによってIPマスカレードテーブルのTTLの扱いを制御することができる。通常、テーブルのTTLは単調に減少するが、FTPのように制御チャネルとデータチャネルからなるアプリケーションでは、制御チャネルに対応するテーブルをデータ転送中に削除するべきではないため、制御チャネルとデータチャネルの両テーブルのTTLを同期させている。ただし、現有の機能では、制御チャネルとデータチャネルの対応を把握することが難しいため、同じホスト間の通信については、すべてのコネクションを関係づけ、TTLを同期させている。しかしながら、このような動作では、多くのテーブルのTTLが同期し、多くのテーブルが長く残留するという現象が起きる。さらに、状況に よっては、ルータのメモリが枯渇する可能性もある。そこで、この処理をFTPの制御チャネルに限定し、メモリの枯渇を予防する選択肢を提供する。

[入力形式]

```
nat descriptor masquerade ttl hold TYPE
```

[パラメータ]

TYPE ... TTLを同期させる方法
- ‘all’ ... すべてのコネクションを対象とする
- ‘ftp’ ... FTPの制御チャネルのみを対象とする

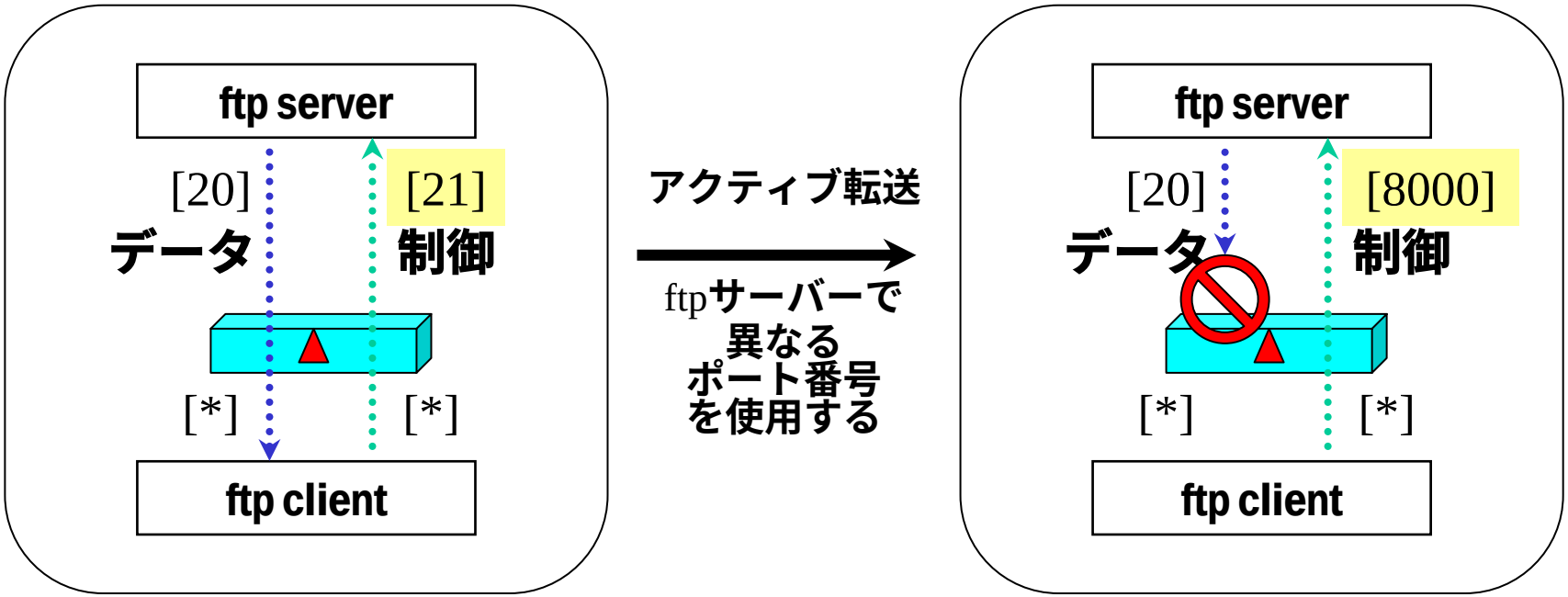
[説明]

TTLの同期をFTPの制御チャネルに限定するときには、パラメータに‘ftp’を設定する。FTPに限定せず、従来と同じように動作させるためには、パラメータに‘all’を設定する。

[デフォルト値]

all

FTP監視ポート指定機能



21番ポートで待ち受け⇒OK

8000番ポートで待ち受け⇒NG

[悩み]

・ftpサーバーの待ち受けポート(LISTEN PORT)を21番以外に指定していると、NAT/IPマスカレードが越えられない。

FTP監視ポート指定機能
～コマンド仕様～

FTPサーバーの待ち受けを「任意のポート番号」でも、FTP通信を適切に行えるようになる。

○NAT/IPマスカレードで、FTPとして認識するポート番号を設定できるようにした。

[入力形式]

```
nat descriptor ftp port DESC PORT [PORT...]
```

[パラメータ]

DESC ... ディスクリプタ番号、1～ 65535

PORT ... ポート番号、1～65535

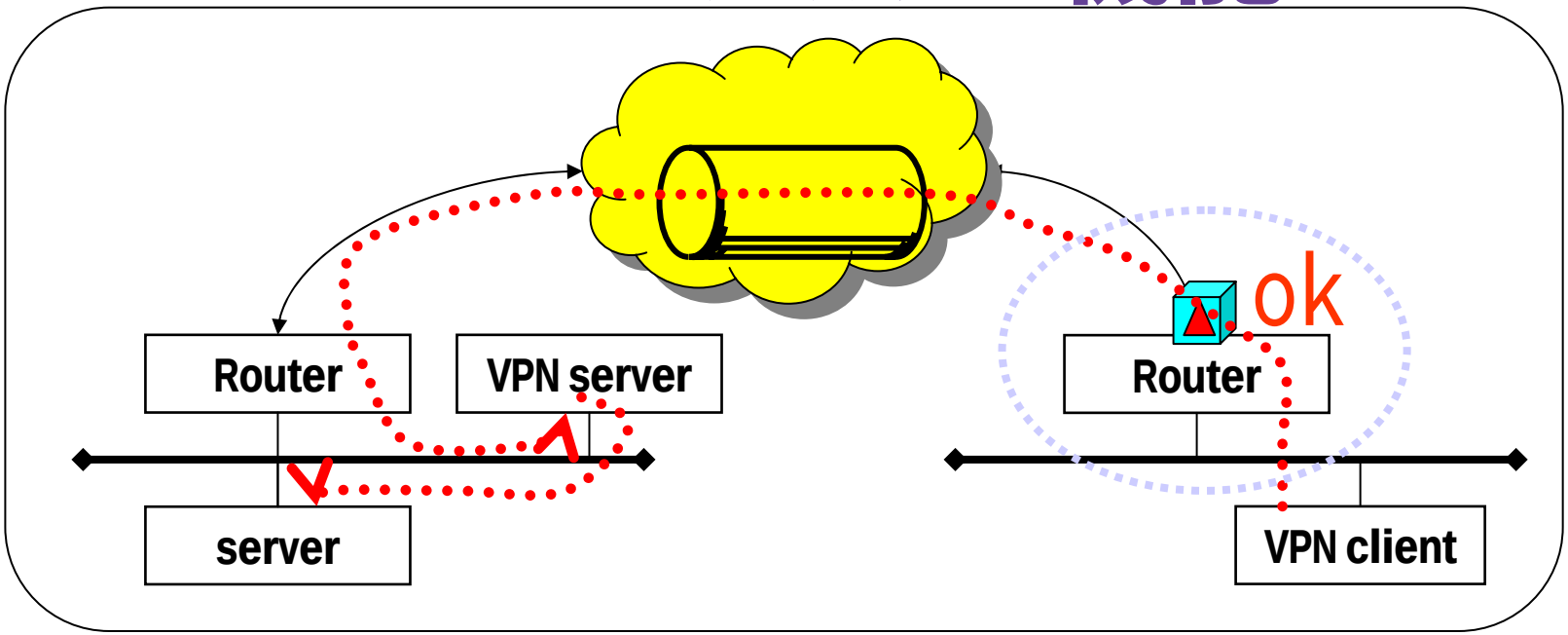
[説明]

TCPで、このコマンドにより設定されたポート番号をFTPの制御チャネルの通信だとみなして処理をする。

[デフォルト]

21

VPNパススルー機能

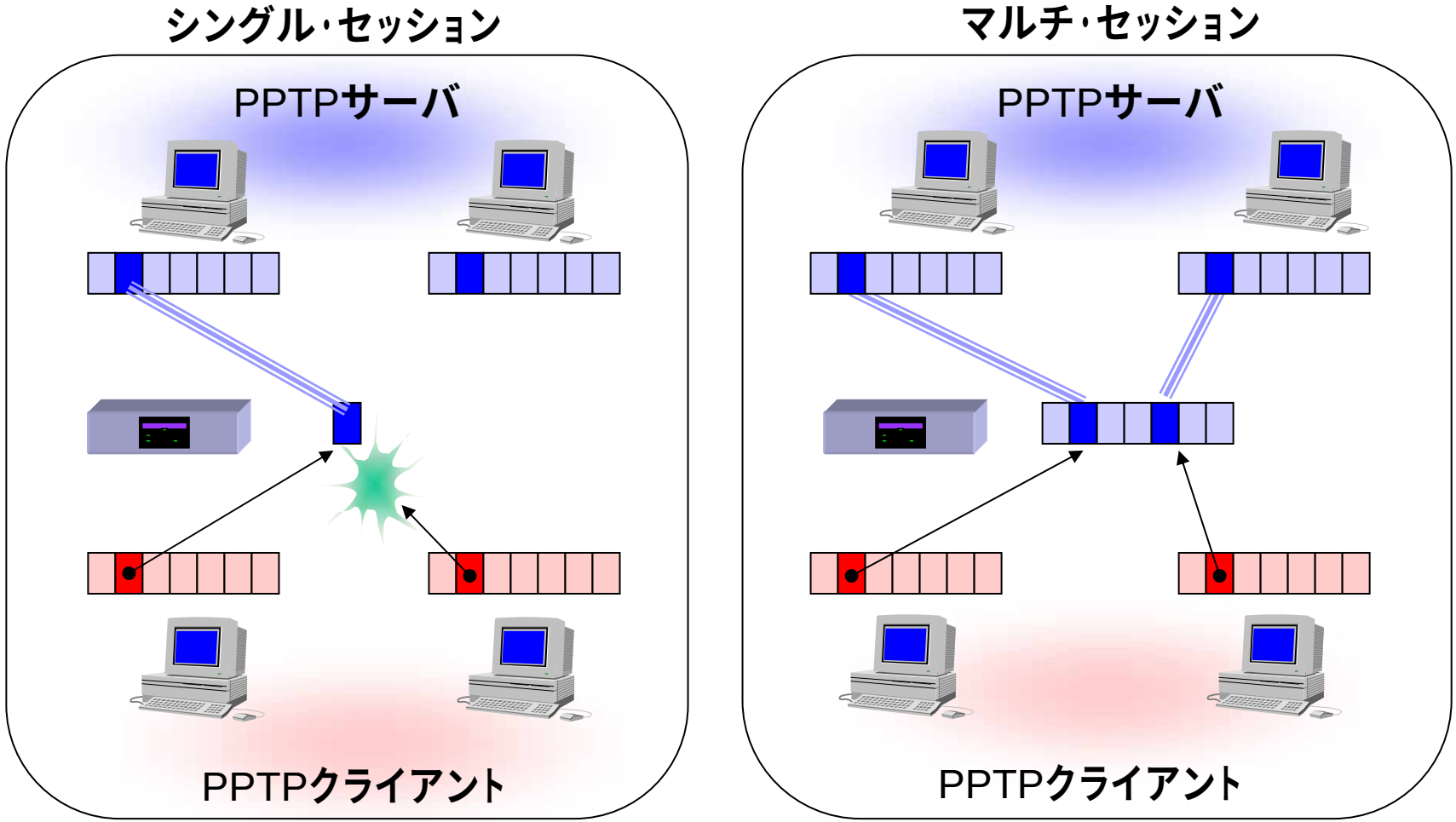


VPNやIPv6トンネルのためにICMP,TCP,UDPとは異なるプロトコルが利用される。これらのプロトコルに対しても、アドレス変換を行う機能。

⇒加えて、Rev.4.00.39より静的IPマスカレードによる固定を可能とした。

VPN種別	変換対象
PPTP	GRE(47) TCP(6),1723
L2TP	UDP(17),1701
IPsec	ESP(50) AH(51)
L2TP over IPsec	ESP(50)

PPTPのマルチセッション対応



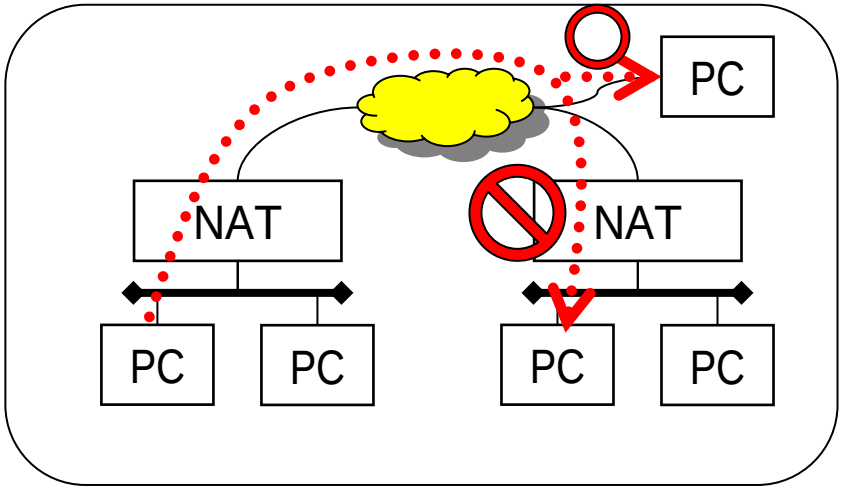
・同時に複数のMicrosoft VPN通信(PPTPによるVPN)が可能となる

PPTPのマルチセッション対応の仕様

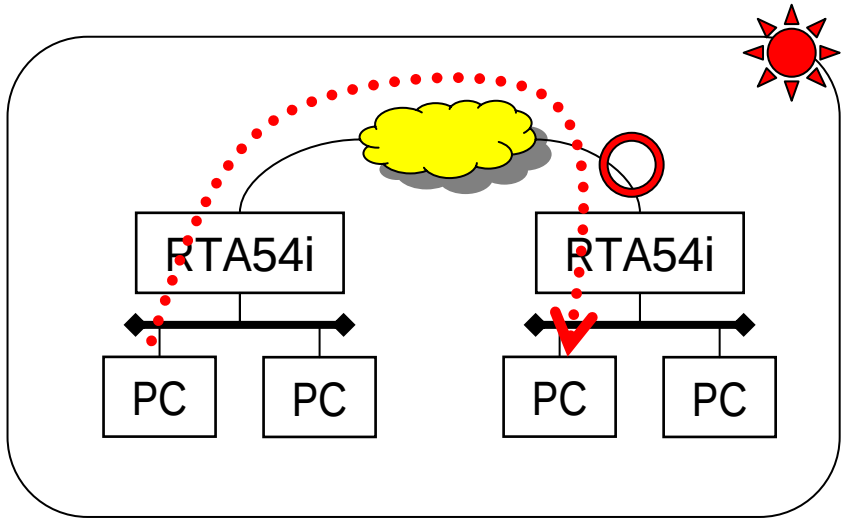
IPマスカレードを動作させている時に、PPTPによるMicrosoft VPNを変換できるようにした。ルータ、Windows PC、Windows サーバのすべてで特別な設定は必要なく、IPマスカレードの内側(プライベートアドレス側)にあるPPTPクライアントである Windows PCから外側(グローバルアドレス側)にあるPPTP サーバであるWindows サーバとの間にPPTPによるVPNトンネルを通常の動作で設定できる。

同時に扱えるPPTPセッションの数に特に制限は設けていない。RTがIPマスカレードで扱える同時セッション数(最大4096)に制限を受ける。PPTPでは制御用と通信用で最低でも2つのセッションを必要とすることに注意。

NetMeeting Version 3.0対応



DMZホスト機能によるNetMeeting対応



NetMeetingの本格対応

- NetMeetingは、ブロードバンド時代のアプリケーション
  ビデオ会議、ホワイトボード、チャット、ファイル転送、
  プログラム共有、リモートデスクトップ共有
- 対応内容の違い
  DMZホスト機能による対応では、NATを使用していない通信相手に限られる。
  本格対応でNAT(IPマスカレード)越しでも通信可能

NetMeeting Version 3.0対応の仕様

NATでNetMeetingに対応する処理を追加した。動作を確認している条件は 以下のとおりであるが、この条件を満たすときでも、ビデオや音声の片通 話などの問題が発生する可能性がある。なお、このような場合に、DMZホスト機能でNetMeetingを実施する端末を設定すると解決できることがある。

- NetMeeting Version 3.0
- ビデオ、音声、チャット、ホワイトボードの動作を確認済み
- ディレクトリサービスに対応しない
- 複数の端末がNATの外側へ同時に接続することはできない
- NATの外側から内側の端末へ接続するためには、下記のような静的 IPマスカレードの設定が必要

(例) NATの内側の端末のIPアドレスが192.168.0.2の場合

```
nat descriptor masquerade static 1 1 192.168.0.2 tcp 1720
nat descriptor masquerade static 1 2 192.168.0.2 tcp 1503
```

NetMeeting機能の対応表

NetMeeting 3.0 機能	説明
オーディオ会議	○ (確認済み)
ビデオ会議	○ (確認済み)
ホワイトボード	○ (確認済み)
チャット	○ (確認済み)
ファイル転送	○ (確認済み)
プログラムの共有	○ (確認済み)
リモート デスクトップ共有	× (未確認)

http://www.microsoft.com/japan/windows/netmeeting/

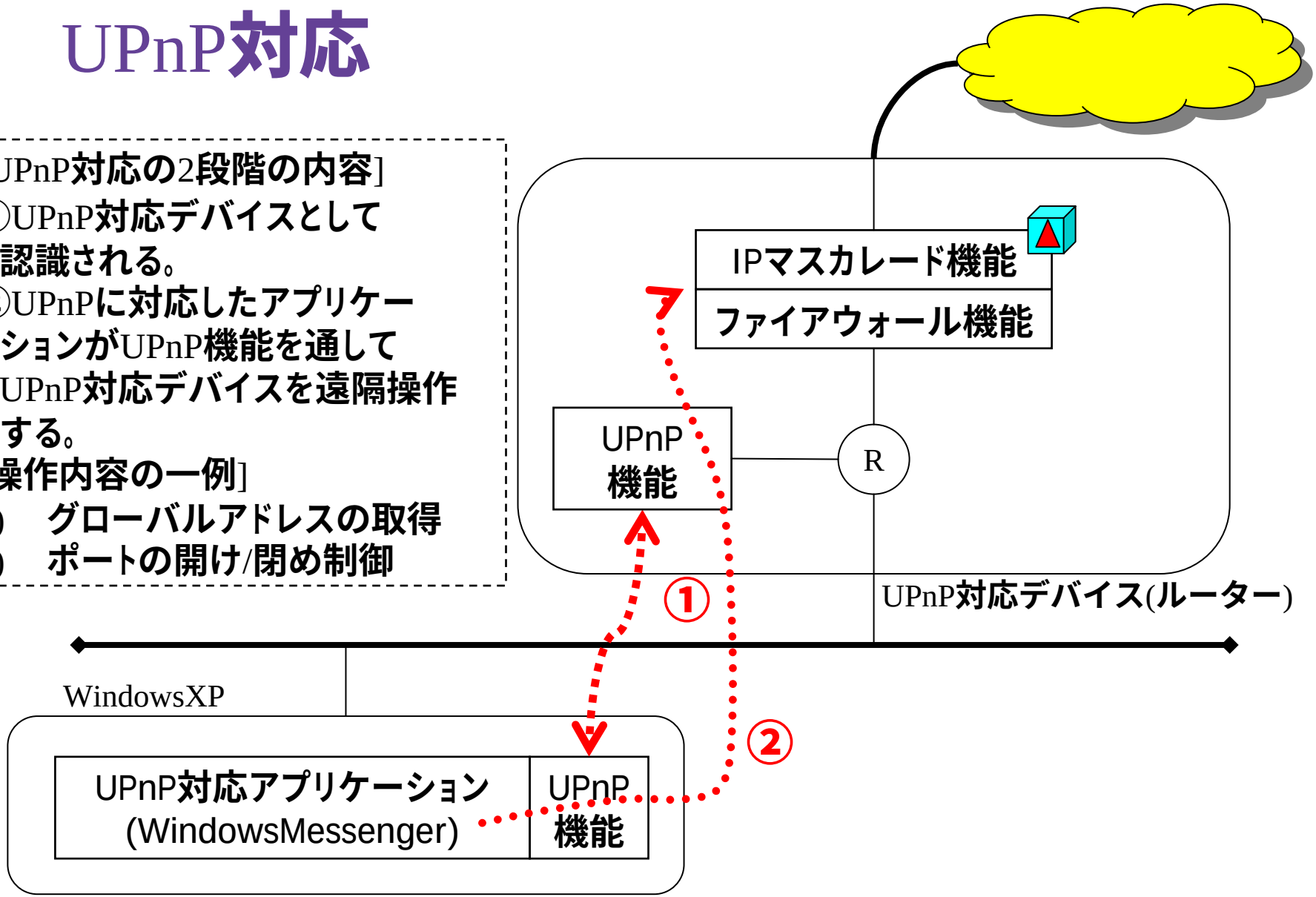
UPnP対応とWindowsMessenger

1) UPnP対応
2) WindowsMessenger対応
   ・NAT越え方法 (その1～その3)
3) 対応内容

http://www.rtpro.yamaha.co.jp/RT/FAQ/UPnP/index.html
http://www.rtpro.yamaha.co.jp/RT/FAQ/Messenger/index.html

UPnP対応

[UPnP対応の2段階の内容]
①UPnP対応デバイスとして認識される。
②UPnPに対応したアプリケーションがUPnP機能を通してUPnP対応デバイスを遠隔操作する。
[操作内容の一例]
1) グローバルアドレスの取得
2) ポートの開け/閉め制御

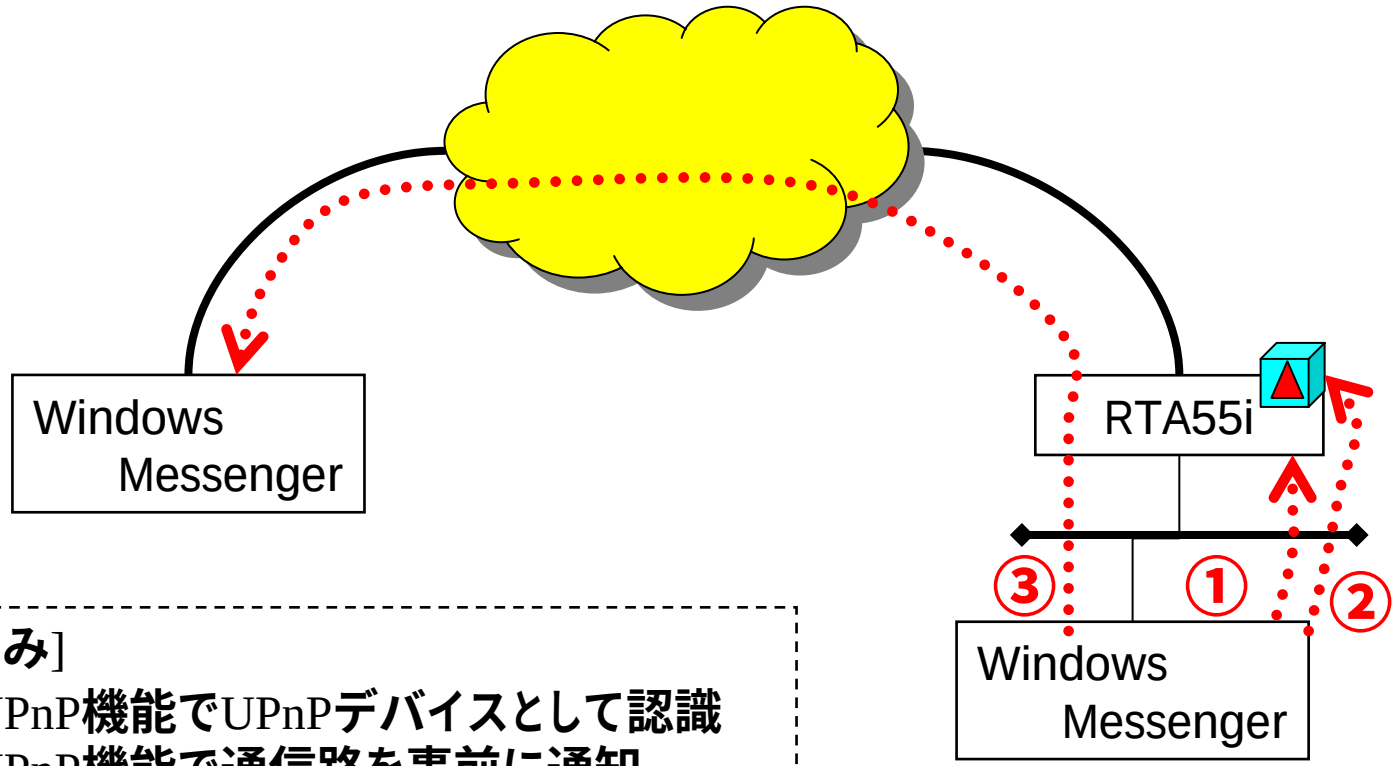


Windows Messenger対応とは？

[やりたいこと]
・IPマスカレード利用環境でWindowsMessengerの
　機能を確実に使いたい。
[手段]
1) UPnP機能による対応
2) WindowsMessenger V4.6のNAT Traversal機能
　＋　DMZホスト機能
3) IPマスカレードでSIPのアドレス書換えによる対応

http://messenger.microsoft.com/ja/

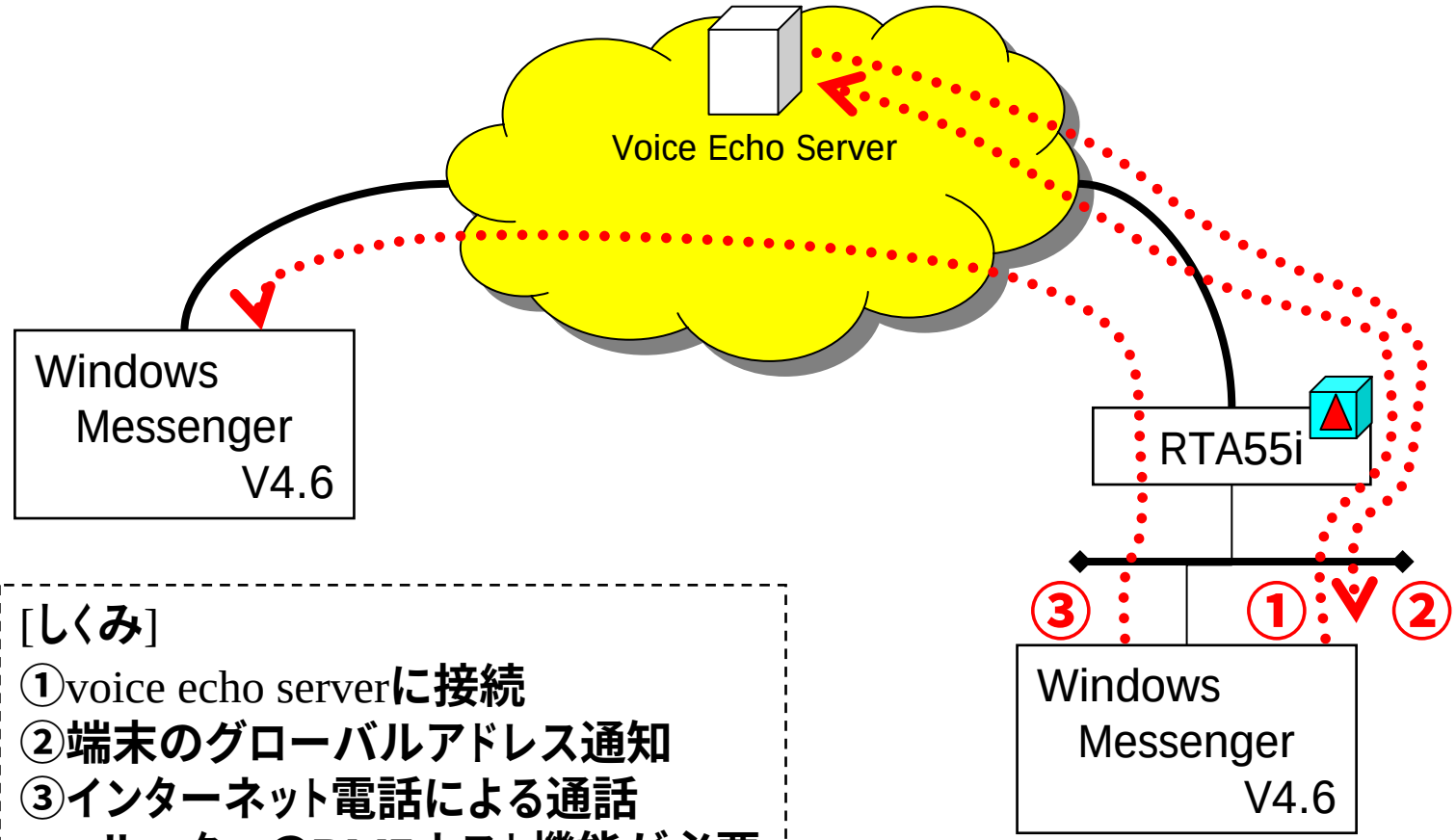
Windows MessengerのNAT越え#1
(UPnP機能対応)



[しくみ]
①UPnP機能でUPnPデバイスとして認識
②UPnP機能で通信路を事前に通知
→ルーターが通信路の開閉
③インターネット電話による通話

http://messenger.microsoft.com/ja/

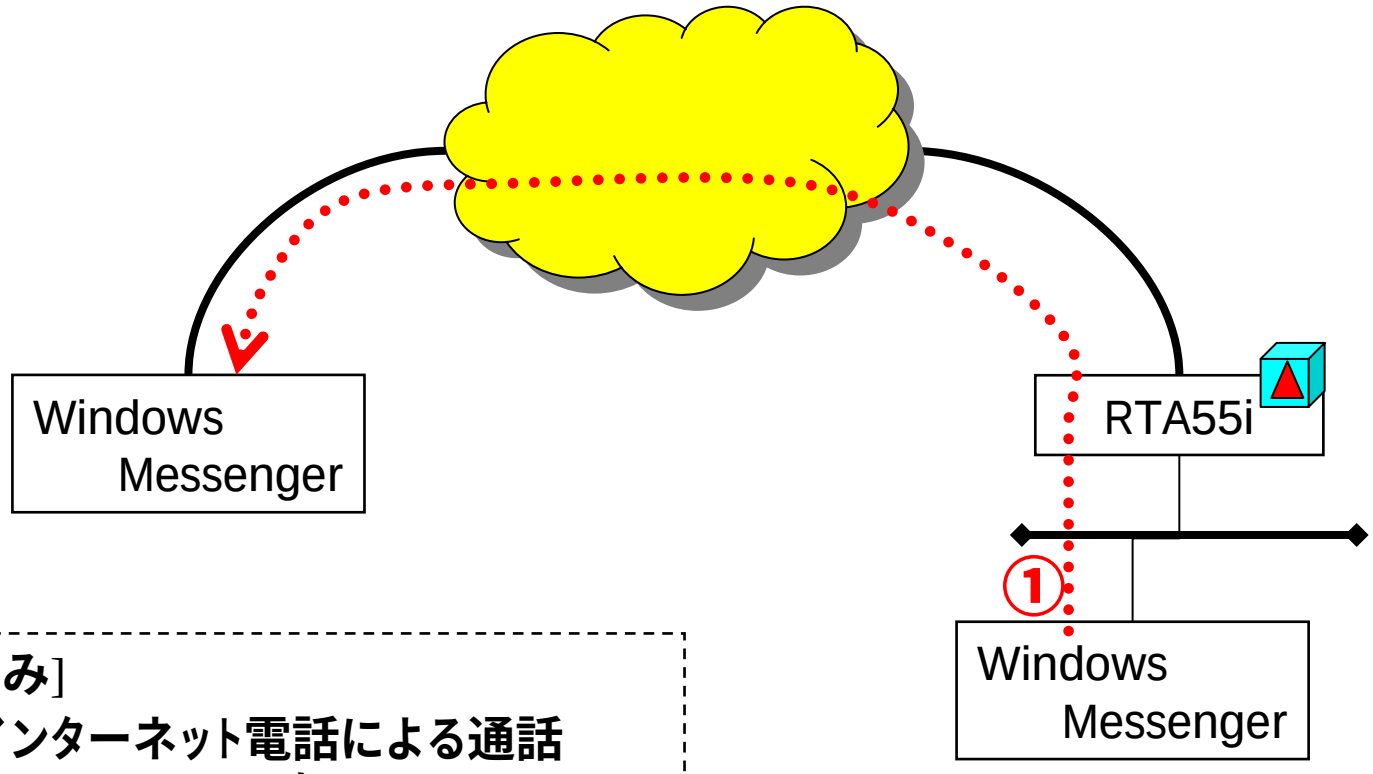
Windows MessengerのNAT越え#2
(Windows MessengerのNAT Traversal機能)



[しくみ]
①voice echo serverに接続
②端末のグローバルアドレス通知
③インターネット電話による通話
→ルーターのDMZホスト機能が必要

http://messenger.microsoft.com/ja/

Windows MessengerのNAT越え#3
(IPマスカレードでSIPのアドレス書換え)



[しくみ]
①インターネット電話による通話
→IPマスカレード処理でSIPで
記述されているアドレス情報の
書換え

http://messenger.microsoft.com/ja/

Windows/MSN Messengerの機能概要

機能名	アドレス変換の影響		UPnP対応
	Windows Messenger	MSN Messenger	
インスタントメッセージ	なし	影響なし	ー
音声チャット	あり(SIP)	あり(SIP)	○
ビデオチャット	あり(SIP)	ー	○
ファイル送信	あり(独自)	あり(独自)	×
電話をかける	あり(SIP)	あり(SIP)	×
リモートアシスタンス	あり(RDP)	ー	○
アプリケーションの共有	あり(SIP)	ー	○
ホワイトボード	あり(SIP)	ー	○

※UPnP非対応機能も、(リモートアシスタンスのように)、将来、UPnP対応される可能性があります。

http://messenger.microsoft.com/ja/

Windows Messenger機能の対応表

WindowsMessenger	説明
インスタントメッセージ	○ (非UPnP)
音声チャット	○ (UPnPアプリ)
ファイル送信	○ (非UPnP、独自対応)
電話をかける	○ (非UPnP、独自対応)
ビデオチャット	○ (UPnP)
ホワイトボード	○ (UPnP)
アプリケーションの共有	○ (UPnP)
リモートアシスタンス	○ (UPnP、WindowsUpdateが必要)

http://messenger.microsoft.com/ja/

ＭＳＮ Messenger機能の対応表

MSN Messenger (3.0以上)	説明
インスタントメッセージ	○ (非UPnP)
音声チャット	○ (4.6以上、UPnP)
ファイル送信	○ (非UPnP、独自対応)
電話をかける	○ (非UPnP、独自対応)

http://messenger.microsoft.com/ja/

(参考) Windows XP機能の対応表

Windows XP	説明
リモートデスクトップ	○ (非UPnP)

[注意事項]

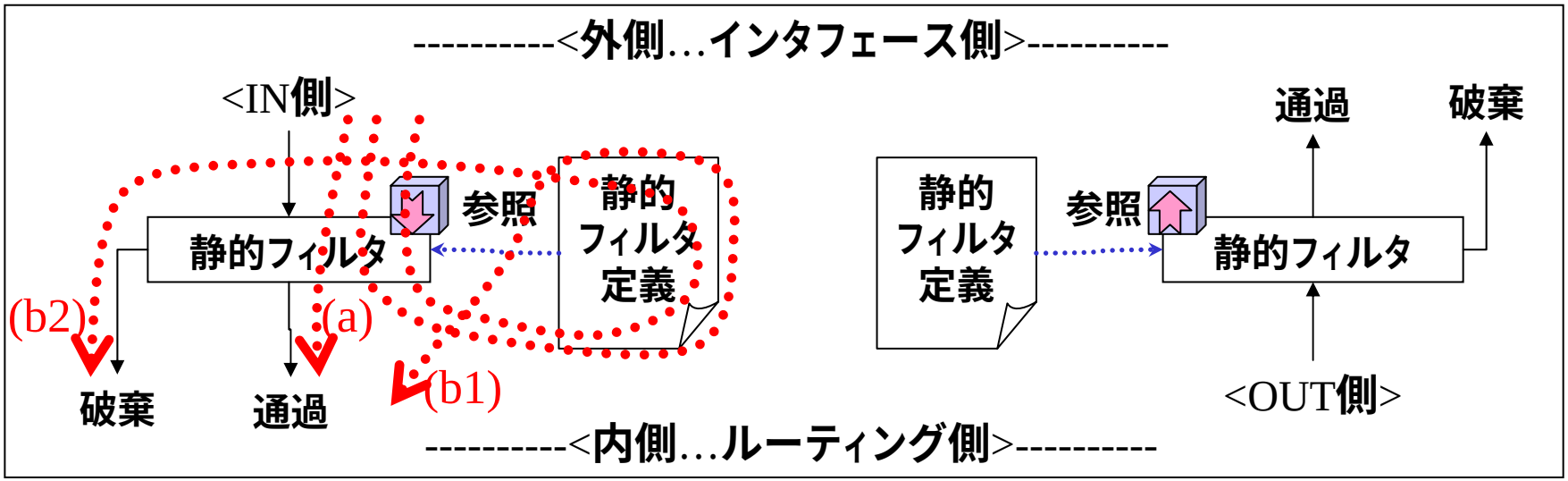
・Windows XPのリモートデスクトップを利用する場合には、静的IPマスカレードで「TCPの3389番ポート」を通すように設定する必要があります。

http://www.microsoft.com/japan/windowsxp/pro/business/remote/remotedesktop.asp

フィルタリング

- **静的フィルタリング**
  - **危険なポートを閉じるフィルタ**
  - **静的セキュリティ・フィルタ**
    established、ftp、**電子メール**、UDP
- **動的フィルタリング**
- **ネットボランチのセキュリティ・レベル**
- **ファイアウォールの構造とセキュリティ・フィルタ**
  - **一部の通信路を塞ぐ**
  - **静的セキュリティ・フィルタ**
    (セキュリティ・レベル5)
  - **動的セキュリティ・フィルタ**
    (セキュリティ・レベル7)
- **不正アクセス検知**

静的フィルタリング



[静的フィルタの処理]

a) フィルタに何か適用されていない状態では、すべて通過する。

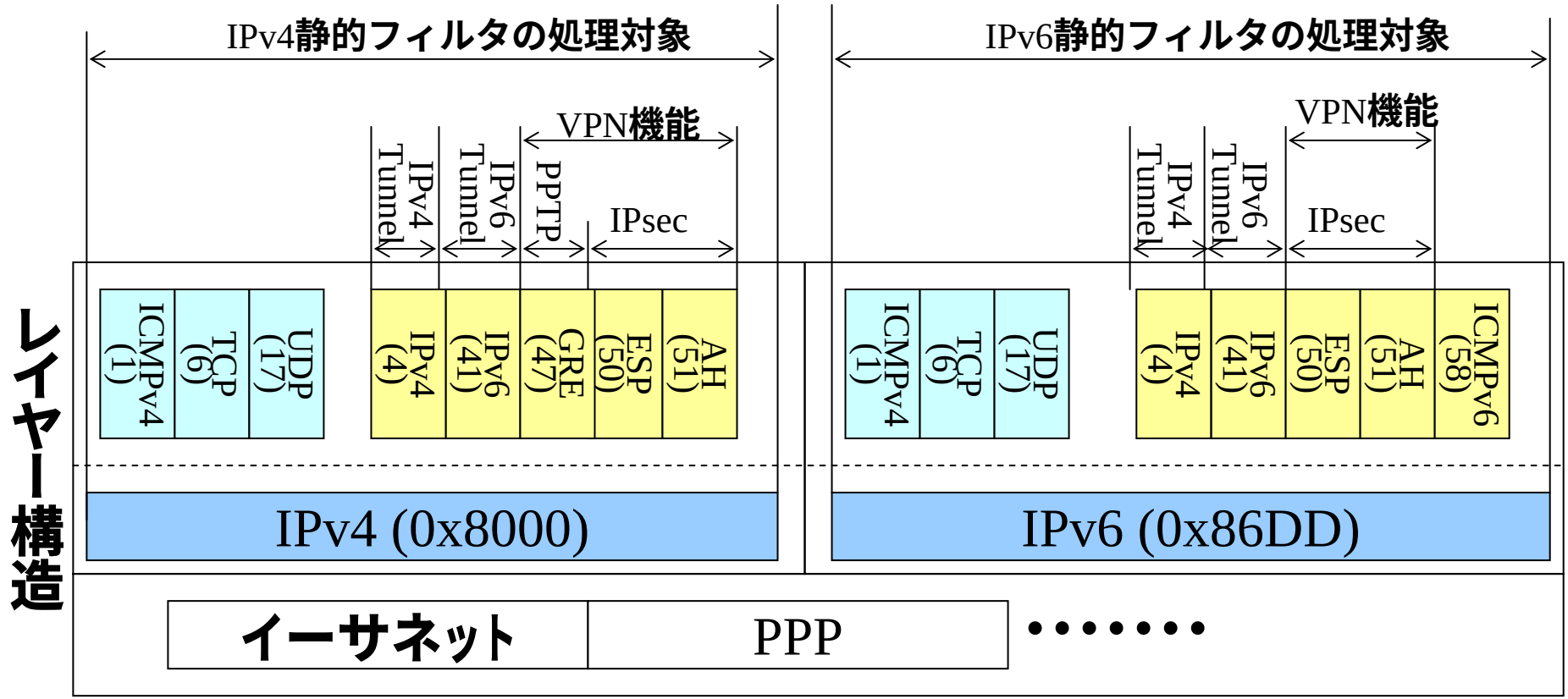
b) フィルタに何か適用されている場合、パケット単位で、

b1) 適用順にパターンマッチングを行い破棄と通過を判別する。

b2) すべてのパターンにマッチングしなければ、破棄される。

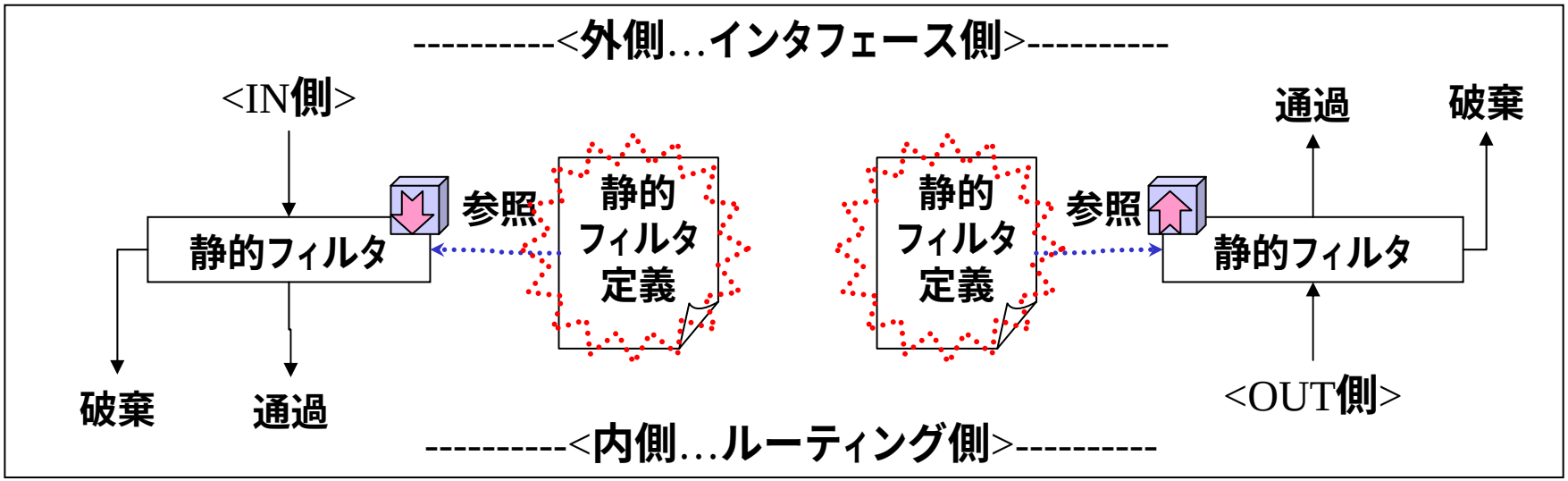
静的フィルタリングの処理対象

VPNやIPv6トンネルのためにICMP,TCP,UDPとは異なるプロトコルが利用される。ファイアウォールでも、これらのプロトコルに対するしてフィルタリング処理が行われる。



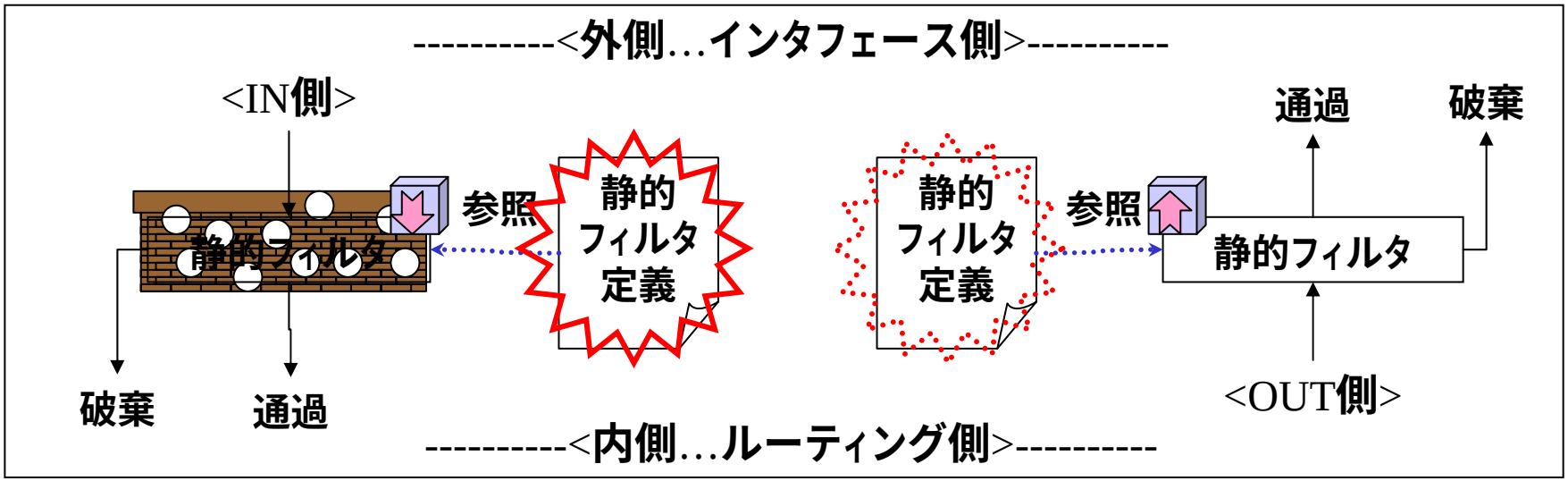
http://www.iana.org/assignments/protocol-numbers
http://www.iana.org/assignments/port-numbers

危険なポートを閉じるフィルタ



[ポリシー]
・基本的に全開。危険なポートだけ閉じる。
[危険なポートの例]
・UNIX,Windows,MachintoshなどのOSで使用している通信
　⇒WindowsのNetBIOSなど (ポート135,137～139,…)
[悩み]
・危険と認知していない通信/攻撃への対処ができない。(予防できない)

静的セキュリティ・フィルタ



[ポリシー]
・基本的に全閉。使用する通信だけを通す。
[使用する通信]
・TCPは、establishedで確保される通信。
・UDPは必要最低限。
[悩み]
・「establishedフィルタで対処できないこと」、「ftpのアクティブ転送」、
「常に開けておくUDP」など

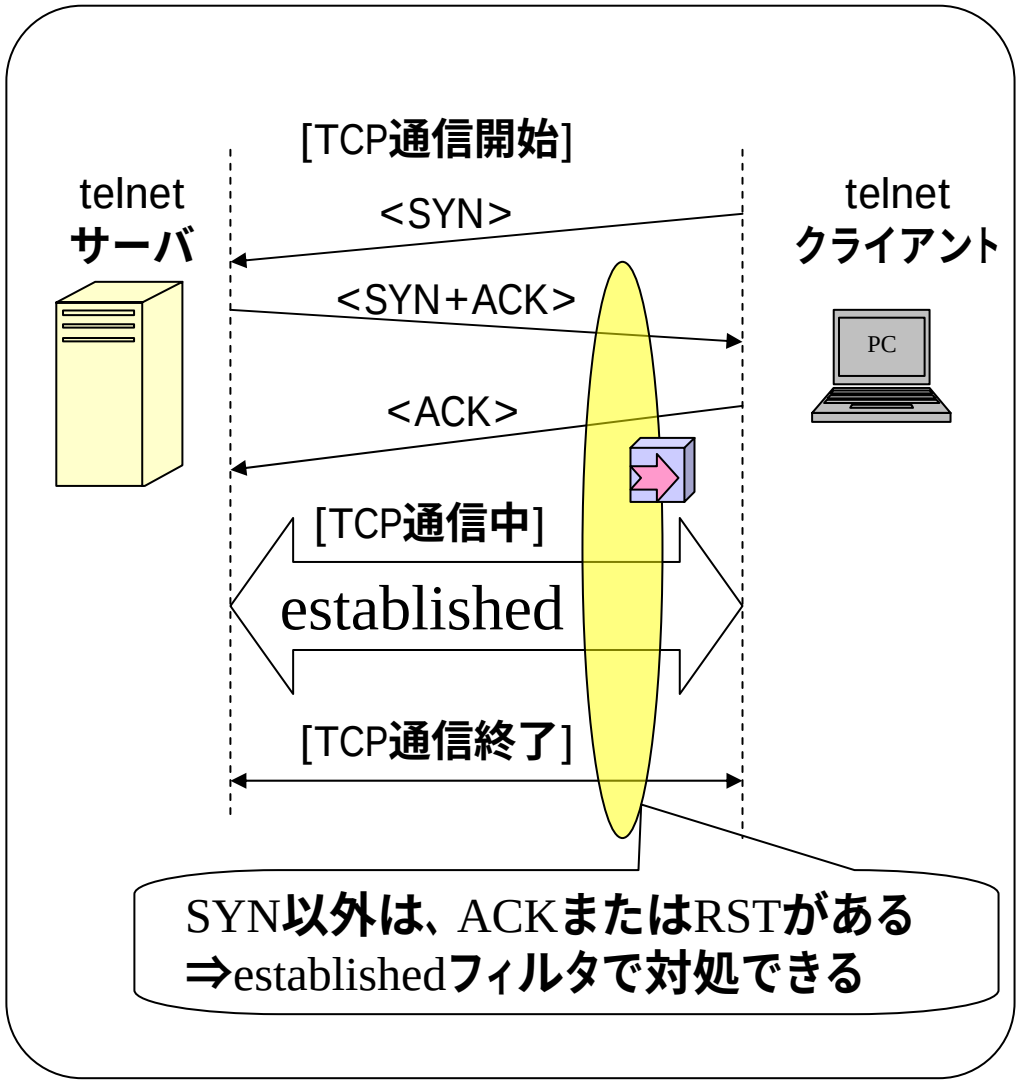
http://www.rtpro.yamaha.co.jp/RT/FAQ/IP-Filter/network-security-filter.html

静的セキュリティ・フィルタの設定例

```
# フィルタ定義例（LAN側ネットワークが192.168.0.0/24の場合）
ip filter 10 reject 192.168.0.0/24 * * * *
ip filter 11 pass * 192.168.0.0/24 icmp * *
ip filter 12 pass * 192.168.0.0/24 established * *
#                                  tcpの片方向性を実現する仕組み
ip filter 13 pass * 192.168.0.0/24 tcp * ident
#                                  メール転送などの時の認証(ident)
ip filter 14 pass * 192.168.0.0/24 tcp ftpdata *
#                                  ftpのアクティブ転送用
ip filter 15 pass * 192.168.0.0/24 udp domain *
#                                  DNSサーバへの問い合わせ(戻り)
ip filter source-route on
ip filter directed-broadcast on
# フィルタ適用例（接続先のPP番号が1の場合）
pp select 1
ip pp secure filter in 10 11 12 13 14 15
```


http://www.rtpro.yamaha.co.jp/RT/FAQ/IP-Filter/network-security-filter.html

TCPのestablishedフィルタ



[目的]
- 静的フィルタリングにより外部からの不必要なTCP接続要求を破棄する。

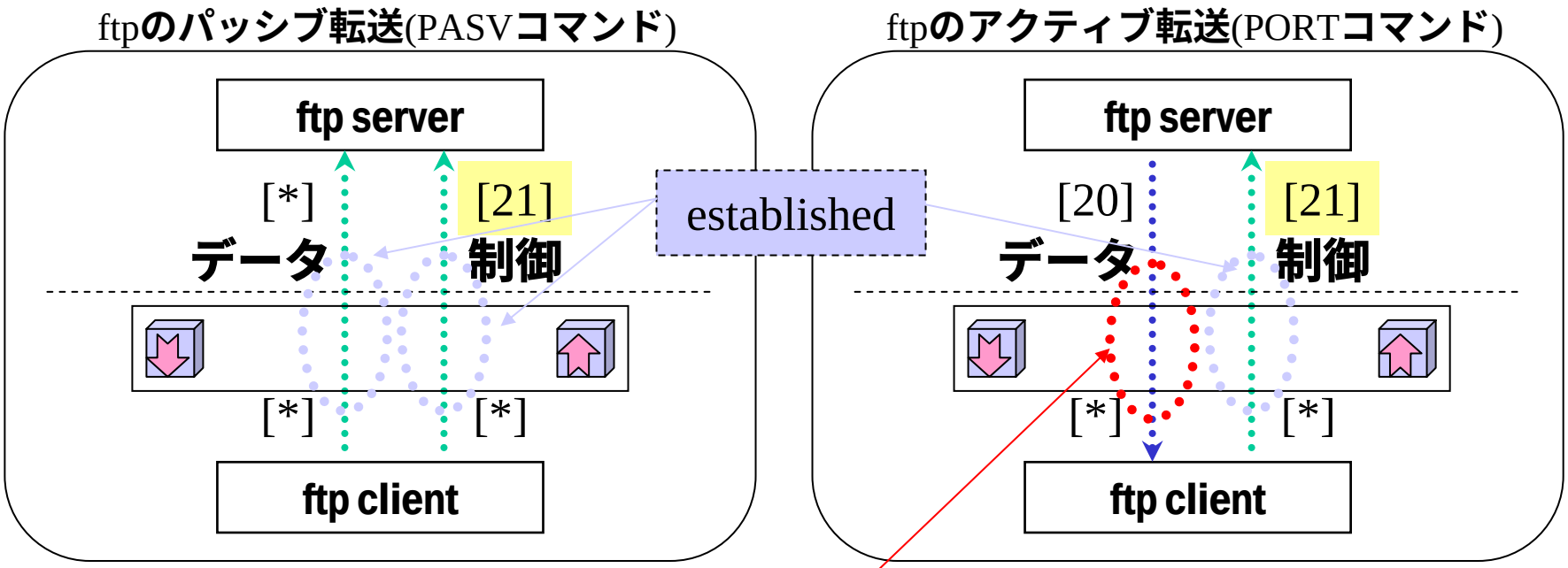
[従来措置]
- 入り口で「SYNのみパケット」を破棄
  ⇒establishedフィルタを適用

[悩み]
- 「ACKつきパケット」の攻撃をされたら…

[解決策]
- 動的フィルタリング
- 利便性とセキュリティのトレードオフ

http://www.rtpro.yamaha.co.jp/RT/FAQ/IP-Filter/ip-filter-established.html

ftp通信のフィルタリング



[悩み]

・ftpのアクティブ転送は、外部からのtcp接続が開始される。
　⇒通常であれば、establishedフィルタで破棄される対象。

・ftpクライアント側は、establishedフィルタでは、十分とはいえない。

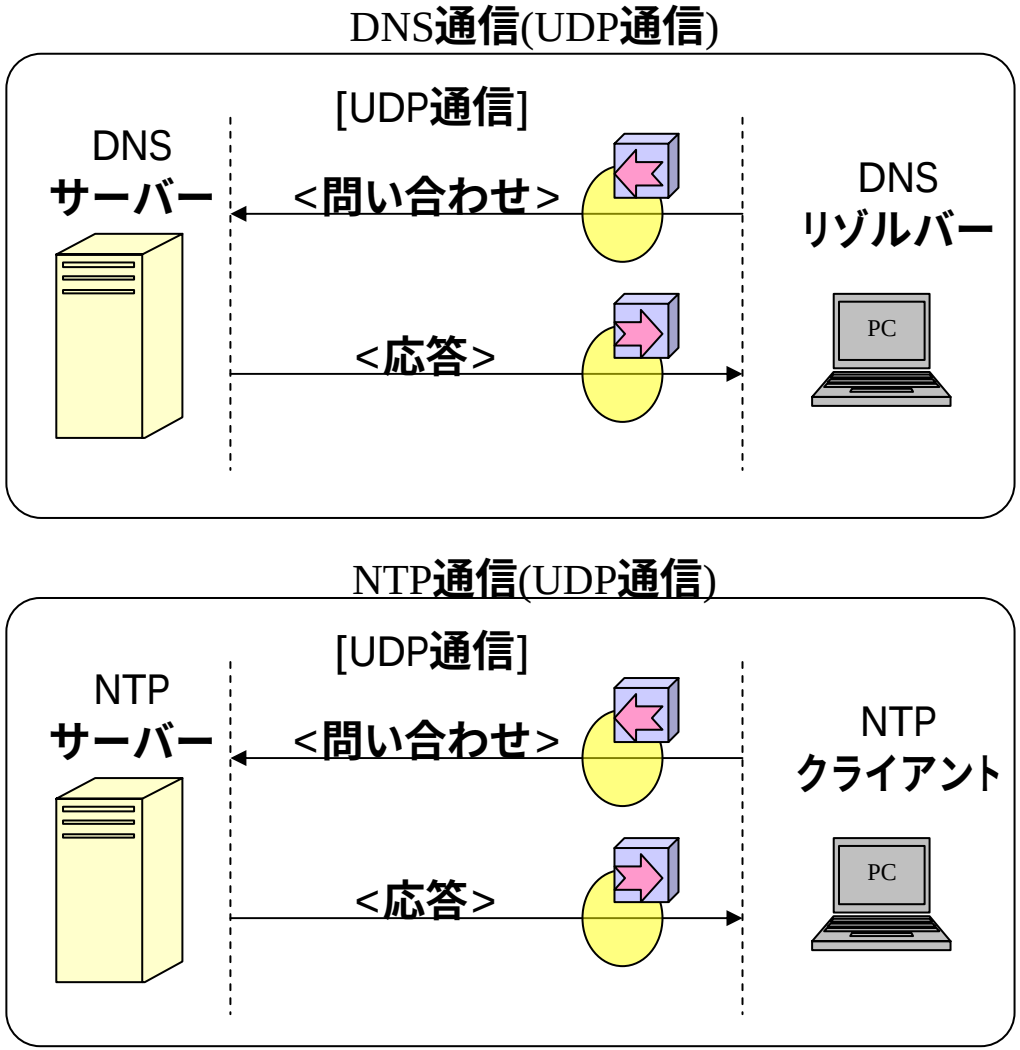
[解決策]

・動的フィルタリング

・利便性とセキュリティのトレードオフ

http://www.rtpro.yamaha.co.jp/RT/FAQ/IP-Filter/ip-filter-established.html

UDPフィルタ(DNSやNTP)



[悩み]

・UDPは、シンプルな通信であるため、チェック機能がほとんど無い。

・UDP通信を許可するためには、応答パケットを常に通過させる必要がある。

[解決案]

・動的フィルタリング

・利便性とセキュリティのトレードオフ

・セキュリティ的に強固な代理サーバを用意する

静的フィルタのタイプ

項目	説明
フィルタ番号	フィルタ定義のための識別番号
フィルタタイプ	pass/reject/restrict、および、ログの有無
始点アドレス	始点となるIPアドレス(ネットワーク指定可)
終点アドレス	終点となるIPアドレス(ネットワーク指定可)
プロトコル	ICMP/TCP/UDPなどのプロトコル指定 ・ICMP専用:icmp-info,icmp-error ・TCP専用:established,tcpfin,tcprst,tcpflag
始点ポート	始点となるポート番号(TCPとUDPのみ有効)
終点ポート	終点となるポート番号(TCPとUDPのみ有効)

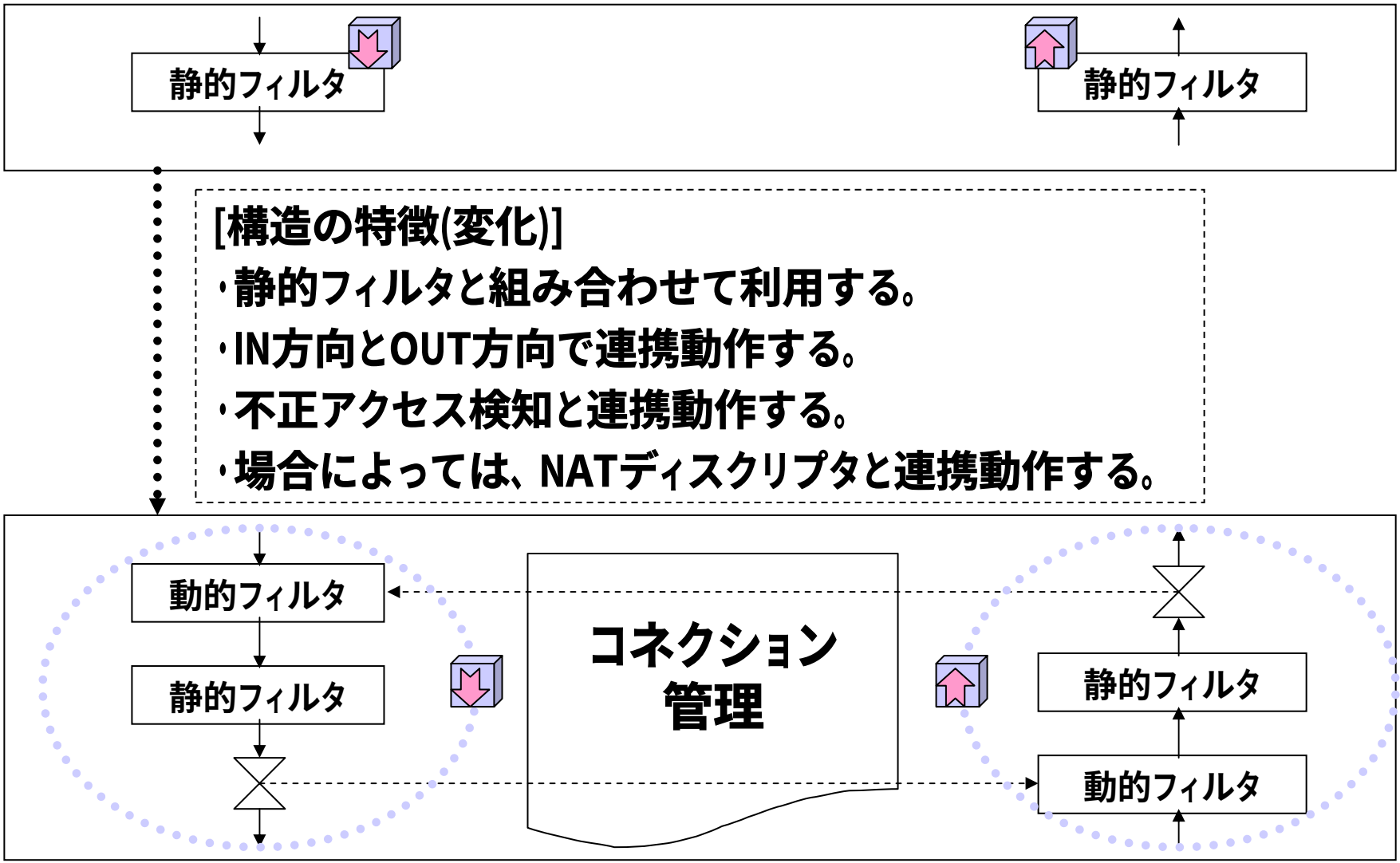
http://www.rtpro.yamaha.co.jp/RT/FAQ/IP-Filter/ip-packet-filter.html

動的フィルタリングの特徴

[目的]
・安全性を確保したフィルタリング設定の難しさの解消
・静的フィルタリングの弱点を補完し、利便性とセキュリティを
両立するしくみの提供
・動的フィルタリングを加えることにより、さらに安全性を高める。

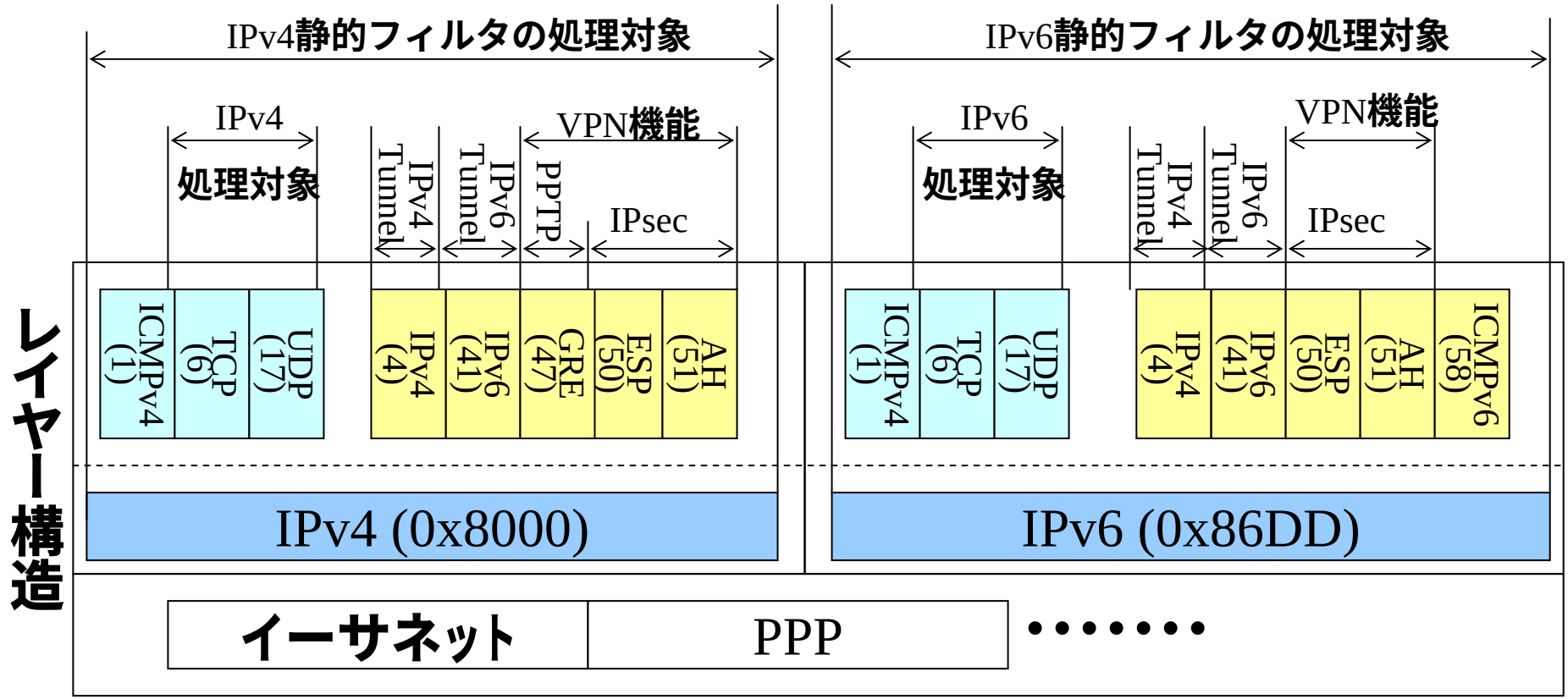
[静的フィルタリングの弱点]
・安全性と安定性を確保した十分なフィルタリングを行うためには、
高度な知識が求められる。
・ftp通信のフィルタリングにおける安全性
・UDP通信のためのフィルタの安全性
・TCP通信のためのestablishedフィルタの安全性

動的フィルタリング構造の特徴



動的フィルタリングの処理対象

動的フィルタリングでは、TCPとUDPを対象としたフィルタリング処理が行われる。加えて、アプリケーションに固有の制御や通信のしくみを考慮したフィルタリングを行うことができる。

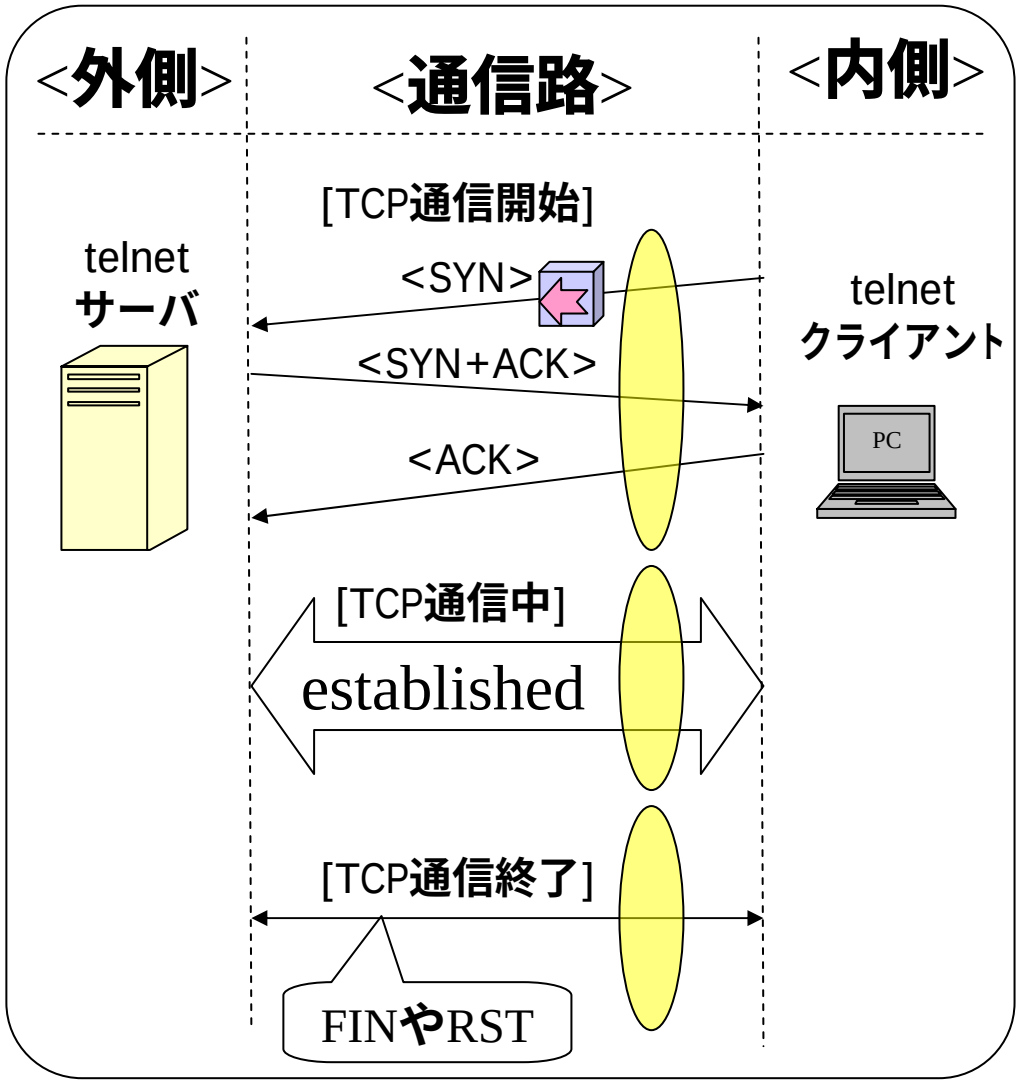


http://www.iana.org/assignments/protocol-numbers
http://www.iana.org/assignments/port-numbers

動的フィルタのアプリケーション名

名称	プロトコル	説明
tcp	tcp	一般的なtcp通信 (コネクションの確立など)
udp	udp	一般的なudp通信(タイマーによる監視など)
ftp	tcp	ftp通信
tftp	udp	tftp通信
domain	udp(tcp)	DNS通信
www	tcp	www通信
smtp	tcp	電子メール(送信)
pop3	tcp	電子メール(受信)
telnet	tcp	telnet通信
netmeeting	tcp,udp	NetMeeting 3.0の通信
自由定義	tcp,udp	トリガー監視、順方向、逆方向を自由定義

TCPの動的フィルタ (基本動作)

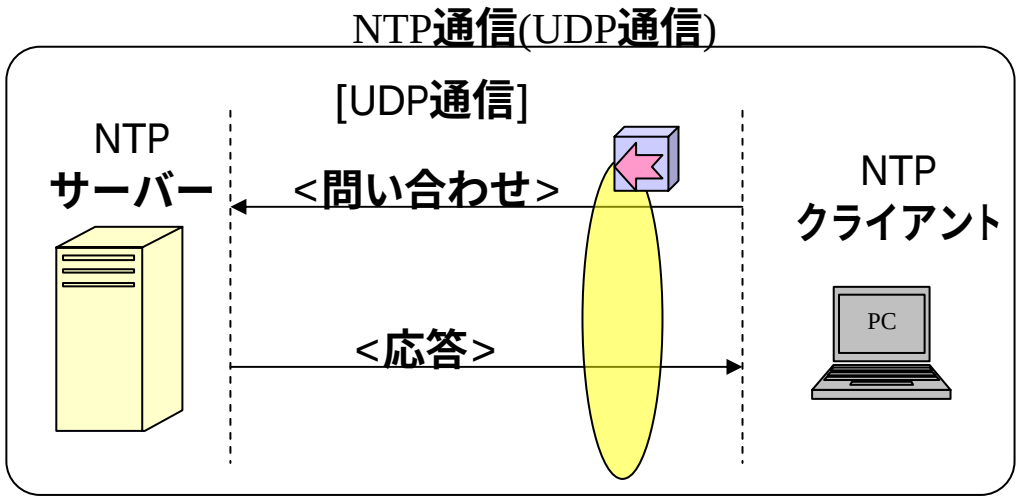


[開くトリガー]
- コネクションを開くSYN情報を持ったパケット

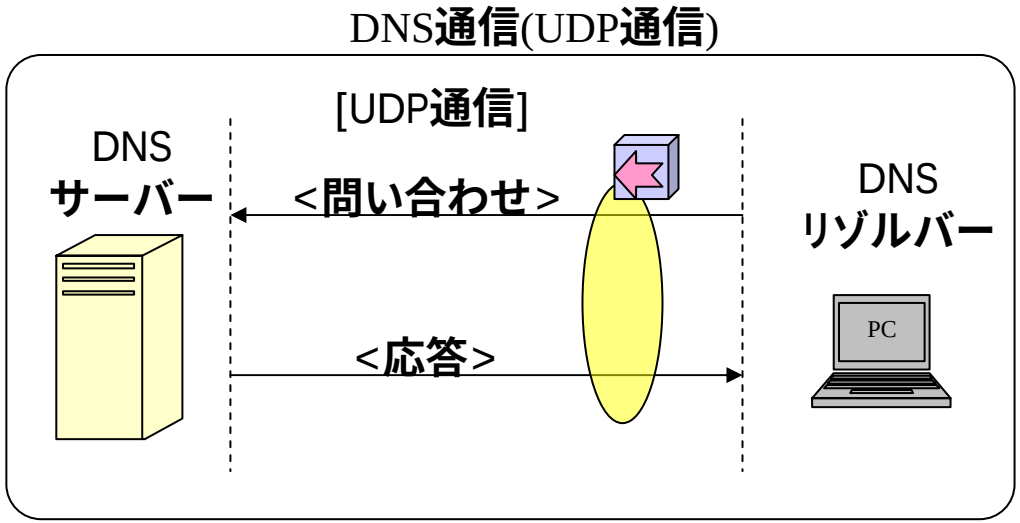
[確立の監視]
- TCPコネクションを開始するハンドシェイクの監視

[閉じるトリガー]
- コネクションを閉じるFINやRSTなどの情報を持ったパケット
- 無通信監視(タイマ)

UDPの動的フィルタ (基本動作)



[開くトリガー]
・該当パケット
[閉じるトリガー]
・タイマーの満了



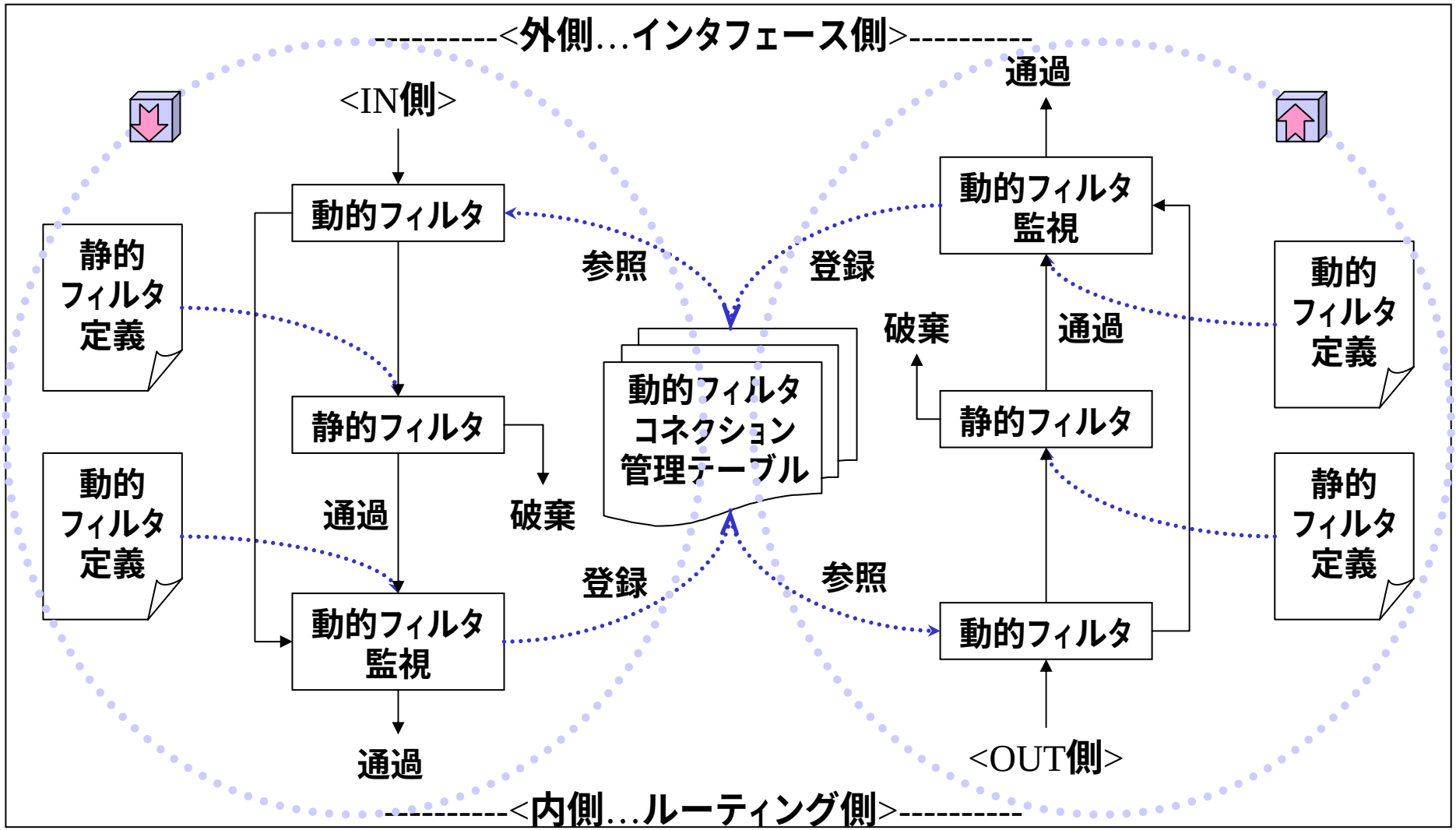
[DNSの処理]
・問い合わせパケットに対して、必ず、応答パケットがある。
→タイマー管理に加えて、応答パケットの到着で閉じる。

セキュリティ・レベル

(ネットボランチのセキュリティ強度の選択機能)

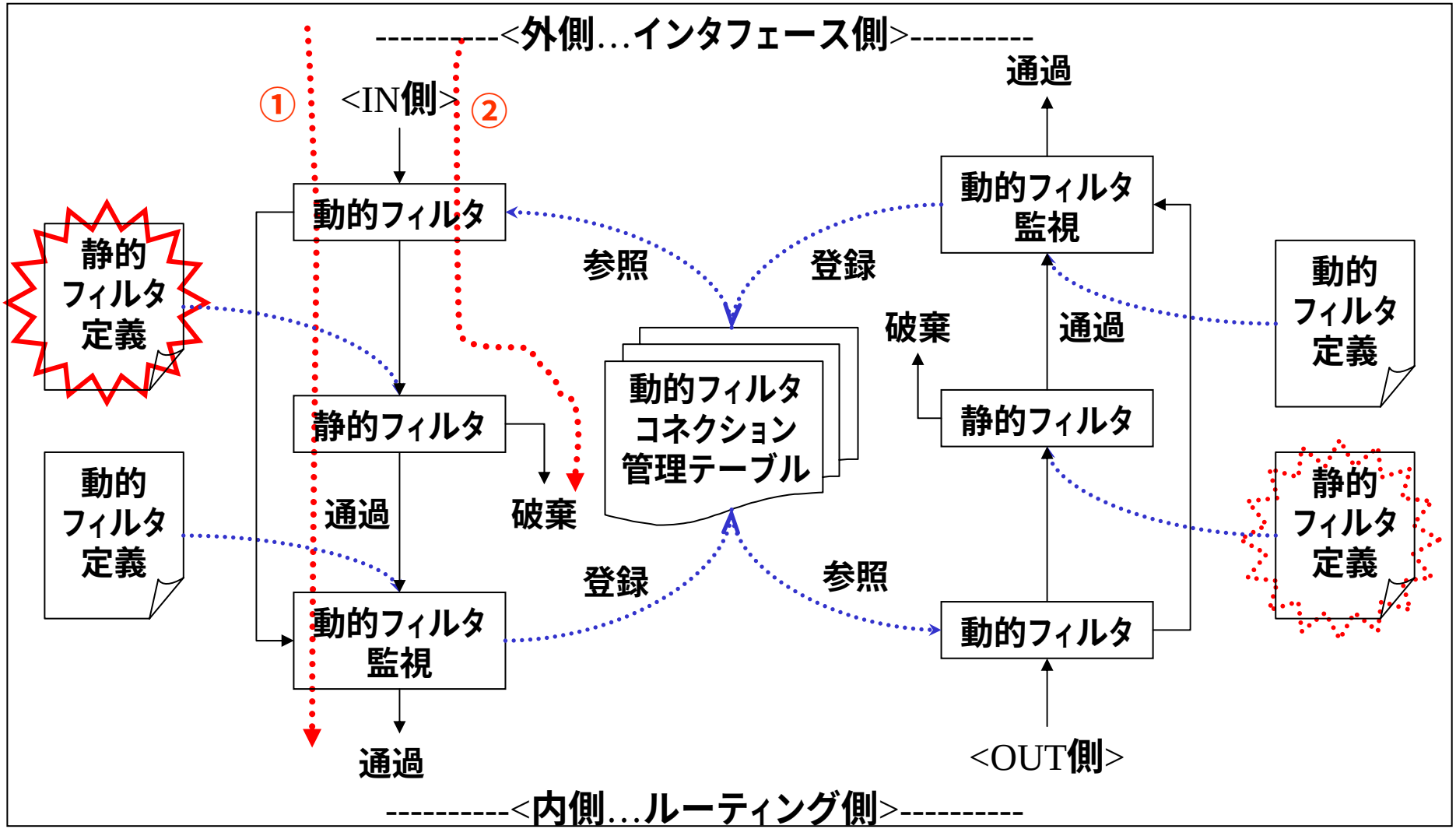
セキュリティ・レベル	1	2	3	4	5	6	7
予期しない発呼を防ぐフィルタ	○	○	○	○	○	○	○
NetBIOS等を塞ぐフィルタ (ポート番号:135,137,138,139,445)		○	○	○	○	○	○
プライベートアドレスのままの通信を禁止するフィルタ			○		○		○
静的セキュリティ・フィルタ (従来のセキュリティフィルタ)				◎	◎		
動的セキュリティ・フィルタ (強固なセキュリティ・フィルタ)						☆	☆

ファイアウォールの構造

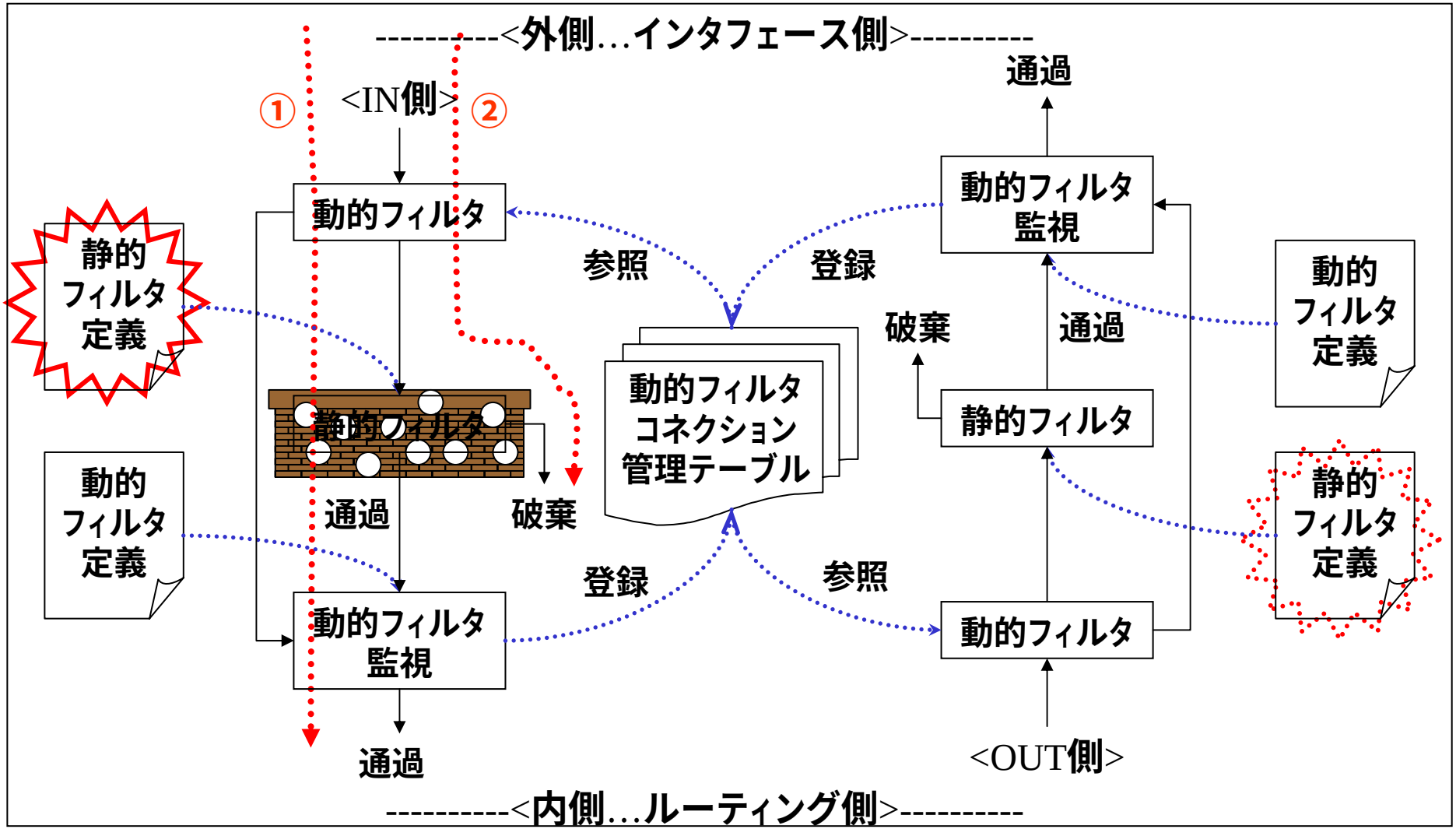


http://www.rtpro.yamaha.co.jp/RT/docs/firewall/index.html

一部の通信路を塞ぐ



静的セキュリティ・フィルタ



設定例#1

(静的セキュリティフィルタ)

[条件]

- ネットボランチ RTA54i
- プロバイダ接続設定の
  セキュリティ・レベル5

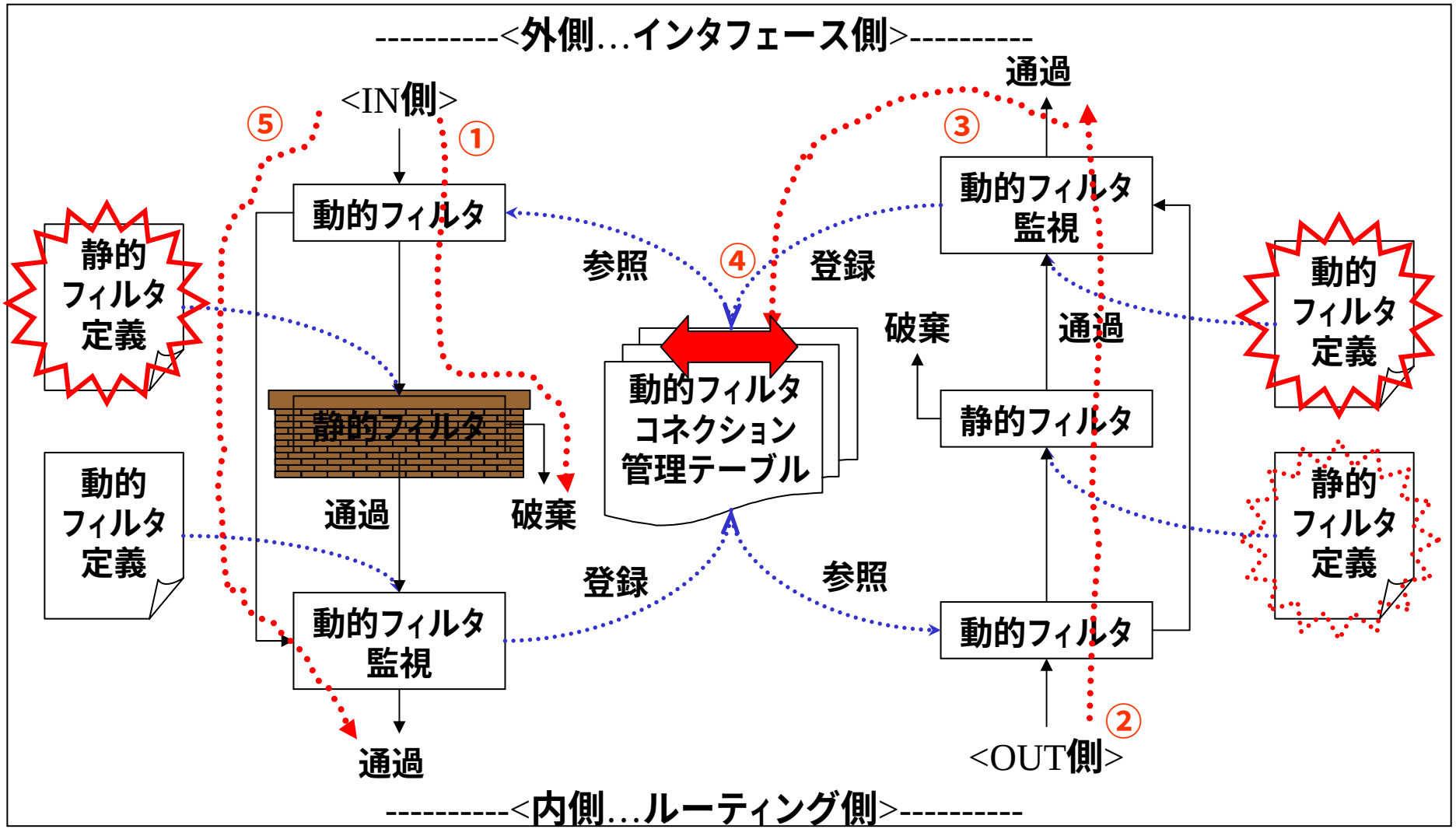
```
入出|# 静的フィルタの定義
■□| ip filter 00 reject 10.0.0.0/8 * * * *
■□| ip filter 01 reject 172.16.0.0/12 * * * *
■□| ip filter 02 reject 192.168.0.0/16 * * * *
■□| ip filter 03 reject 192.168.0.0/24 * * * *
□■| ip filter 10 reject * 10.0.0.0/8 * * *
□■| ip filter 11 reject * 172.16.0.0/12 * * *
□■| ip filter 12 reject * 192.168.0.0/16 * * *
□■| ip filter 13 reject * 192.168.0.0/24 * * *
■■| ip filter 20 reject * * udp,tcp 135 *
■■| ip filter 21 reject * * udp,tcp * 135
■■| ip filter 22 reject * * udp,tcp netbios_ns-netbios_ssn *
■■| ip filter 23 reject * * udp,tcp * netbios_ns-netbios_ssn
■■| ip filter 24 reject * * udp,tcp 445 *
■■| ip filter 25 reject * * udp,tcp * 445
□■| ip filter 26 restrict * * tcpfin * www,21,nntp
□■| ip filter 27 restrict * * tcprst * www,21,nntp
■□| ip filter 30 pass * 192.168.0.0/24 icmp * *
■□| ip filter 31 pass * 192.168.0.0/24 established * *
■□| ip filter 32 pass * 192.168.0.0/24 tcp * ident
■□| ip filter 33 pass * 192.168.0.0/24 tcp ftpdata *
□□| ip filter 34 pass * 192.168.0.0/24 tcp,udp * domain
■□| ip filter 35 pass * 192.168.0.0/24 udp domain *
□□| ip filter 36 pass * 192.168.0.0/24 udp * ntp
□□| ip filter 37 pass * 192.168.0.0/24 udp ntp *
□■| ip filter 99 pass * * * * *
```

```
入出| # 動的フィルタの定義
□□| ip filter dynamic 80 * * ftp
□□| ip filter dynamic 81 * * domain
□□| ip filter dynamic 82 * * www
□□| ip filter dynamic 83 * * smtp
□□| ip filter dynamic 84 * * pop3
□□| ip filter dynamic 98 * * tcp
□□| ip filter dynamic 99 * * udp
```

```
# 接続先のフィルタの入力(IN)と出力(OUT)の適用
pp select 1
ip pp secure filter in 00 01 02 03 20 21 22 23 24 25 30 31 32 33 35
ip pp secure filter out 10  11 12 13 20 21 22 23 24 25 26 27 99
```


http://www.rtpro.yamaha.co.jp/RTA54i/ScreenShot/40310/security-level5.html

動的セキュリティ・フィルタ



設定例#2

(動的セキュリティフィルタ)

[条件]

- ネットボランチ RTA54i
- プロバイダ接続設定の
  セキュリティ・レベル7

```
入出|# 静的フィルタの定義
■□| ip filter 00 reject 10.0.0.0/8 * * * *
■□| ip filter 01 reject 172.16.0.0/12 * * * *
■□| ip filter 02 reject 192.168.0.0/16 * * * *
■□| ip filter 03 reject 192.168.0.0/24 * * * *
□■| ip filter 10 reject * 10.0.0.0/8 * * *
□■| ip filter 11 reject * 172.16.0.0/12 * * *
□■| ip filter 12 reject * 192.168.0.0/16 * * *
□■| ip filter 13 reject * 192.168.0.0/24 * * *
■■| ip filter 20 reject * * udp,tcp 135 *
■■| ip filter 21 reject * * udp,tcp * 135
■■| ip filter 22 reject * * udp,tcp netbios_ns-netbios_ssn *
■■| ip filter 23 reject * * udp,tcp * netbios_ns-netbios_ssn
■■| ip filter 24 reject * * udp,tcp 445 *
■■| ip filter 25 reject * * udp,tcp * 445
□■| ip filter 26 restrict * * tcpfin * www,21,nntp
□■| ip filter 27 restrict * * tcprst * www,21,nntp
■□| ip filter 30 pass * 192.168.0.0/24 icmp * *
□□| ip filter 31 pass * 192.168.0.0/24 established * *
■□| ip filter 32 pass * 192.168.0.0/24 tcp * ident
□□| ip filter 33 pass * 192.168.0.0/24 tcp ftpdata *
□□| ip filter 34 pass * 192.168.0.0/24 tcp,udp * domain
□□| ip filter 35 pass * 192.168.0.0/24 udp domain *
□□| ip filter 36 pass * 192.168.0.0/24 udp * ntp
□□| ip filter 37 pass * 192.168.0.0/24 udp ntp *
□■| ip filter 99 pass * * * * *
```

```
入出| # 動的フィルタの定義
□■| ip filter dynamic 80 * * ftp
□■| ip filter dynamic 81 * * domain
□■| ip filter dynamic 82 * * www
□■| ip filter dynamic 83 * * smtp
□■| ip filter dynamic 84 * * pop3
□■| ip filter dynamic 98 * * tcp
□■| ip filter dynamic 99 * * udp
```

```
# 接続先のフィルタの入力(IN)と出力(OUT)の適用
pp select 1
ip pp secure filter in 00 01 02 03 20 21 22 23 24 25 30 32
ip pp secure filter out 10 11 12 13 20 21 22 23 24 25 26 27 99 dynamic 80 81 82 83 84 98 99
```


http://www.rtpro.yamaha.co.jp/RTA54i/ScreenShot/40310/security-level7.html

不正アクセス検知

[目的]
・この機能は、侵入(Intrusion)や攻撃(attack)を目的とするパケットを受信したときに、それを検出してユーザに通知する。

※侵入に該当するか否かを正確に判定することは難しく、完全な検知が不可能であることに注意してください。

[特徴]
・RTシリーズの実装では、不正なパケットの持つパターン(signature)を比較することで侵入や攻撃を検出します。基本的には、パターンの比較はパケット単位の処理ですが、それ以外にも、コネクションの状態に基づく検査や、ポートスキャンのような状態を持つ攻撃の検査も実施します。
・ネットボランチでは、ログによる報告に加え、ブザーや電子メールで検知状態を通知します。
・不正アクセスが明らかであれば、該当パケットを破棄させることも可能です。

不正アクセス検知の内容#1

種別	名称	判定条件	
IP ヘッダ	Unknown IP protocol	protocolフィールドが101以上のとき	▲
	Land atack	始点IPアドレスと終点IPアドレスが同じとき	
	Short IP header	IPヘッダの長さがlengthフィールドの長さよりも短いとき	○
	Malformed IP packet	lengthフィールドと実際のパケットの長さが違うとき	○

[記号の意味]

無印:設定次第で破棄する

○:不正アクセス検知機能でなくても、異常と判断し、破棄する

△:設定に関わらず破棄しない (危険度が低い、または、誤検出の確率が高い)

▲:設定に関わらず破棄する (危険度が高い、および、誤検出の確率が低い)

★:動的フィルタと併用することにより、不正アクセス検知機能が有効になる。

不正アクセス検知の内容#2

種別	名称	判定条件
IP オプション ヘッダ	Malformed IP opt	オプションヘッダの構造が不正であるとき
	Security IP opt	Security and handling restriction header を受信したとき
	Loose routing IP opt	Loose source routing header を受信したとき
	Record route IP opt	Record route header を受信したとき
	Stream ID IP opt	Stream identifier header を受信したとき
	Strict routing IP opt	Strict source routing header を受信したとき
	Timestamp IP opt	Internet timestamp header を受信したとき

不正アクセス検知の内容#3

種別	名称	判定条件	
フラグメント	Fragment storm	大量のフラグメントを受信したとき	
	Large fragment offset	フラグメントのoffsetフィールドが大きいとき	
	Too many fragment	フラグメントの分割数が多いとき	
	Teardrop	teardropなどのツールによる攻撃を受けたとき	▲
	Same fragment offset	フラグメントのoffsetフィールドの値が重複しているとき	
	Invalid fragment	そのほかのリアセンブル不可能なフラグメントを受信したとき	▲

不正アクセス検知の内容#4

種別	名称	判定条件
ICMP	ICMP source quench	source quenchを受信したとき
	ICMP timestamp req	timestamp requestを受信したとき
	ICMP timestamp reply	timestamp replyを受信したとき
	ICMP info request	information requestを受信したとき
	ICMP info reply	information replyを受信したとき
	ICMP mask request	address mask requestを受信したとき
	ICMP mask reply	address mask replyを受信したとき
	ICMP too large	1024バイト以上のICMPを受信したとき

不正アクセス検知の内容#5

種別	名称	判定条件	
UDP	UDP short header	UDPのlengthフィールドの値が8よりも小さいとき	▲
	UDP bomb	UDPヘッダのlengthフィールドの値が大きすぎるとき	
	UDP port scan	ポートスキャンを受けたとき	△
TCP	TCP queue overflow	TCPのパケットキューが長くなったとき	★
	TCP no bits set	フラグに何もセットされていないとき	
	TCP SYN and FIN	SYNとFINが同時にセットされているとき	
	TCP FIN and no ACK	ACKのないFINを受信したとき	
	TCP port scan	ポートスキャンを受けたとき	△
	TCP SYN flooding	一定時間に大量のSYNを受けたとき	

不正アクセス検知の内容#6

種別	名称	判定条件	
FTP	FTP improper port	PORTやPASVコマンドで指定されるポート番号が1024〜65535の範囲でないとき	★
SMTP	SMTP pipe attack	From:などのヘッダにパイプ「|」を含むとき	★
	SMTP decode alias	ヘッダに「: decode@」を含むとき	★
	SMTP DEBUG command	DEBUGコマンドを受信したとき	★
	SMTP EXPN command	EXPNコマンドを受信したとき	★
	SMTP VRFY command	VRFYコマンドを受信したとき	★
	SMTP WIZ command	WIZコマンドを受信したとき	★

インターネット電話
VoIPとは？
～知識の整理～

- VoIP関連用語
- インターネット電話の変化

VoIP関連用語#1

(総務省、IPネットワーク技術に関する研究会報告書)
http://www.soumu.go.jp/s-news/2002/020222_3.html

「IP電話」：

ネットワークの一部又は全部においてIPネットワーク技術を利用して提供する音声電話サービスとする。

「インターネット電話」：

IP電話のうち、WWW等のアプリケーションに利用されているものと同じIPネットワークを利用するもの（以下では、単に「インターネット」とする。）を、特に「インターネット電話」とする。

「VoIP」：Voice over IP

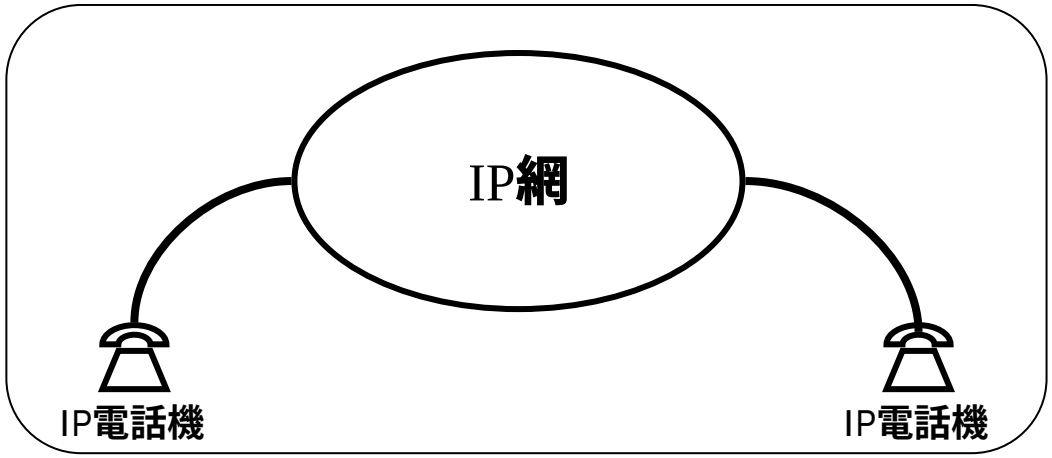
IP電話やインターネット電話を実現する技術の総称

プロトコルには、H.323、MGCP、SIPなどいくつかある。

「ITSP」：Internet Telephony Service Provider

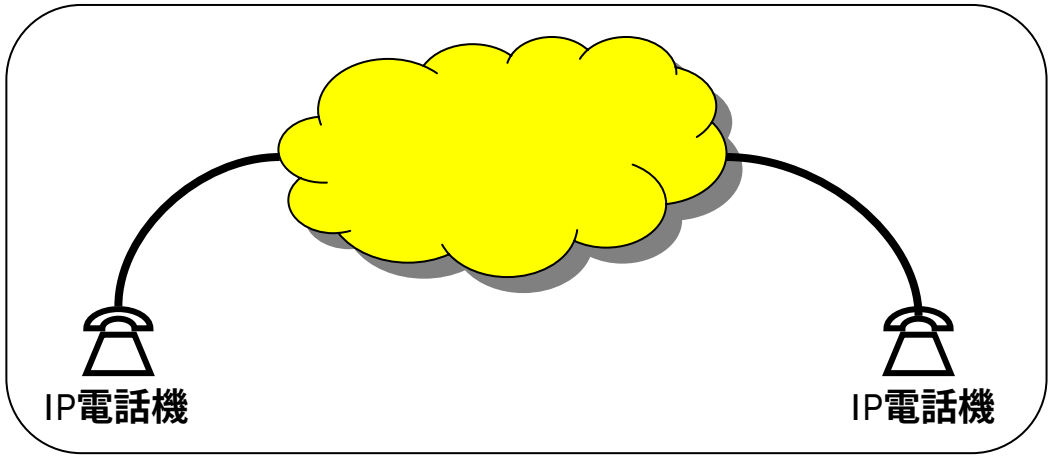
IP電話やインターネット電話サービスを提供する事業者

IP電話とインターネット電話



IP電話

[回線の特徴]
・ギャランティー型
→帯域制御、優先制御、
帯域保証、…
(+) 高音質
(-) 高コスト



インターネット電話

[回線の特徴]
・ベストエフォート型
→パケット遅延、パケット損失、
…
(-) 低音質
(+) 低コスト

VoIP関連用語#2

(総務省、IPネットワーク技術に関する研究会報告書)
http://www.soumu.go.jp/s-news/2002/020222_3.html

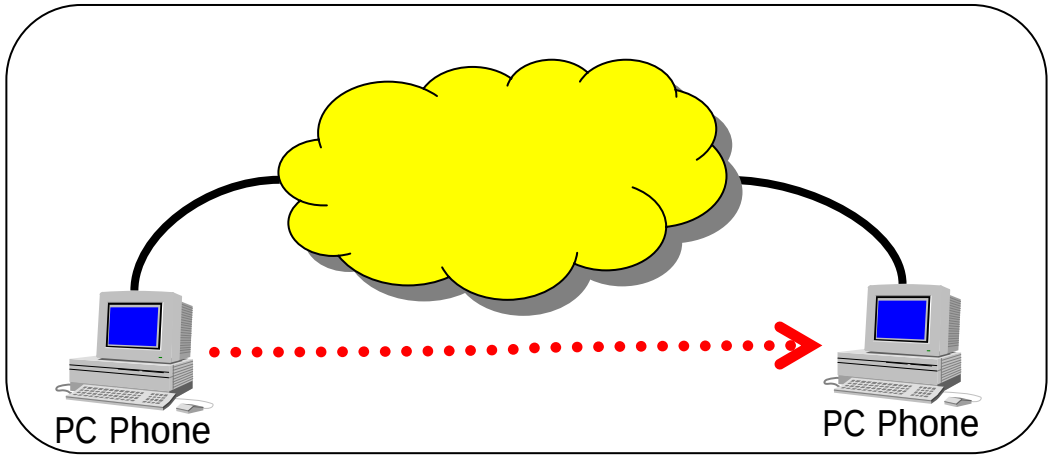
「PC-to-PCタイプのIP電話サービス」：
1994年頃より、ダイヤルアップによるインターネット接続環境で利用するパソコンのソフトウェアが登場。

「PC-to-Phoneタイプの IP電話サービス」：
1996年頃には、パソコンから一般加入電話に電話できるようなサービスが登場。

「Phone-to-Phoneタイプの IP電話サービス」：
1997年頃になると、インターネットの両端にゲートウェイを置いた一般加入電話相互の接続サービスが始まる。

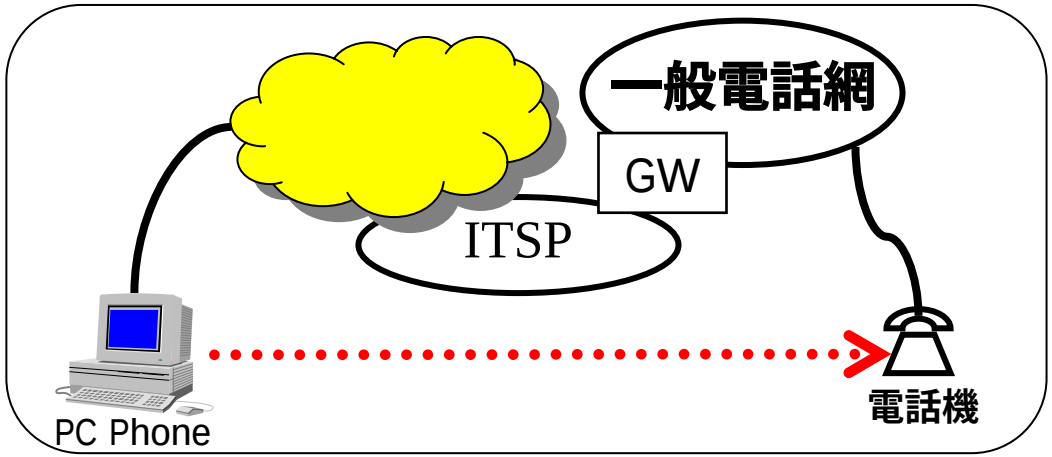
「Phone-to-PCタイプの IP電話サービス」：
PCの電話番号、常時接続されたPC、などの課題があり実際に提供されるサービスは無い。

「PC-to-PC」と「PC-to-Phone」



PC-to-PC

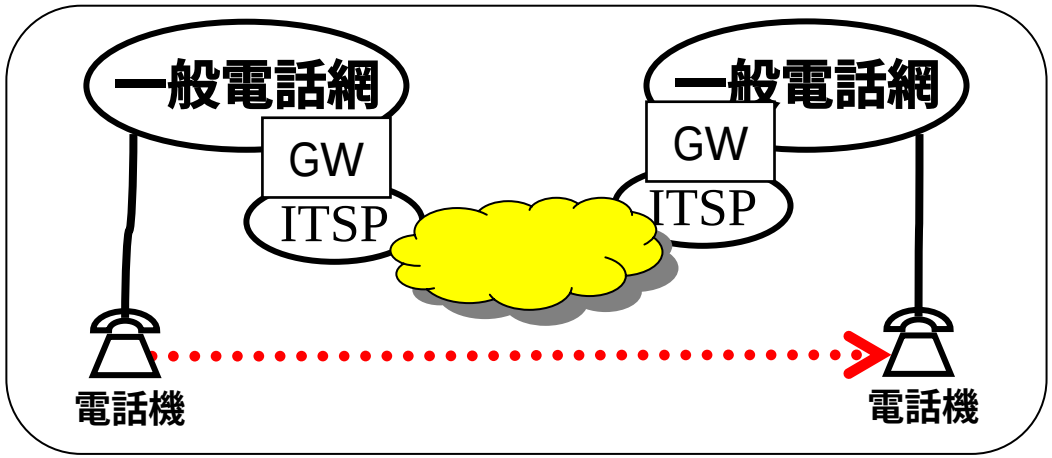
[回線の特徴]
・1994年～
・ダイヤルアップによる
　インターネット接続環境
(-) 低音質、パソコン必須
(+) 低コスト



PC-to-Phone

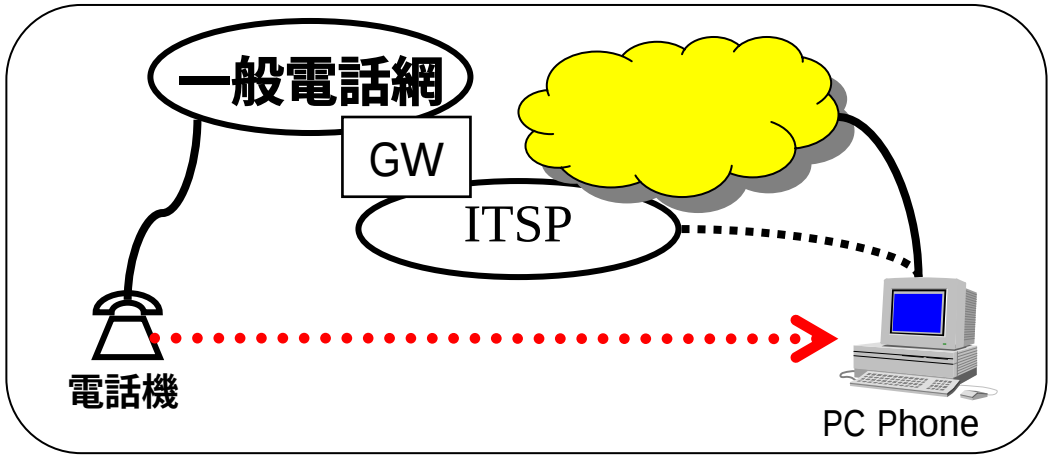
[回線の特徴]
・1996年～
・ダイヤルアップによる
　インターネット接続環境
(-) 低音質、パソコン必須
(+) 低コスト

「Phone-to-Phone」と「Phone-to-PC」



Phone-to-Phone

[回線の特徴]
・1997年～
・パソコンを使用しない
(-) 低音質
(+) 手軽、低コスト

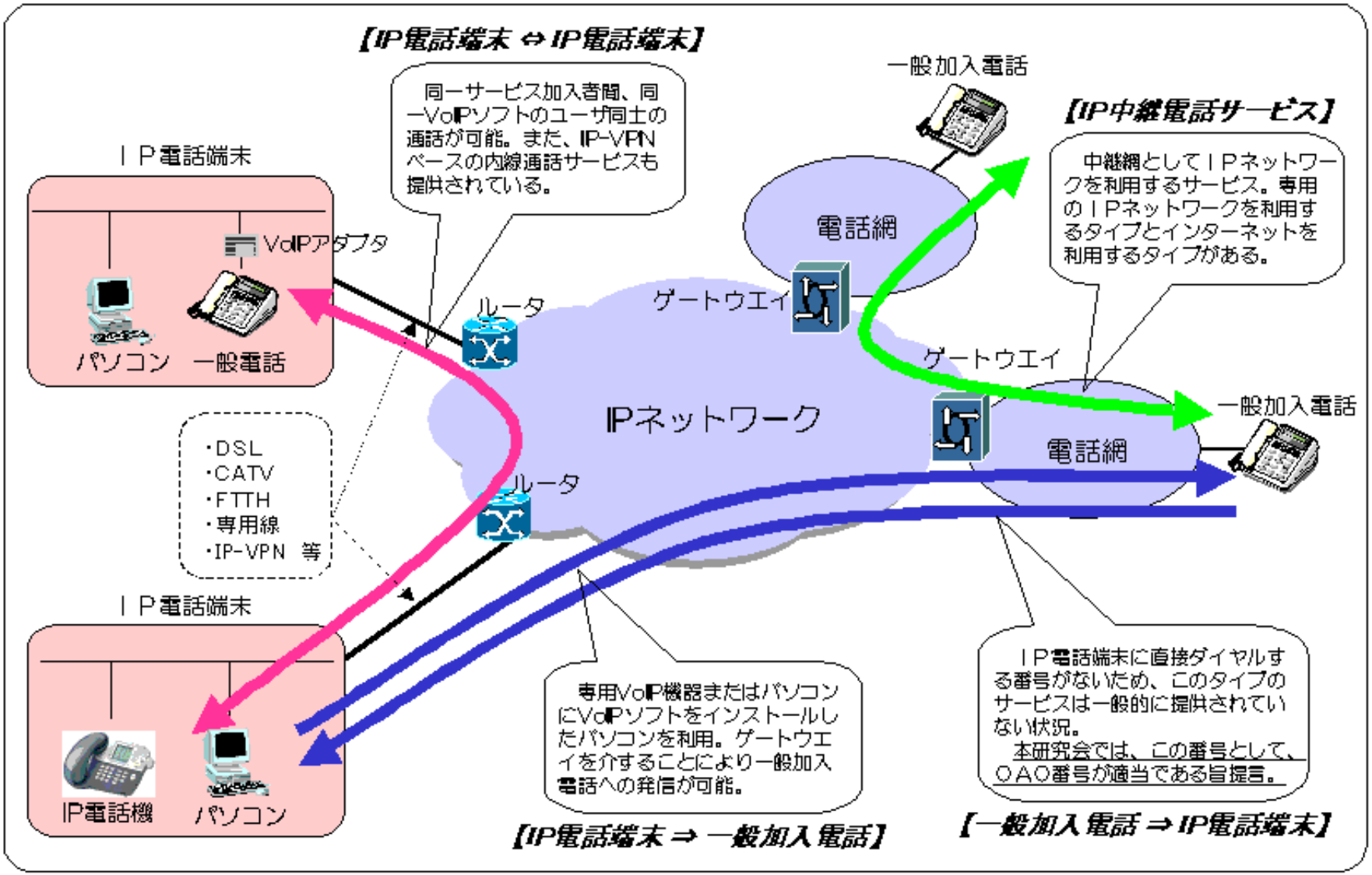


Phone-to-PC

[回線の特徴]
・未提供
(-) 常時接続性、電話番号

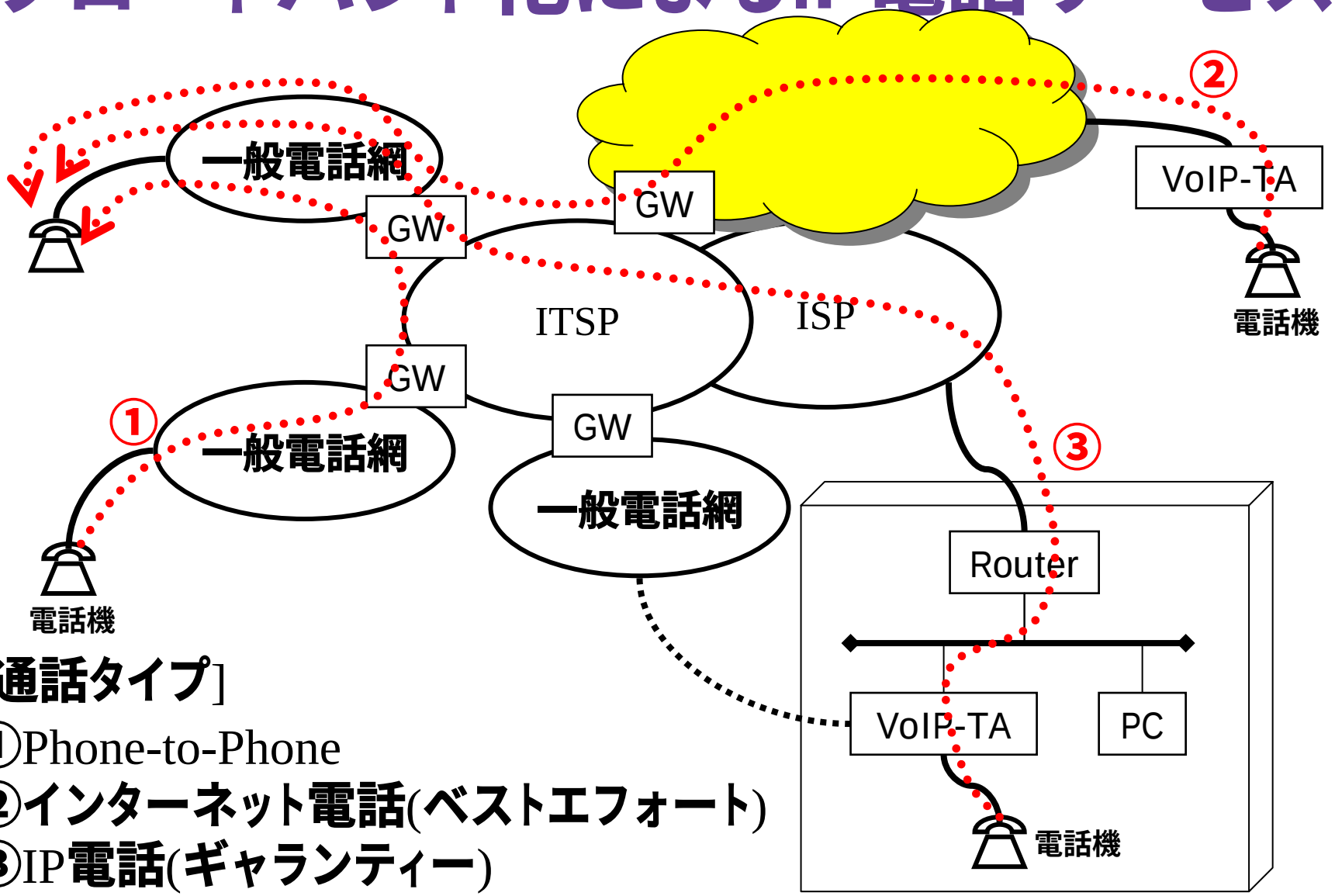
ブロードバンド化による IP電話サービス

(総務省、IPネットワーク技術に関する研究会報告書)
http://www.soumu.go.jp/s-news/2002/020222_3.html



※ 本研究会では、これらすべてのタイプのIP電話サービスにおいて、ユーザが容易に理解できるようなエンドトゥエンドの品質を表示することが適当であるとし、また、それぞれのサービスの品質が適正に比較できるように、IP電話の品質評価方法等の標準化作業を官民が協力して推進していくことが必要である旨提言。

ブロードバンド化によるIP電話サービス



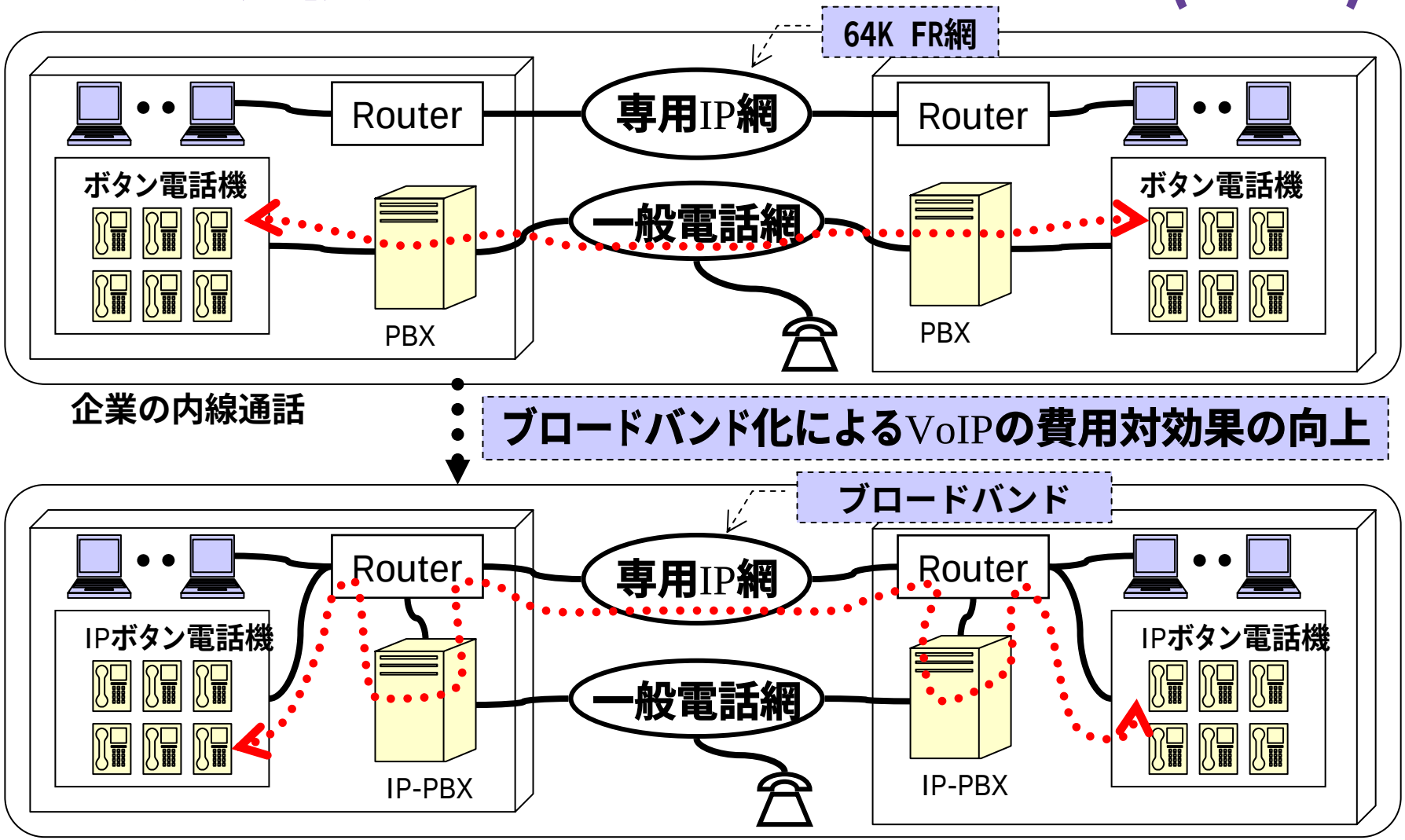
[通話タイプ]

①Phone-to-Phone

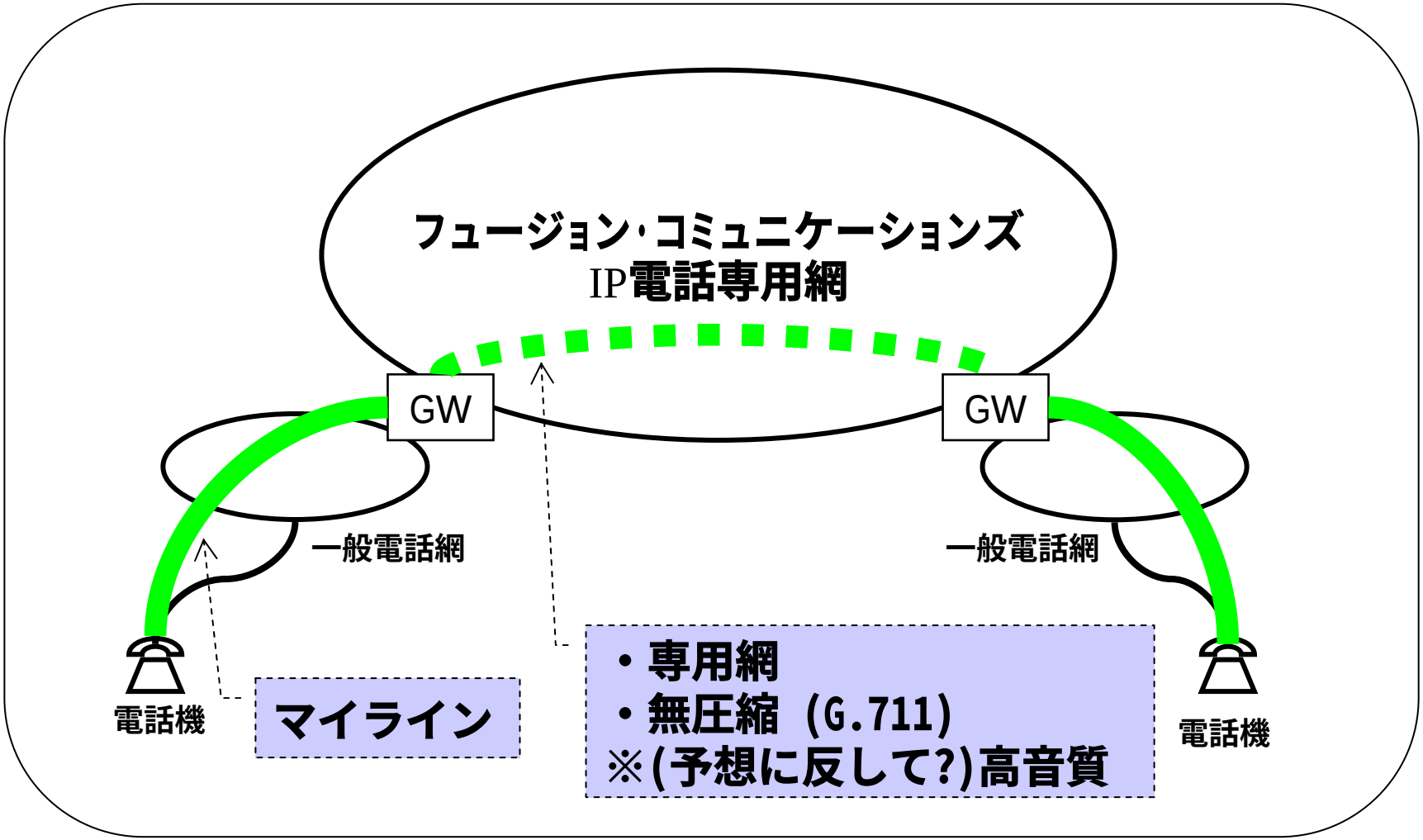
②インターネット電話(ベストエフォート)

③IP電話(ギャランティー)

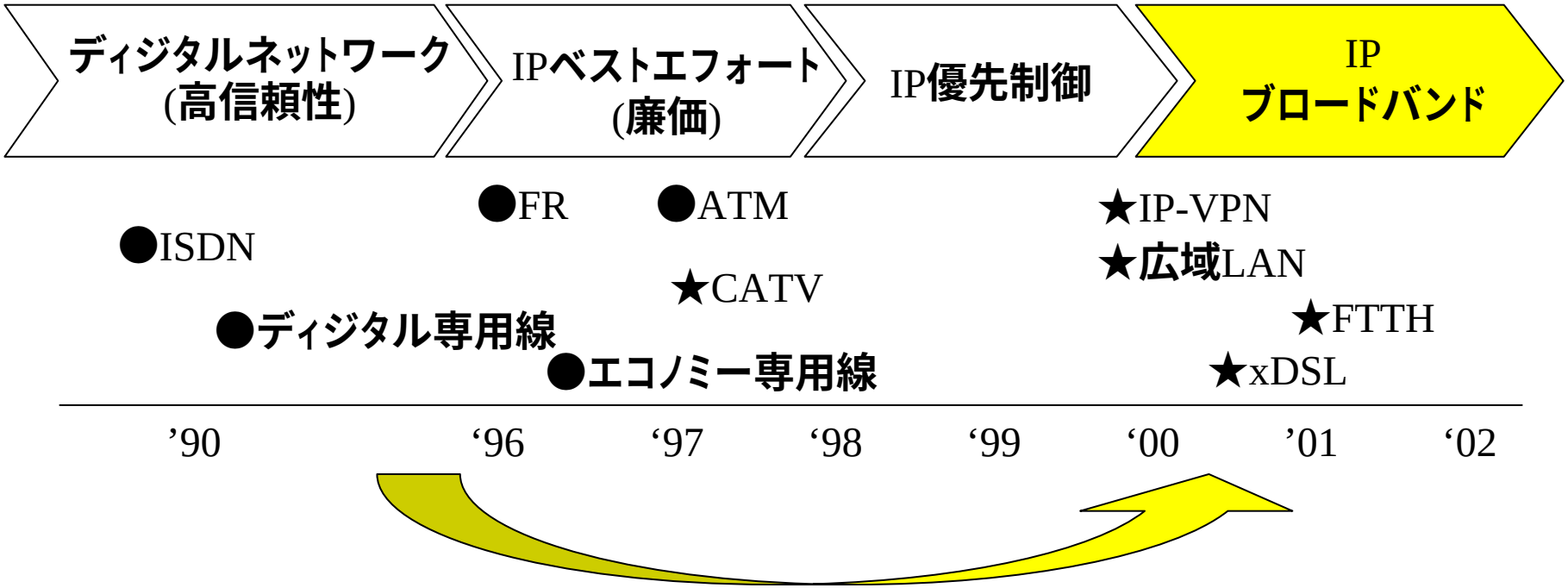
大規模ビジネスホンのVoIP化(IT化)



フュージョンにみられるIP電話の変化



ブロードバンドとVoIPの関連性



	ナローバンド →	ブロードバンド
回線 (IP通信)	低速、小容量、高コスト、間欠接続 →高信頼性、帯域保証	高速、大容量、低コスト、常時接続 →ベストエフォート、リアルタイム性向上
音声データ (VoIP)	音声の帯域占有率が大きい →高コスト (優先/帯域制御)	音声の帯域占有率が小さい →低コスト(投資効果が大きい)
プロトコル (VoIP)	H.323+音声圧縮(64kbps⇒8kbps) →複雑+低音質	SIP+音声無圧縮(G.711,64kbps) →シンプル+高音質

ブロードバンドによる インターネット電話の変化

[ブロードバンド]
- 広帯域
- 低廉性
- 常時接続環境

[プロトコルの変化]
- H.323→SIP
- 複雑→シンプル

[音声データの変化]
- 圧縮→無圧縮
- 高音質 (G.711)

ブロードバンド時代 の インターネット電話

イーサネット
～知識の整理～

イーサネットの規格

種類	距離	ノード数	ケーブル種類
10BASE2	185m	30	同軸(直径5mm)
10BASE5	500m	100	同軸(直径10mm)
10BASE-T	100m		UTP (カテゴリ3~)
10BASE-F	1000m	2	光ファイバ(MMF)
100BAST-TX	100m		UTP/STP(カテゴリ5~),10BASE-T互換
100BAST-FX	412m	2	光ファイバ(MMF)
100BASE-T4	100m		UTPケーブル(カテゴリ3〜)
1000BASE-T	100m		UTPケーブル(カテゴリ5e~)
1000BASE-CX	25m		シールドされた銅線
1000BASE-SX	220〜550	2	光ファイバ(MMF)
1000BASE-LX	550/5000	2	光ファイバ(MMF/SMF)

イーサネットの用語#1

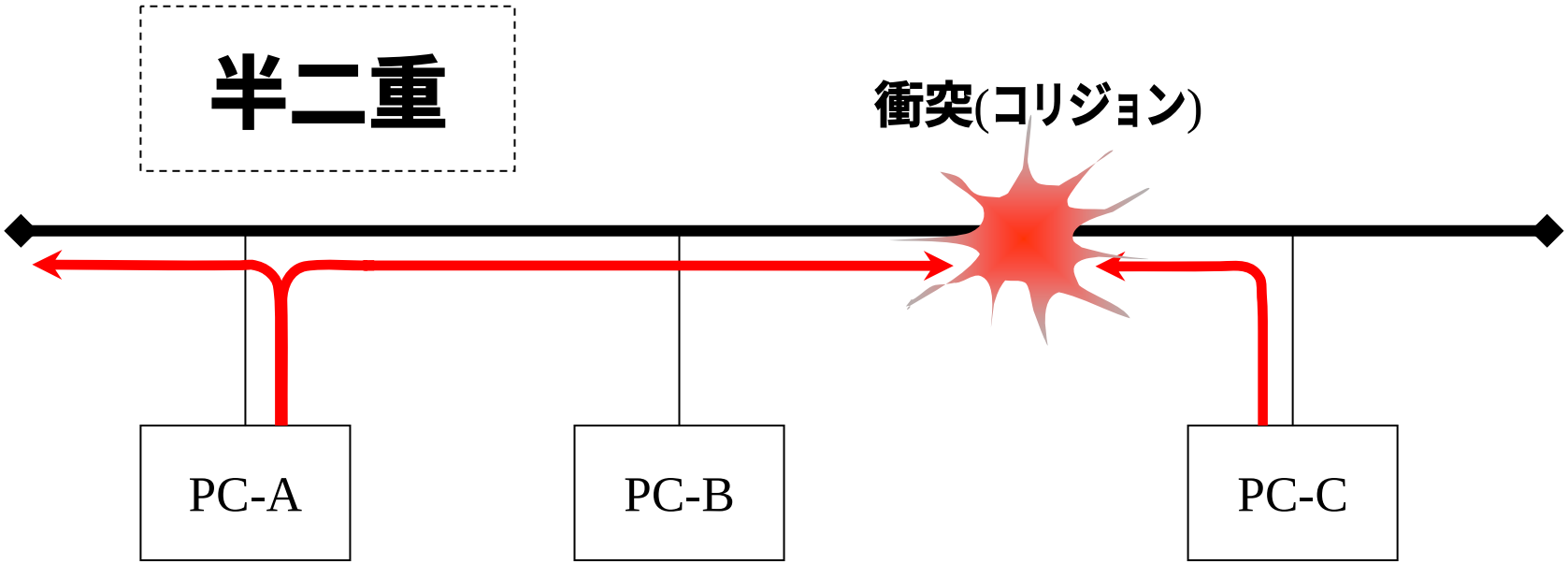
呼称	説明
イーサネット	10BASEシリーズ (IEEE 802.3)
ファースト･イーサネット	100BASEシリーズ (IEEE 802.3u)
ギガビット･イーサネット	1000BASEシリーズ (IEEE 802.3z, IEEE 802.3ab)

表記	コンピュータの内部表現 (2進数系)	伝送速度の数値表現 (10進数系)
1k	1024 (2^10)	1000 (10^3)
1M	1024K (2^20)	1000k (10^6)
1G	1024M (2^30)	1000M (10^9)

イーサネットの用語#2

	英語表記	説明
UTP	Unshielded Twisted Pair Cable	シールドなしツイストペアケーブル
STP	Shielded Twisted Pair Cable	シールドされたツイストペアケーブル
MMF	Multi Mode Fiber	マルチモード光ファイバー
SMF	Single Mode Fiber	シングルモード光ファイバー

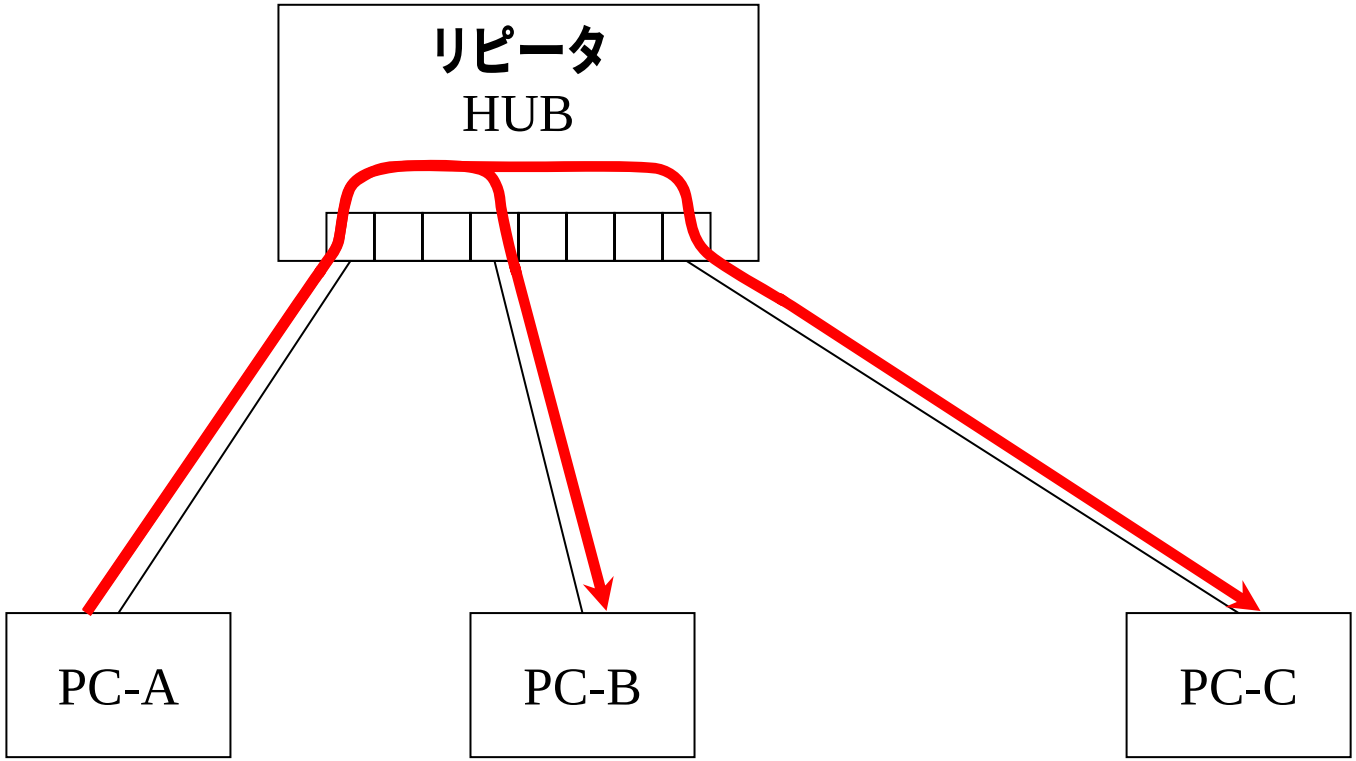
イーサネット#1 (バス型)



CSMA/CD: Carrier Sense Multiple Access with Collision Detection

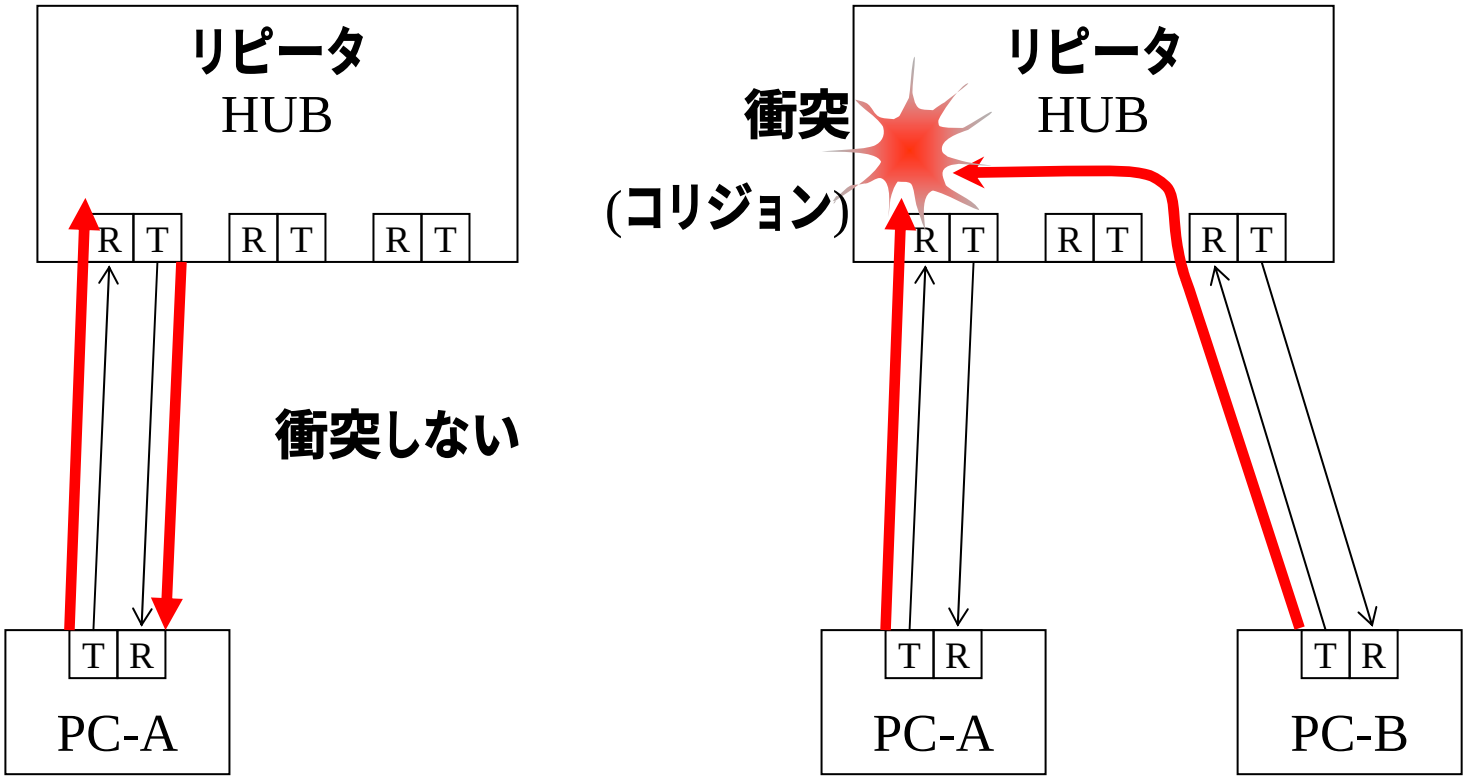
端末はパケットを送る前に他の端末が伝送路を使用しているかどうか確認する。未使用であれば送信するのだが、タイミングが悪いと衝突(Collision)**する。衝突したら、再送する。衝突が多いと速度低下する。**

イーサネット#2 (スター型)

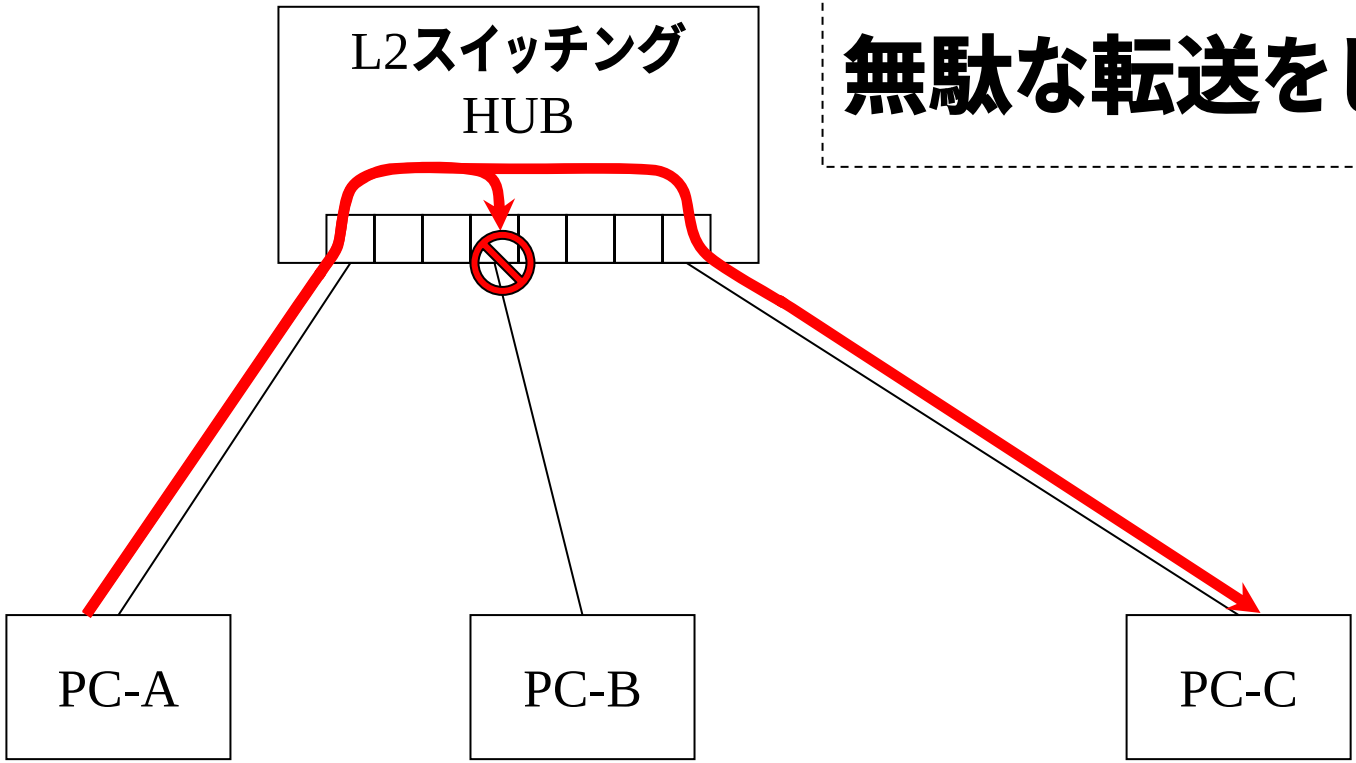


イーサネット#3 (ツイストペア線)

全二重(も可能)

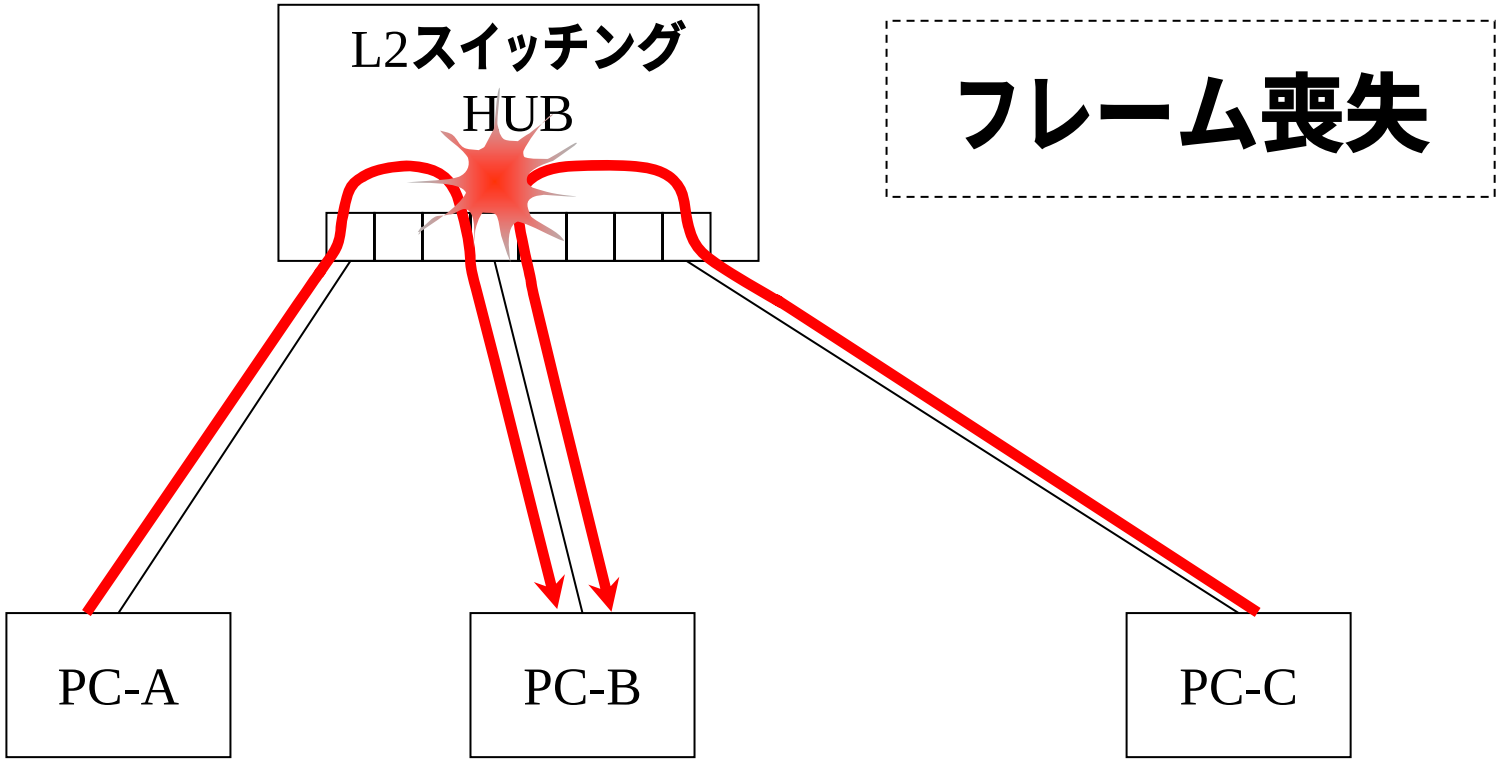


イーサネット#4 (スター型)

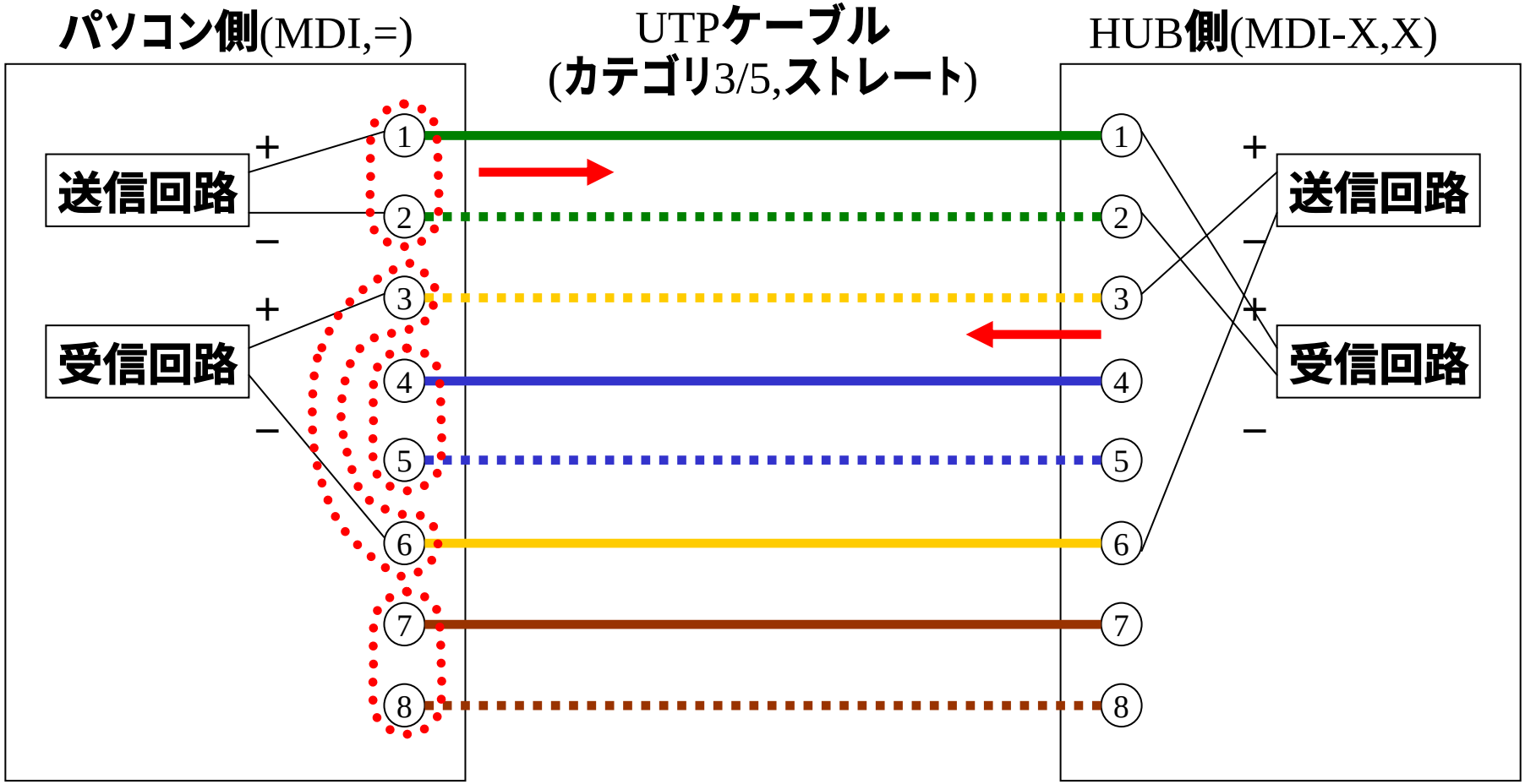


無駄な転送をしない

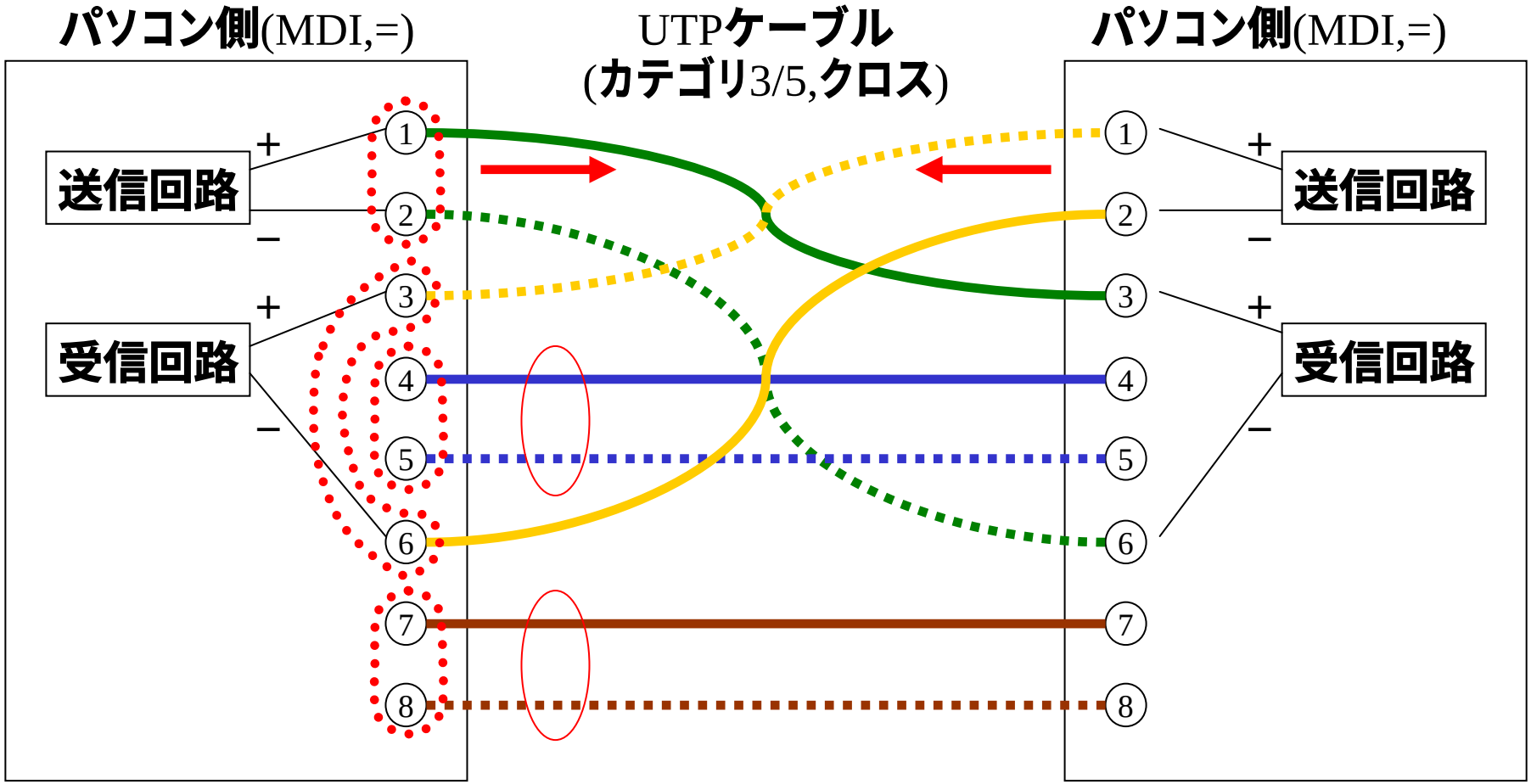
イーサネット#5 (スター型)



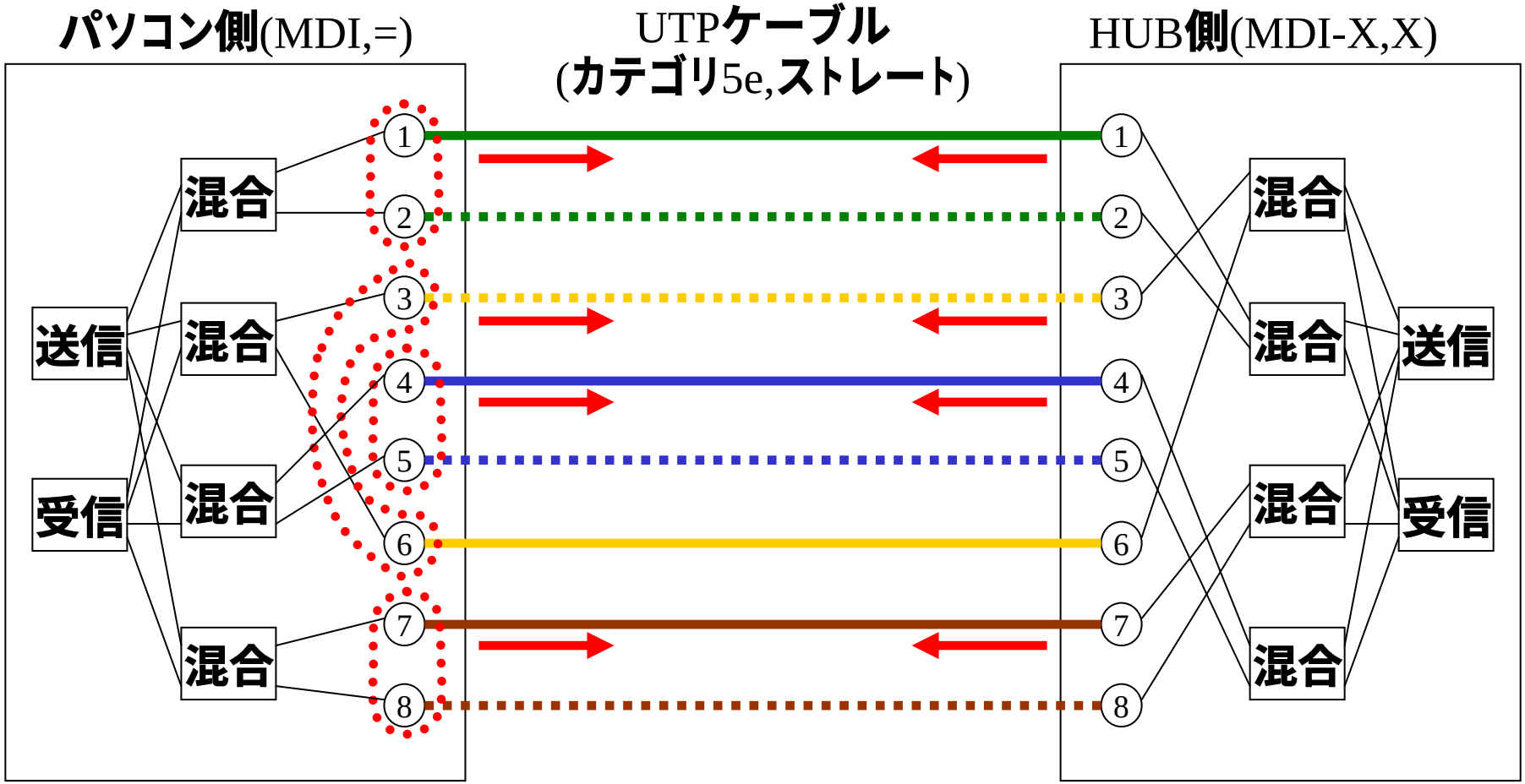
10BASE-T/100BASE-TX #1



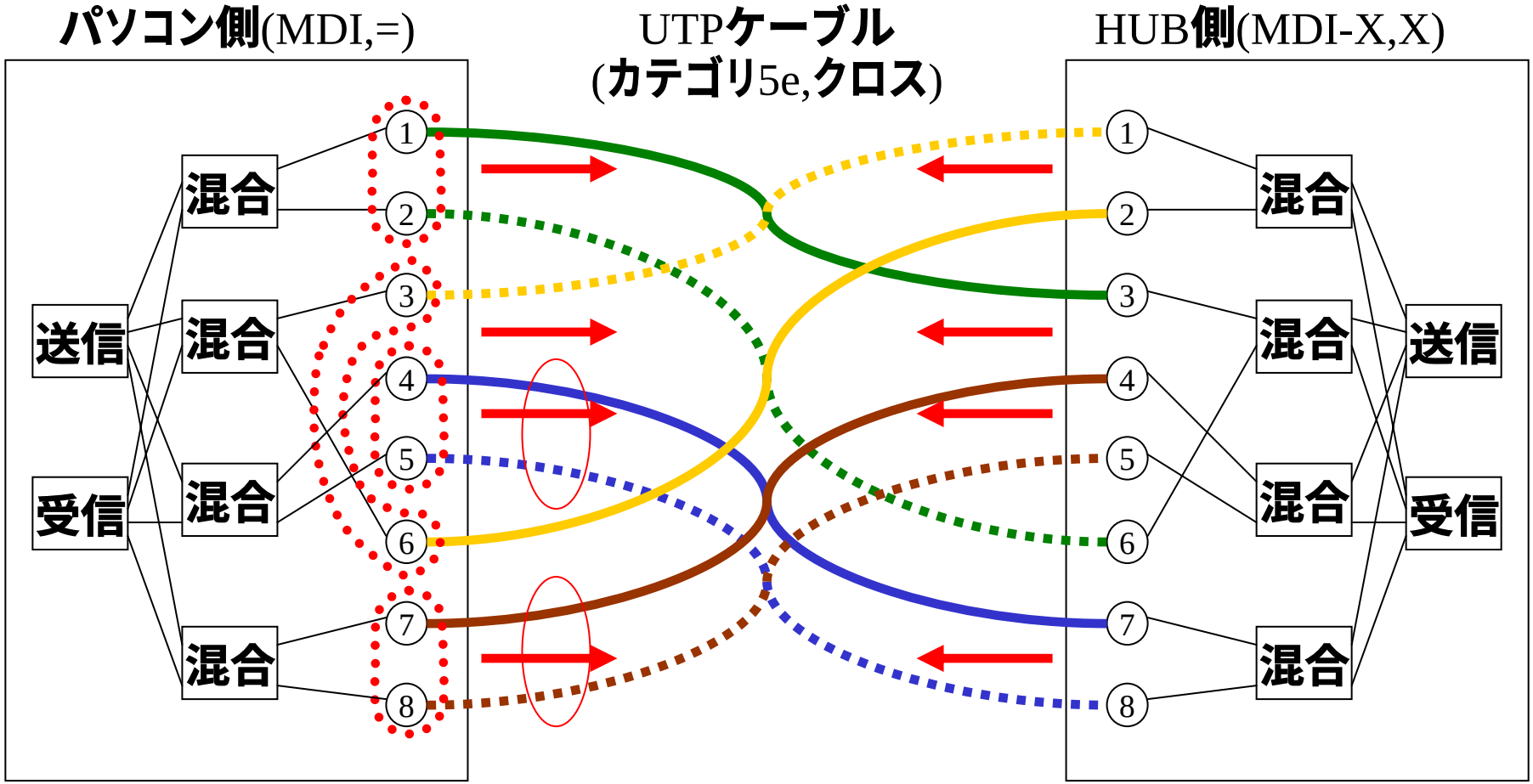
10BASE-T/100BASE-TX #2



1000BASE-T #1


パソコン側(MDI,=)
UTPケーブル
(カテゴリ5e,ストレート)
HUB側(MDI-X,X)
送信
受信
混合
混合
混合
混合
1
2
3
4
5
6
7
8
1
2
3
4
5
6
7
8
混合
混合
混合
混合
送信
受信

1000BASE-T #2



Auto Negotiation(自動認識)

		自動認識	固定設定			
			100Mbps 全二重	100Mbps 半二重	10Mbps 全二重	10Mbps 半二重
自動認識		100Mbps 全二重	×	100Mbps 半二重	×	10Mbps 半二重
固定設定	100Mbps 全二重	×	100Mbps 全二重	×	×	×
	100Mbps 半二重	100Mbps 半二重	×	100Mbps 半二重	×	×
	10Mbps 全二重	×	×	×	10Mbps 全二重	×
	10Mbps 半二重	10Mbps 半二重	×	×	×	10Mbps 半二重

イーサネットのフレームフォーマット

Ethernetフレームフォーマット

プリアンブル (8) フレーム開始信号	送信元 MAC アドレス (6)	宛先 MAC アドレス (6)	イーサネット タイプ (2) 0x0800	IPパケット (46〜1500)	FCS (4)

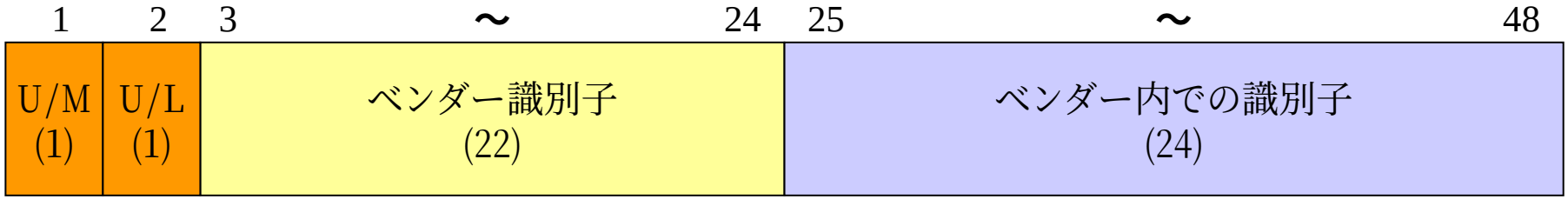
0000〜05DC	IEEE 802.3 Length Field (0〜1500)
0800	Internet Protocol version 4 (IPv4)
0806	ARP (Address Resolution Protocol)
8035	RARP (Reverse Address Resolution Protocol)
8037	IPX (Novell NetWare)
86DD	Internet Protocol version 6 (IPv6)
8863	PPPoE Discovery Stage
8864	PPPoE Session Stage

(参考) IEEE 802.3 Ethernetフレームフォーマット

プリアンブル (8) フレーム開始信号	送信元 MAC アドレス (6)	宛先 MAC アドレス (6)	フレーム長 (2)	LLC (3)	SNAP (5)	データ (38〜1492)	FCS (4)

MACアドレス

(16進数表記)
XX：XX：XX ： XX：XX：XX



1ビット目:ユニキャストアドレス(0)/マルチキャストアドレス(1)
2ビット目:ユニバーサルアドレス(0)/ローカルアドレス(1)
3～24:ベンダー識別子 (OUI:Organizationally Unique Identifier)
　　http://standards.ieee.org/regauth/oui/
25～48:製品毎の番号

ff:ff:ff:ff:ff:ff → ブロードキャストアドレス
00:a0:de:xx:xx:xx → ヤマハ製品

※ビットの配列と16進数値は、オクテット単位で、LSBとMSBが逆

無線LAN
～知識の整理～

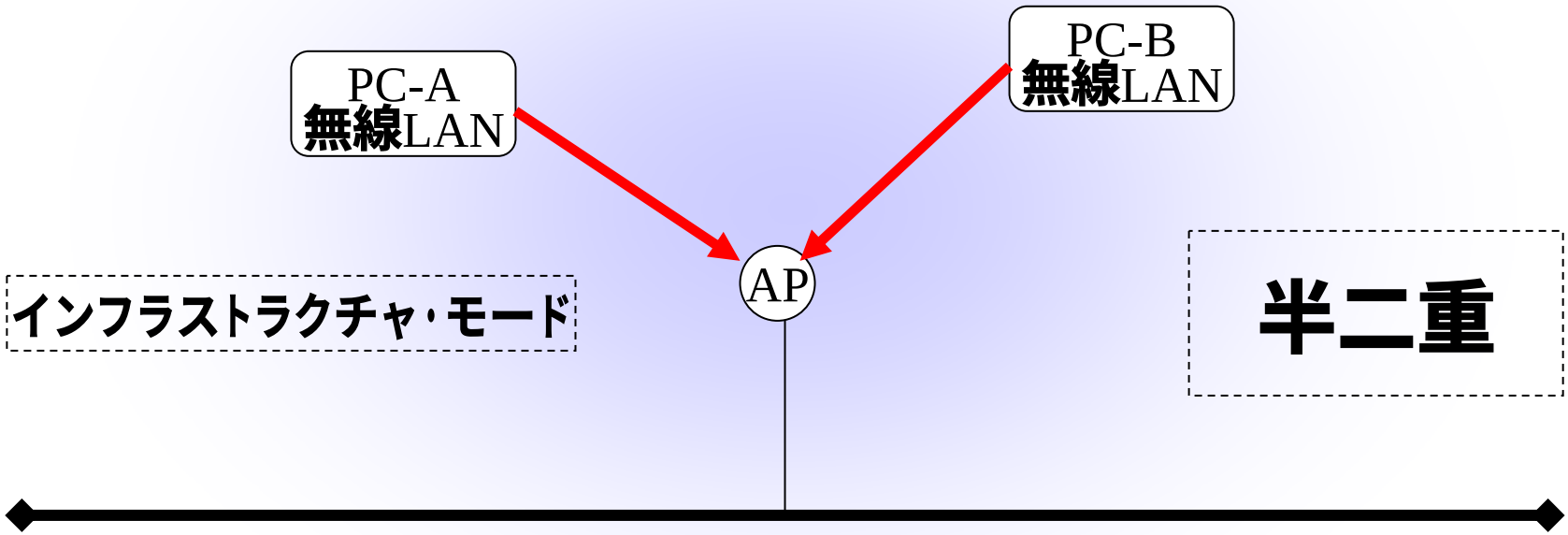
無線アクセス

	使用周波数帯域	最大伝送速度
携帯電話	800MHz 1.5GHz	9.6, 14.4, 28.8, 64kbps
PHS	1.9GHz	32, 64, 128kbps
IMT2000	2GHz	64, 384kbps
Bluetooth	2.4GHz	**下り**:723kbps、**上り**:57kbps
無線LAN	2.4GHz	1,2Mbps (IEEE 802.11**の一部**)
	2.4GHz	1,2,5,11Mbps (IEEE 802.11b) 22Mbps (IEEE 802.11g**の一部**)
	5GHz(**屋内**)	6**〜**54Mbps (IEEE 802.11a)
FWA	22,26GHz	10Mbps (1**対多地点**, **伝送距離半径**1km**程度**)
	22,26,38GHz	156Mbps (1**対**1, **伝送距離**5km**程度**)

IEEE 802.11シリーズ

		規格名	概要
PHY関連	2.4GHz帯関連	IEEE802.11b	現行の2.4GHz帯の物理層の基本仕様
		IEEE802.11g	2.4GHz帯の高速化仕様
	5GHz帯関連	IEEE802.11a	5GHz帯の物理層の基本仕様
		IEEE802.11h	ヨーロッパ用の仕様
	その他	IEEE802.11d	世界各国用の仕様
MAC関連		IEEE802.11c	ブリッジとして動かすために必要な機能の追加
		IEEE802.11e	QoS機能の追加
		IEEE802.11f	異なるベンダーのアクセスポイント間での相互接続性の保証
		IEEE802.11i	セキュリティ機能の強化

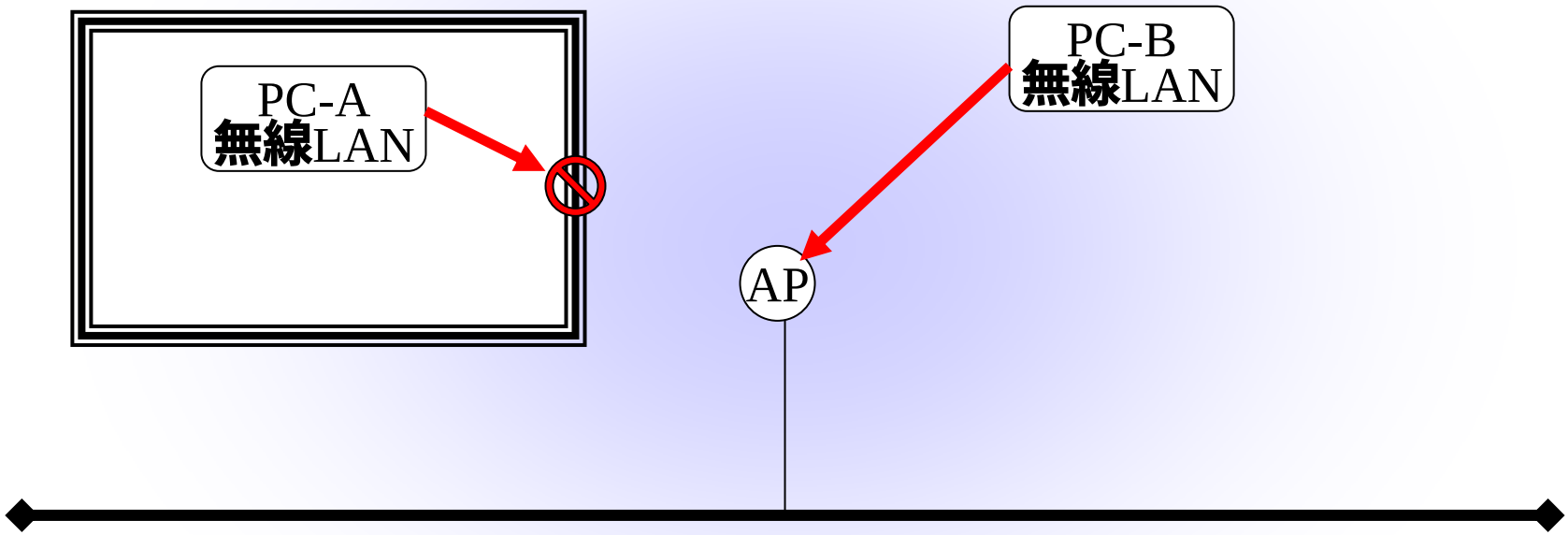
無線LAN (IEEE 802.11b)



CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance

無線では、複数の端末が同時にパケットを送っても干渉などを検知できないので、誰も電波を出していないのを確認してから、ランダムな時間を待ってから、パケットを送り始める。アクセスポイントは、受信したら、ACK**を返信する。**

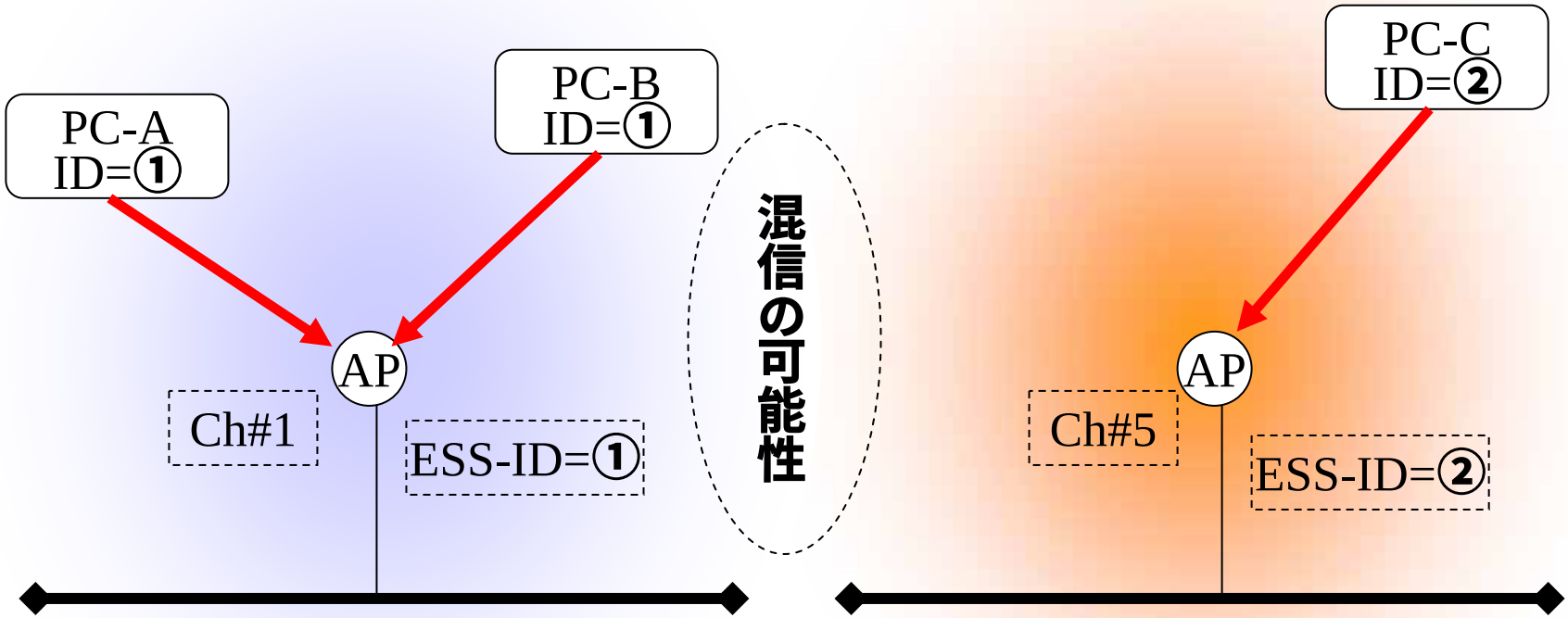
障害物



[障害物]

木造か、鉄筋コンクリートか、というより、壁や床や天井がどんな材料で構成されているかが重要です。電波を通しにくい素材を多用していれば、電波は通りにくくなります。

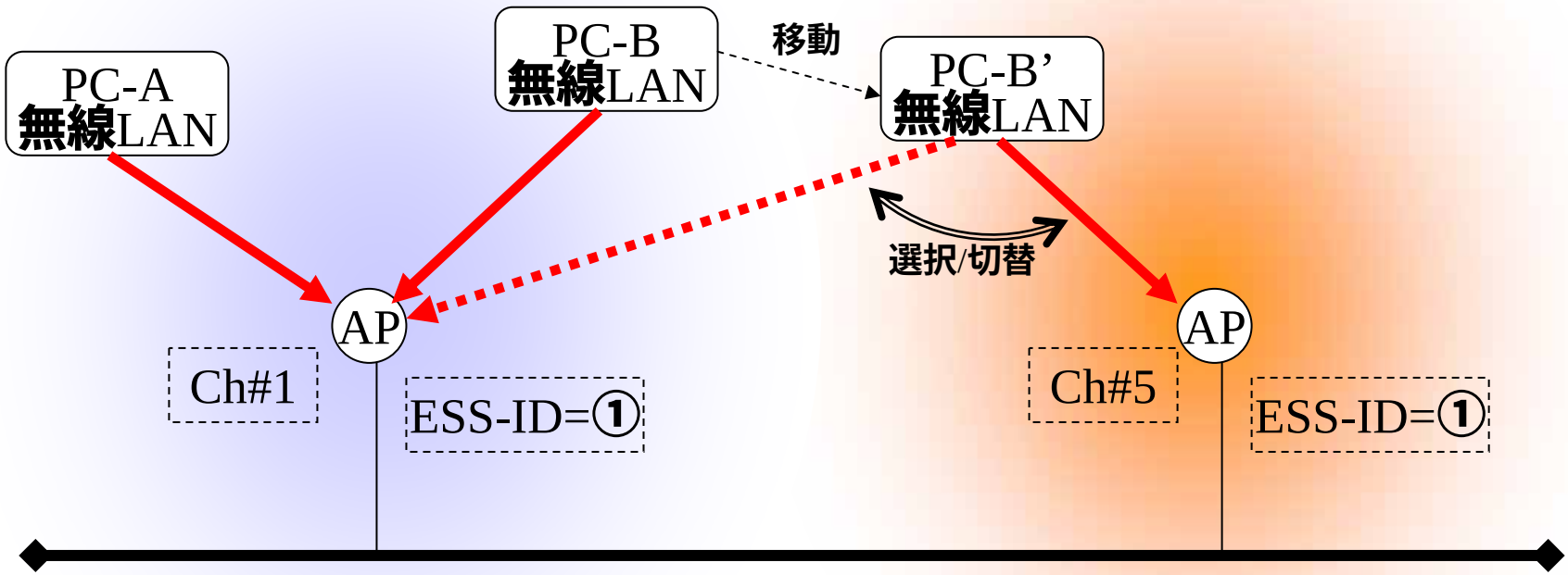
無線チャネルとESS-ID



[複数のアクセスポイント]

- 複数のアクセスポイント置く場合には、アクセスポイントで使用するチャネルを変更する。1～14のチャネルが重なり合っているため
- 異なるネットワークにそれぞれアクセスポイントを置く場合には、ESS-IDという識別子を利用して区別する。

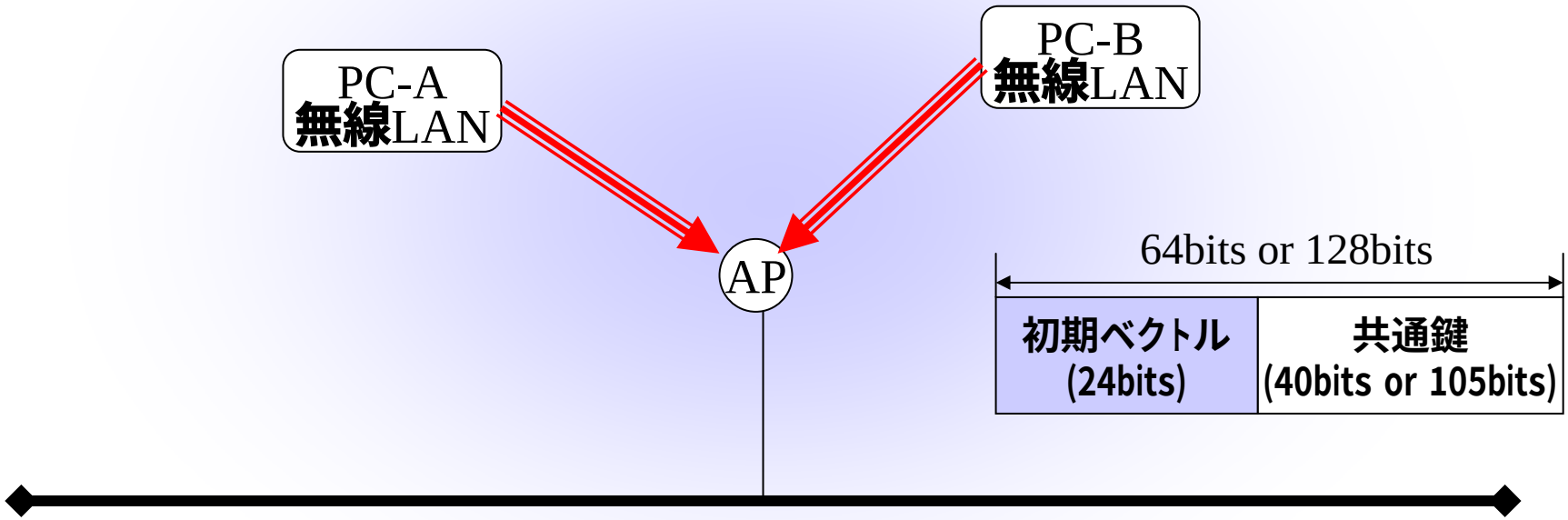
ローミング



[複数のアクセスポイント]

・同じネットワークに属する複数のアクセスポイントが設置されている場合には、条件の良いアクセスポイントが選ばれる。

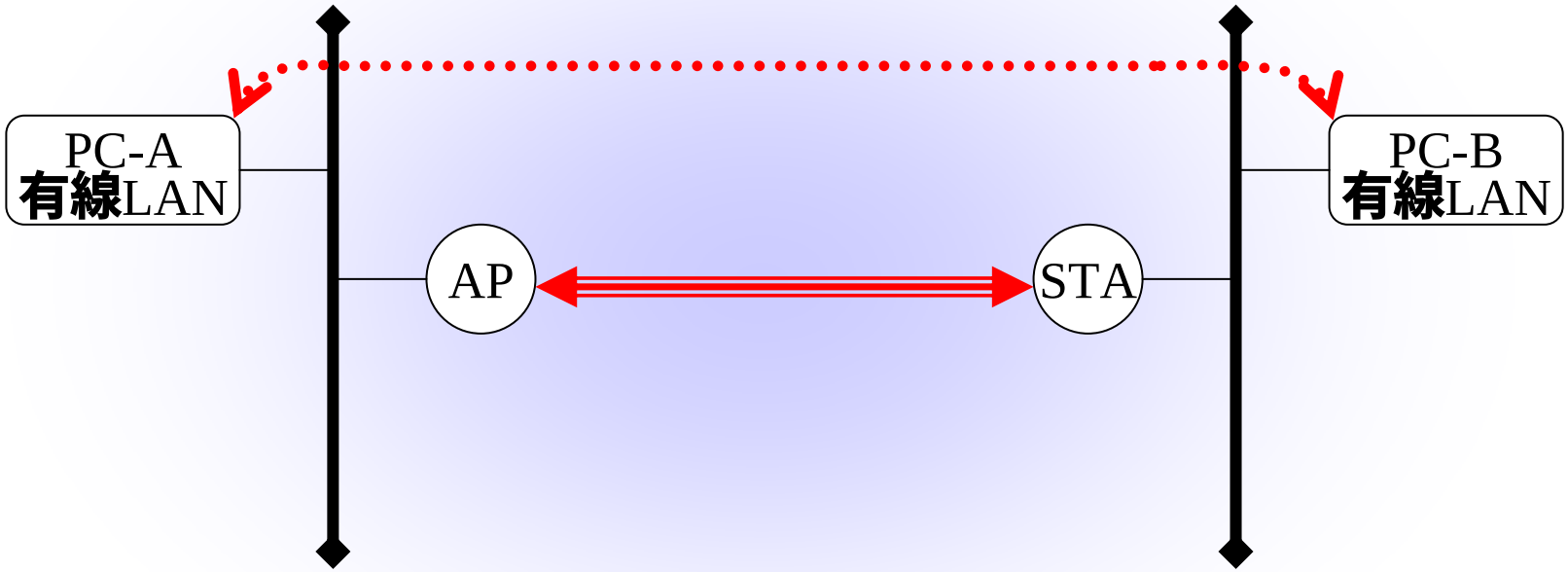
WEP



WEP: Wired equivalent privacy

- 認証と暗号を使って有線LAN並みのセキュリティを確保するためのしくみ
- 64ビットと128ビットがある。

無線ブリッジ



- ひとつのネットワークとして運用したい2つの有線LANを無線LANで繋ぐしくみ
- WDS(wireless distribution system)機能、または、ベンダーに依存する機能

データリンクなど
～知識の整理～

●イーサネットのフレームフォーマット
●PPPのフレームフォーマット
●PPP通信の概念
●PPPの役割
●PPPoEのフレームフォーマット
●PPPoEの役割(PPPoEクライアントとルーター)

PPPのフレームフォーマット

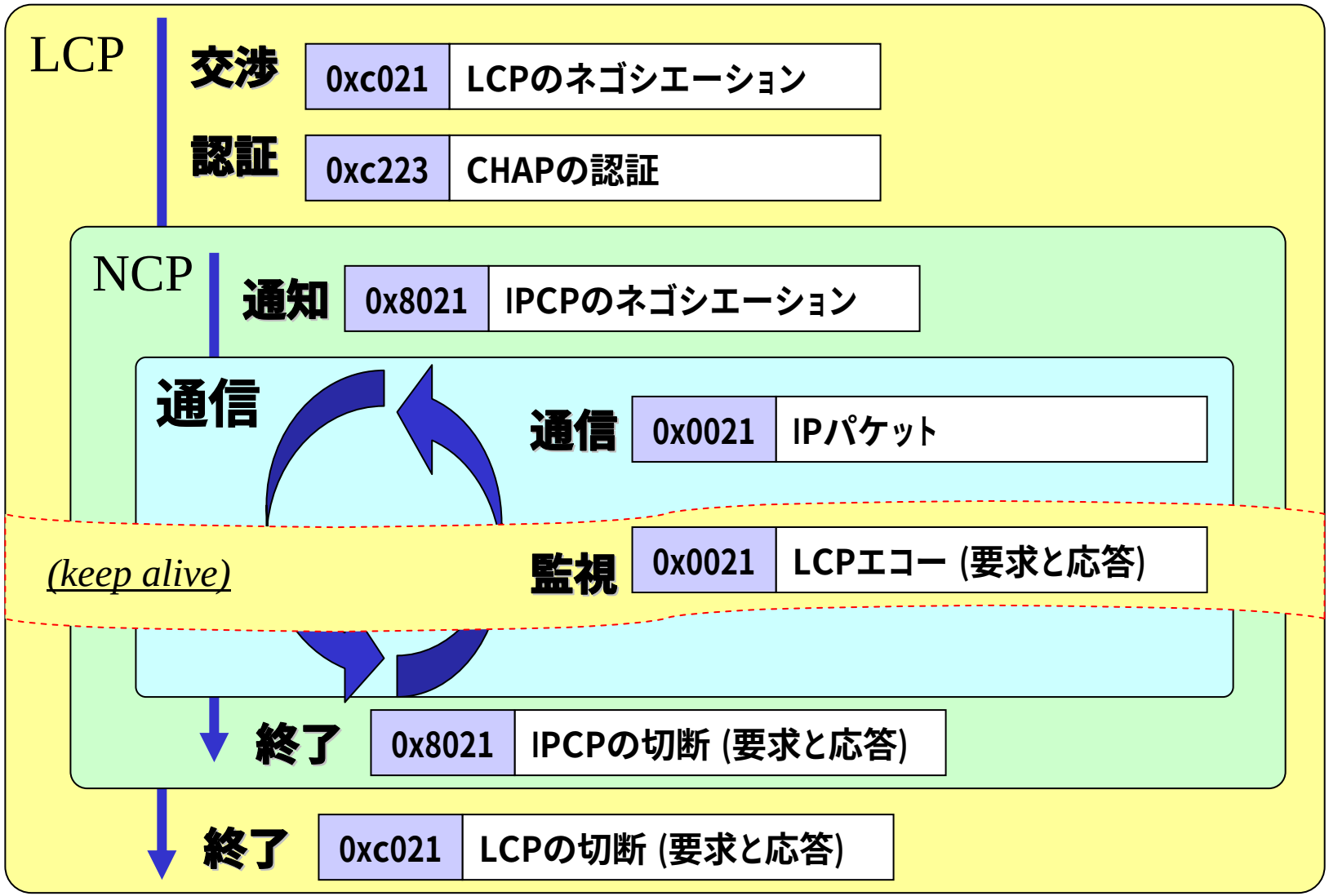
アプリケーション
TCP
IP
PPP
ISDN

PPPフレームフォーマット (cf.HDLC)

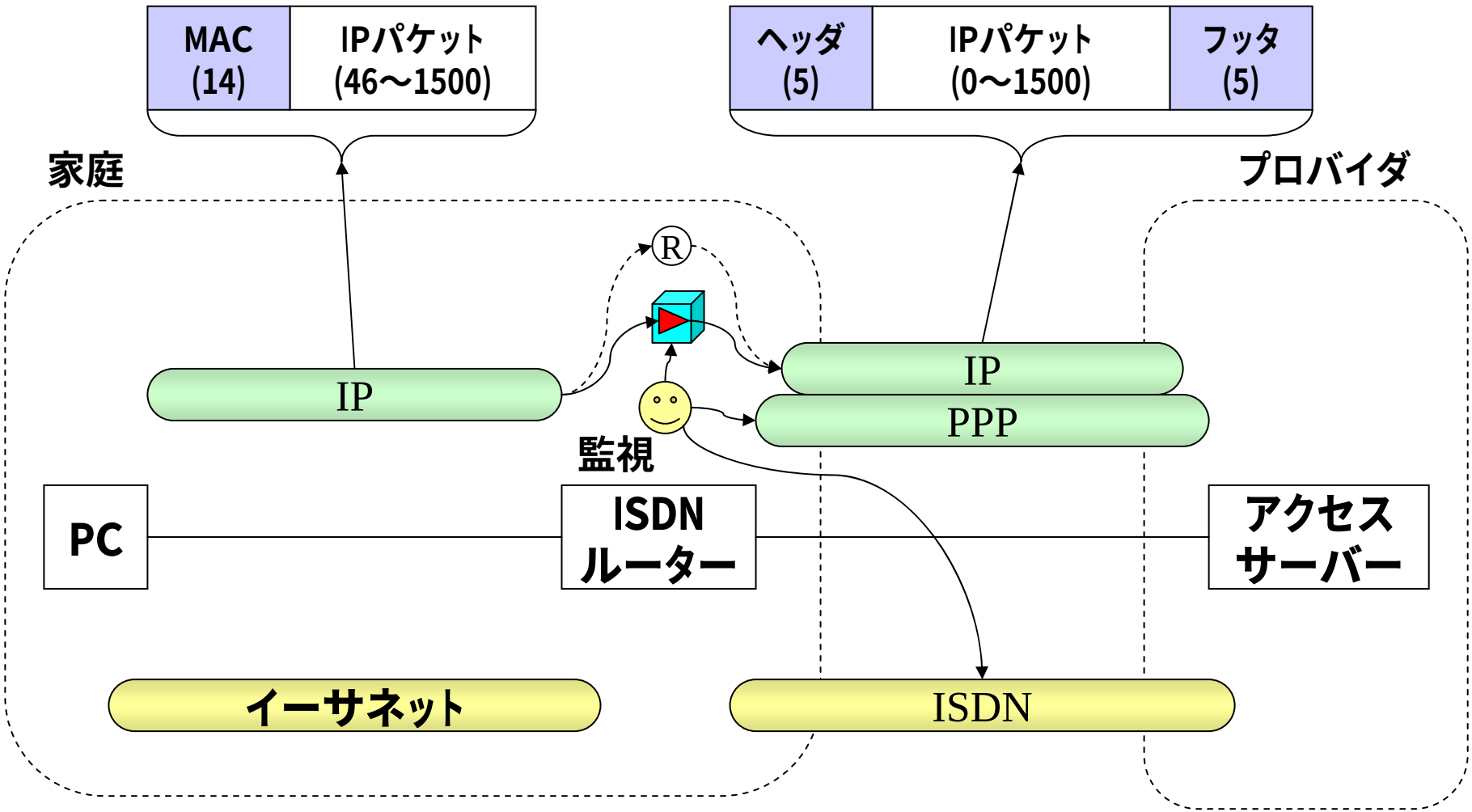
フラグ (1) 01111110	アドレス (1) 11111111	制御 (1) 00000011	タイプ (2)	IPパケット (0～1500)	FCS (4)	フラグ (1) 01111110

c021	LCP	LCPのネゴシエーション情報
c223	LCP	認証情報
8021	NCP	IPCPのネゴシエーション情報
0021	通信	IPパケット

PPP通信の概念

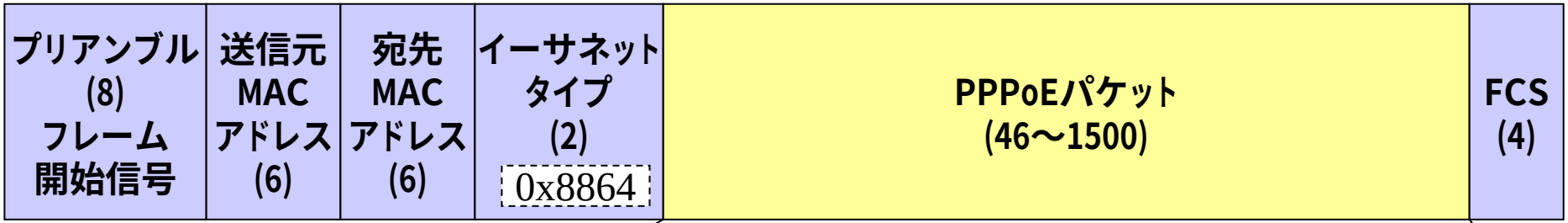


PPPの役割

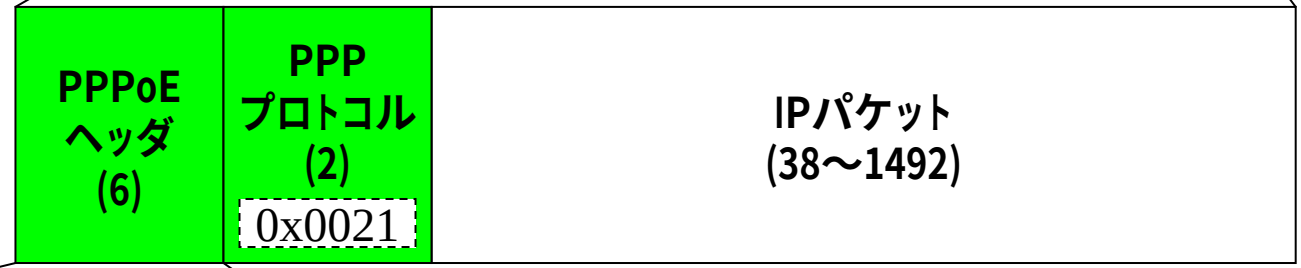


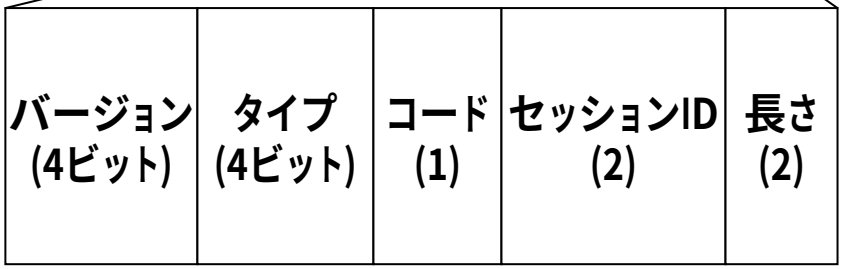
PPPoEのフレームフォーマット

Ethernetフレームフォーマット

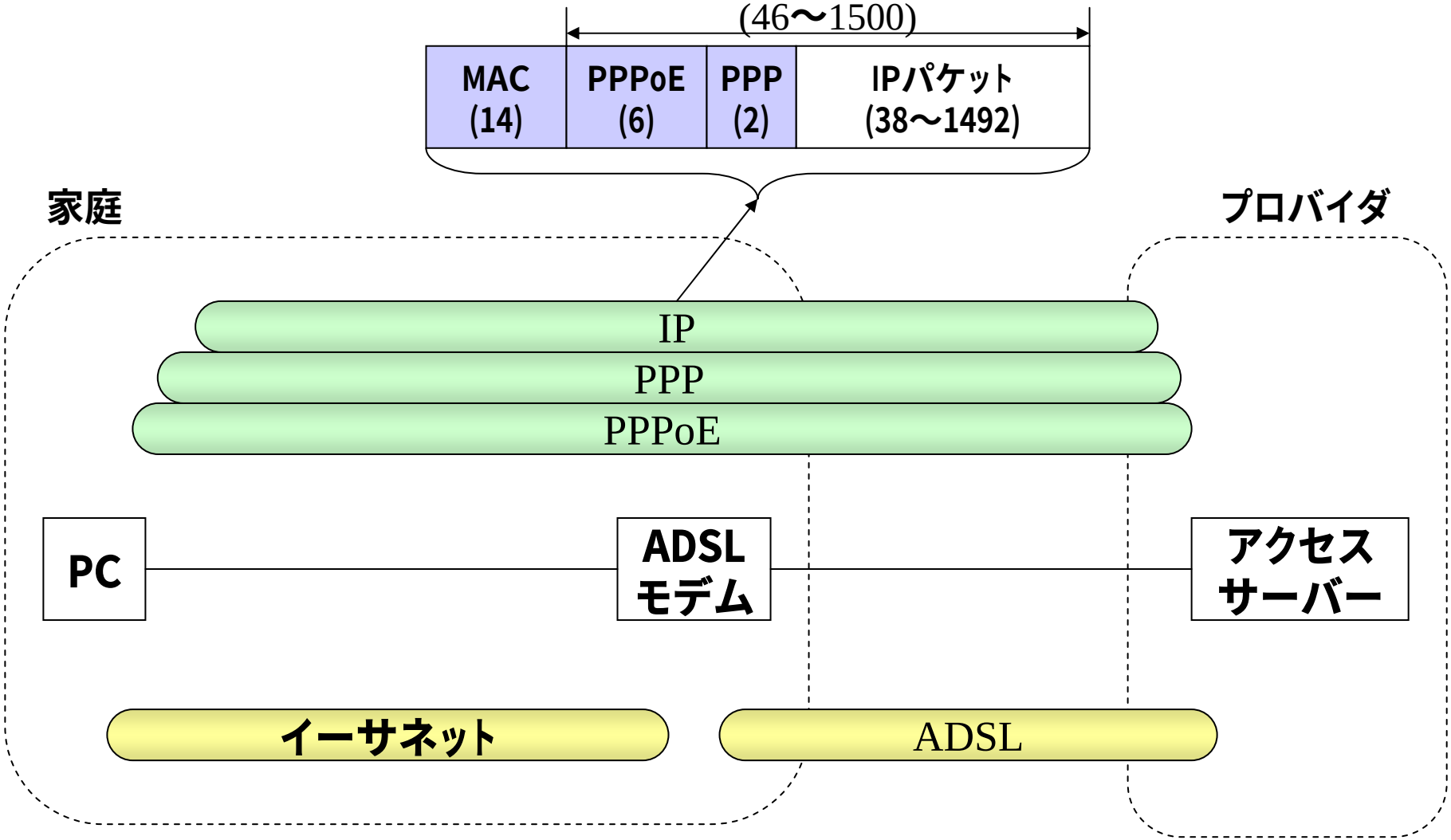


PPPoEフレームフォーマット

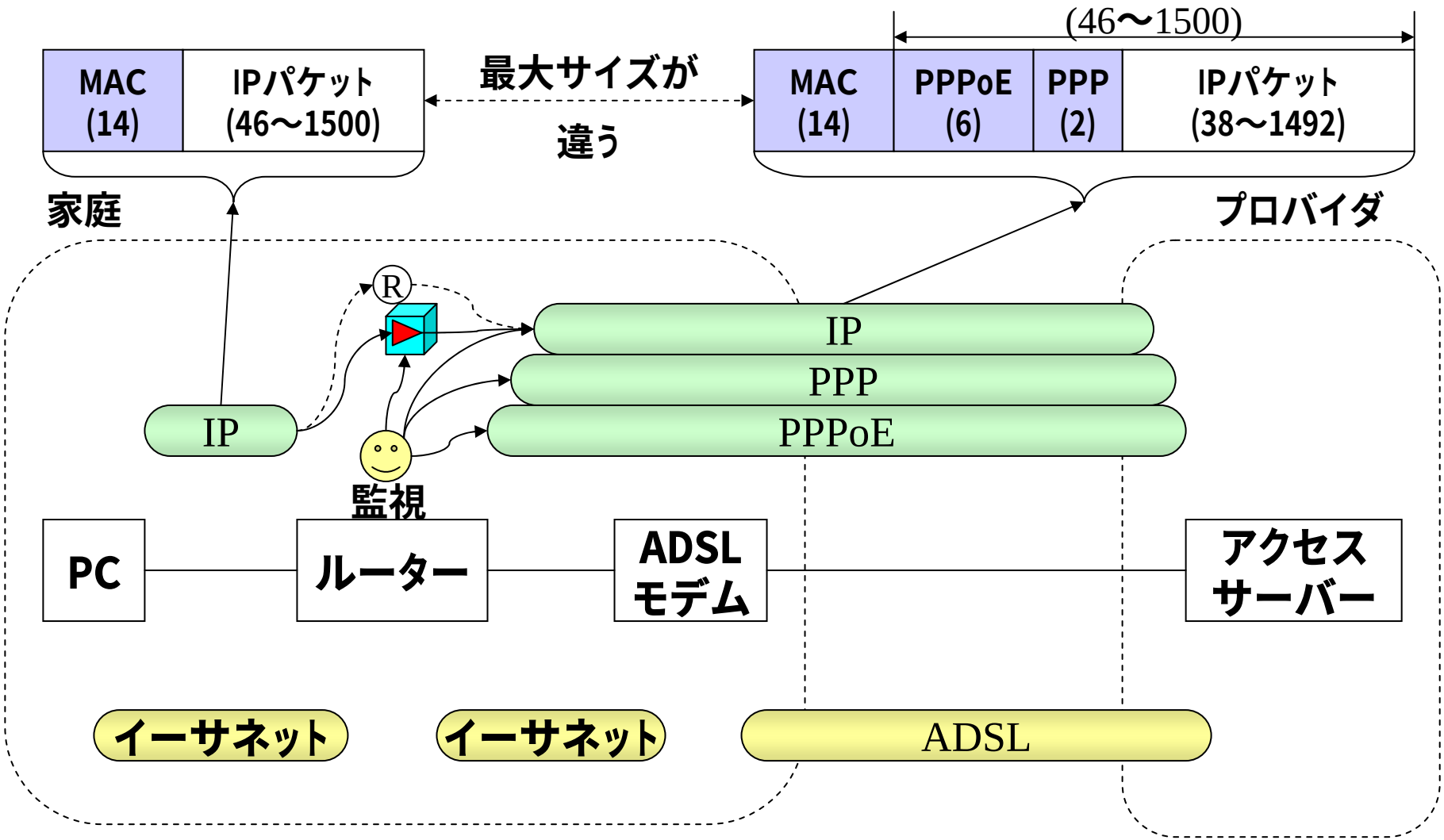




PPPoEの役割(PPPoEクライアント)



PPPoEの役割(ルーター使用)

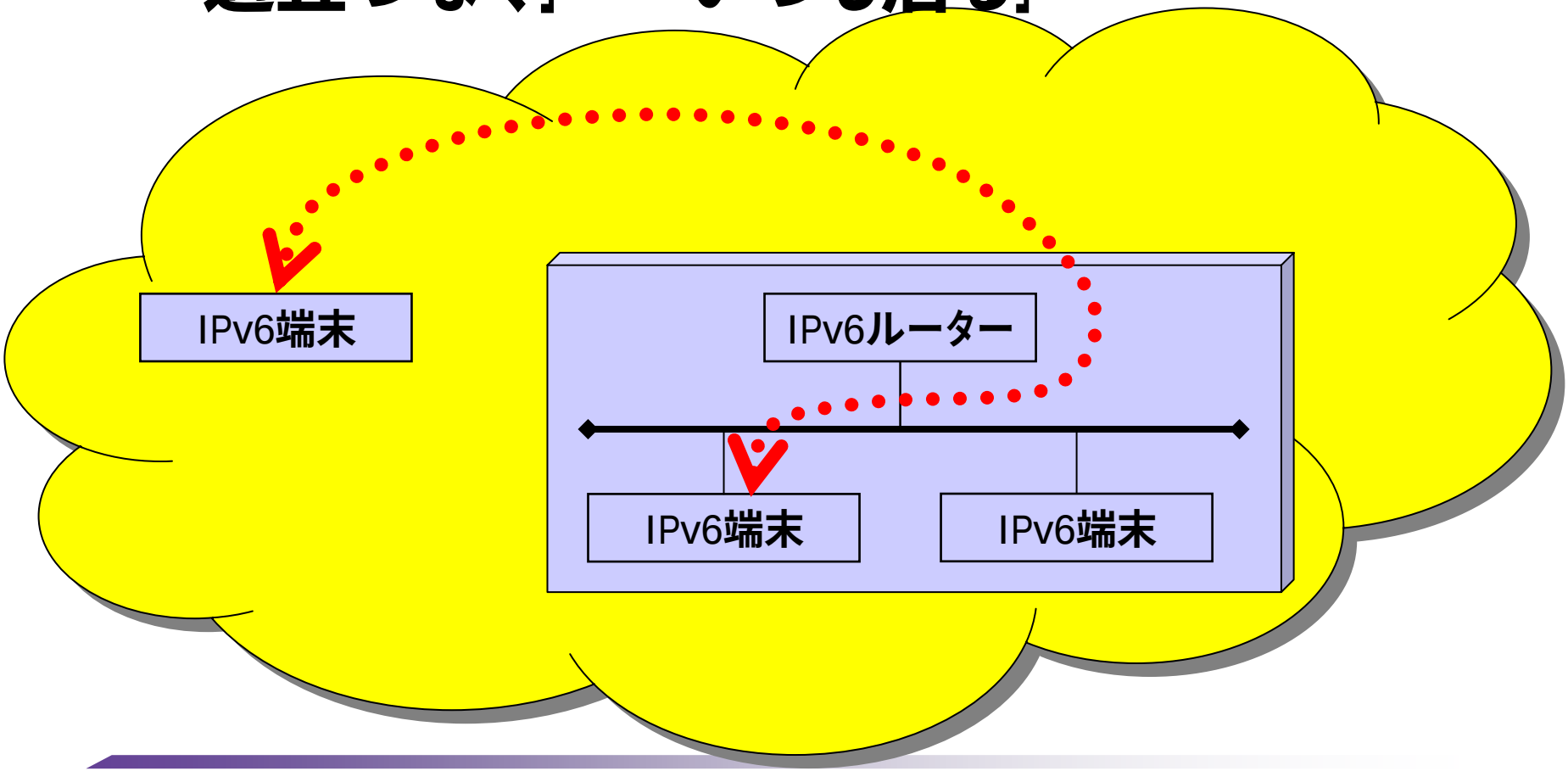


IPv6
～知識の整理～

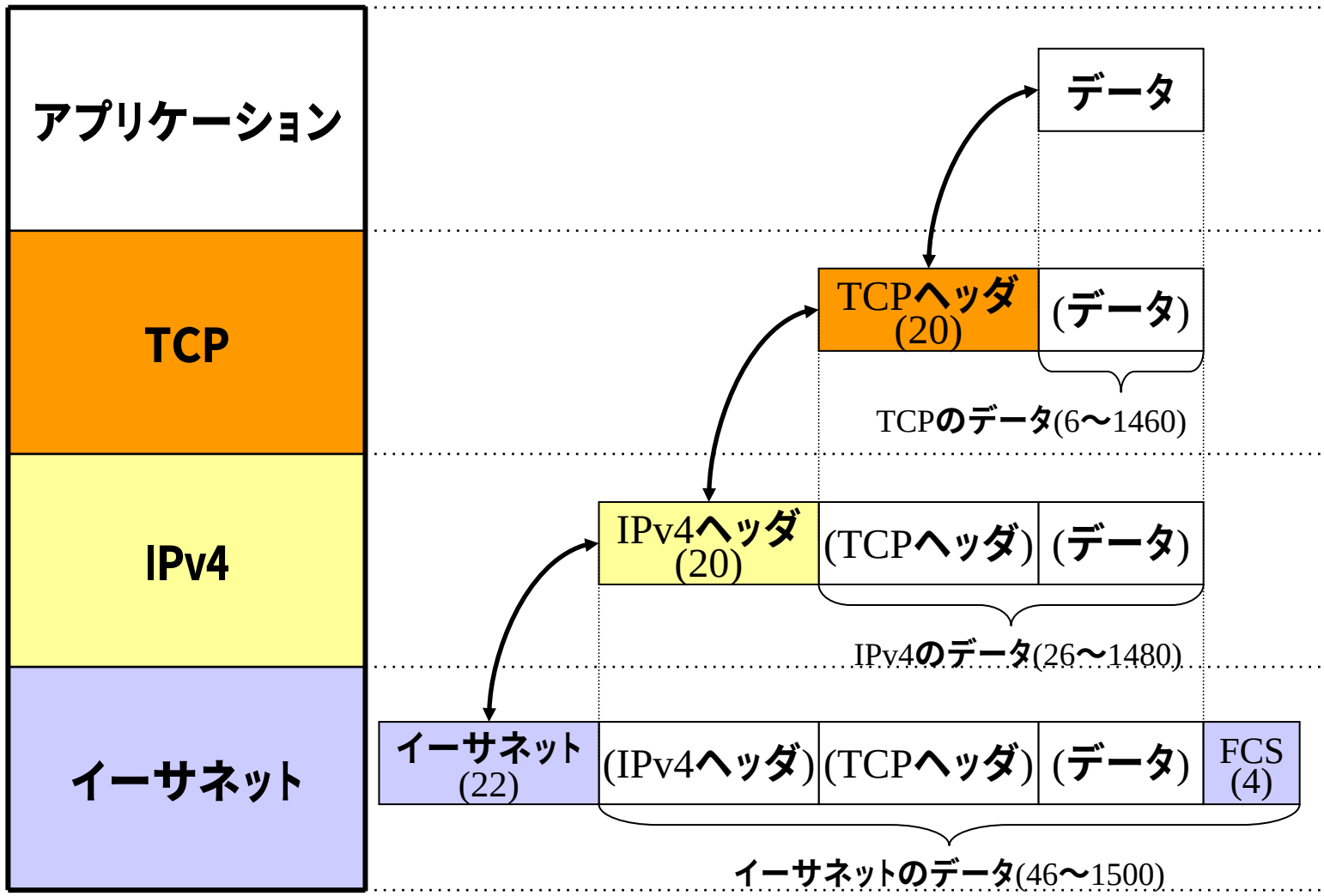
家庭におけるIPv6

家一軒がインターネットの一部になる。

・「適宜つなぐ」→「いつも居る」

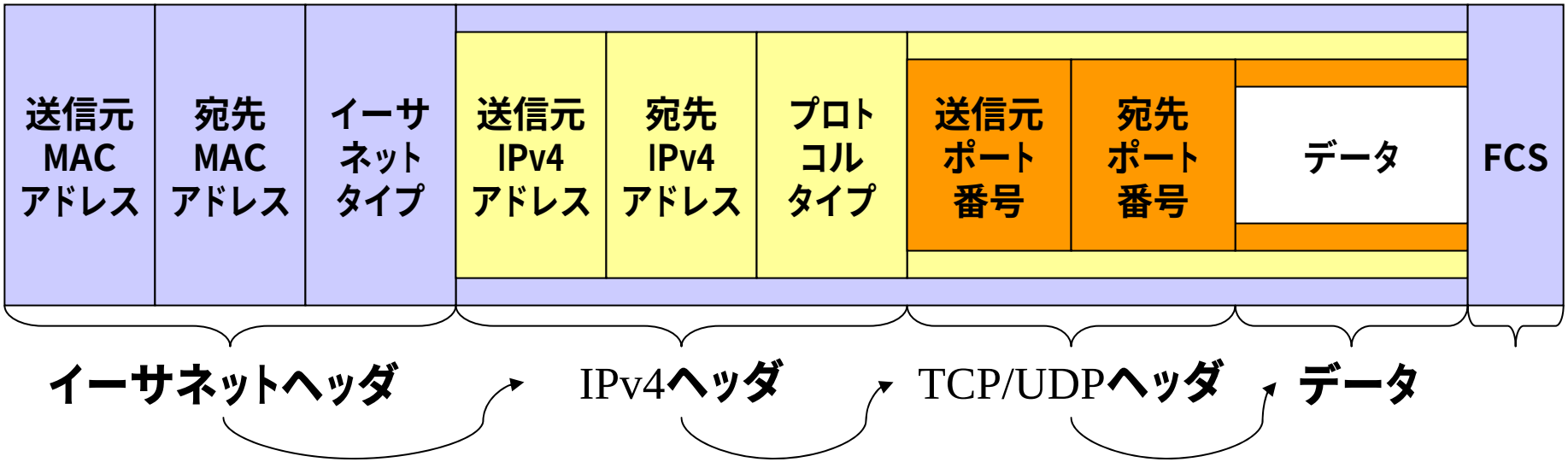


IPv4パケットと階層構造

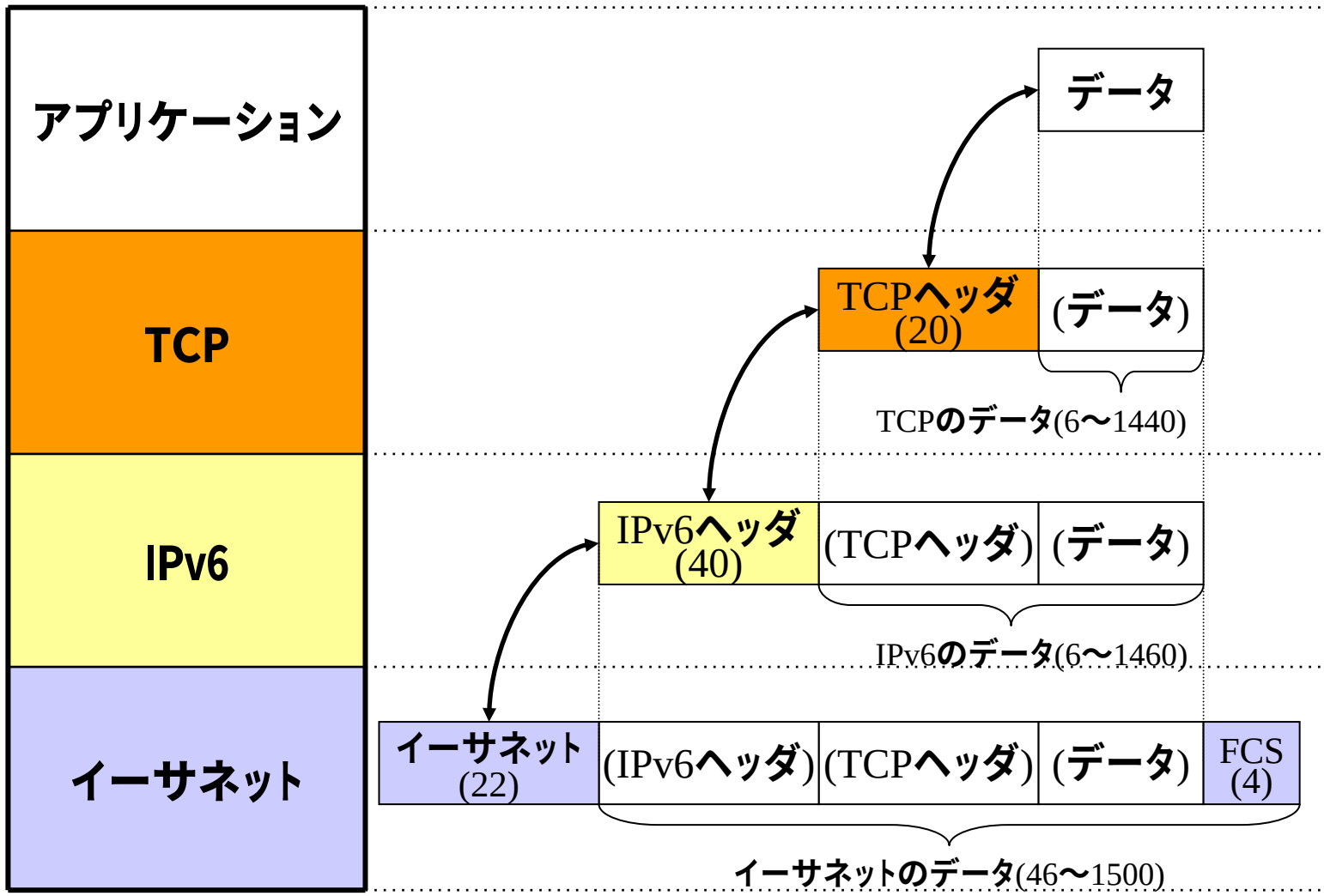


TCP/IPの階層モデル

イーサネットを流れるIPv4パケット

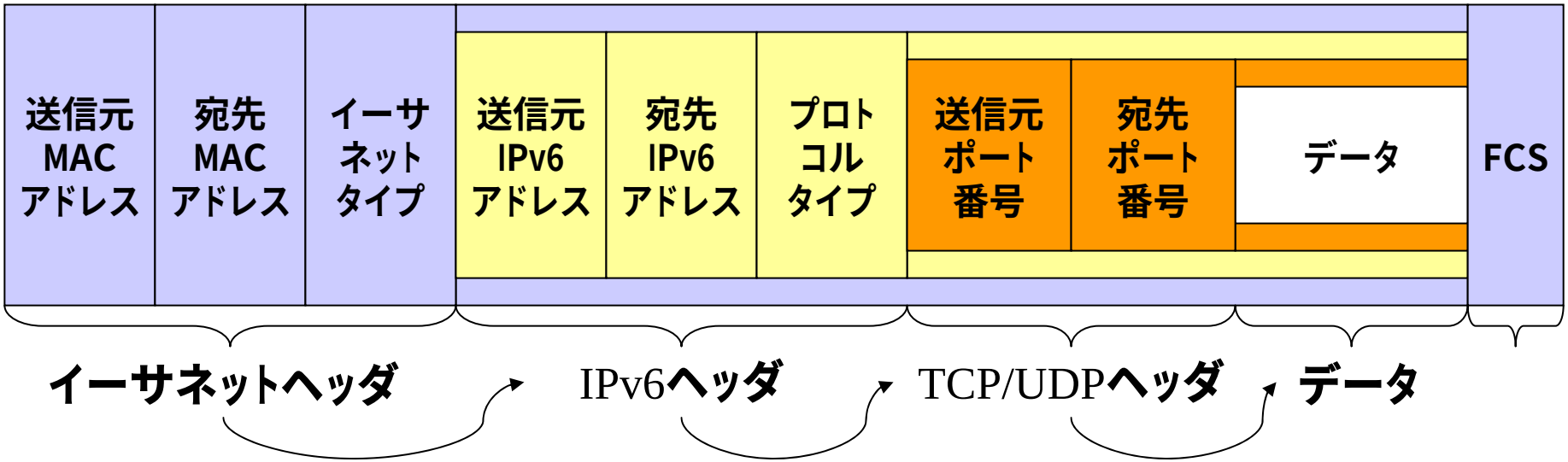


IPv6パケットと階層構造

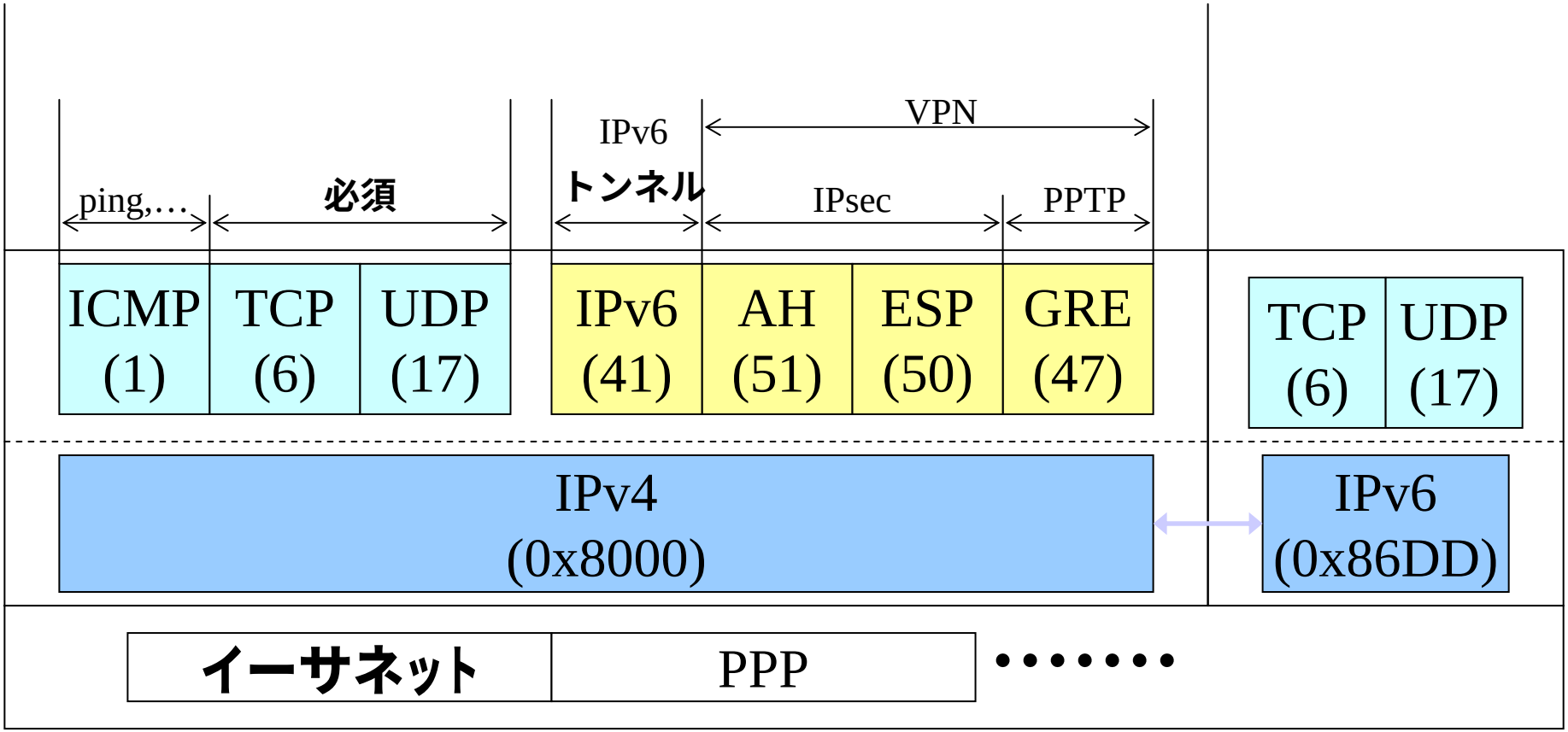


TCP/IPの階層モデル

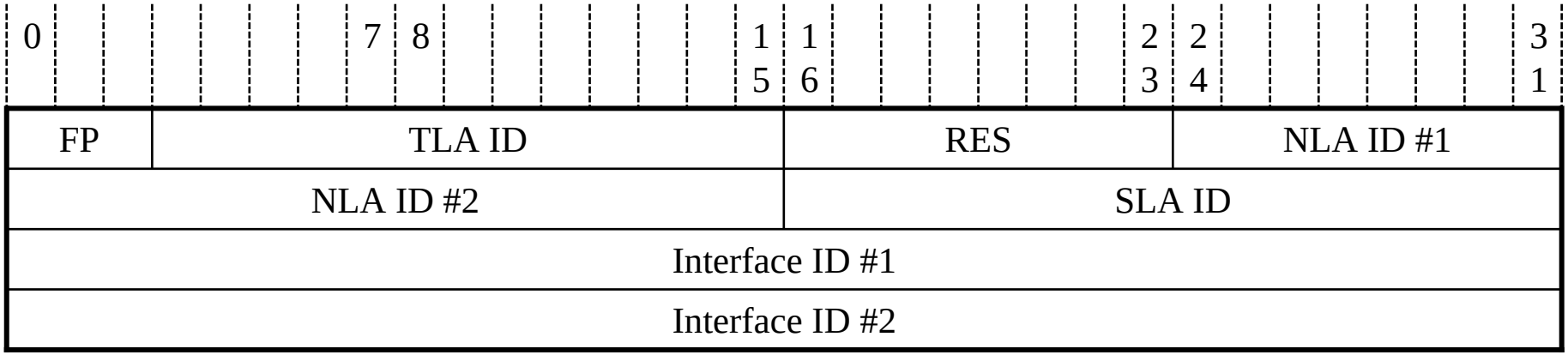
イーサネットを流れるIPv6パケット



IPv4/IPv6と上位層プロトコル



IPv6アドレス



(16進数表記)

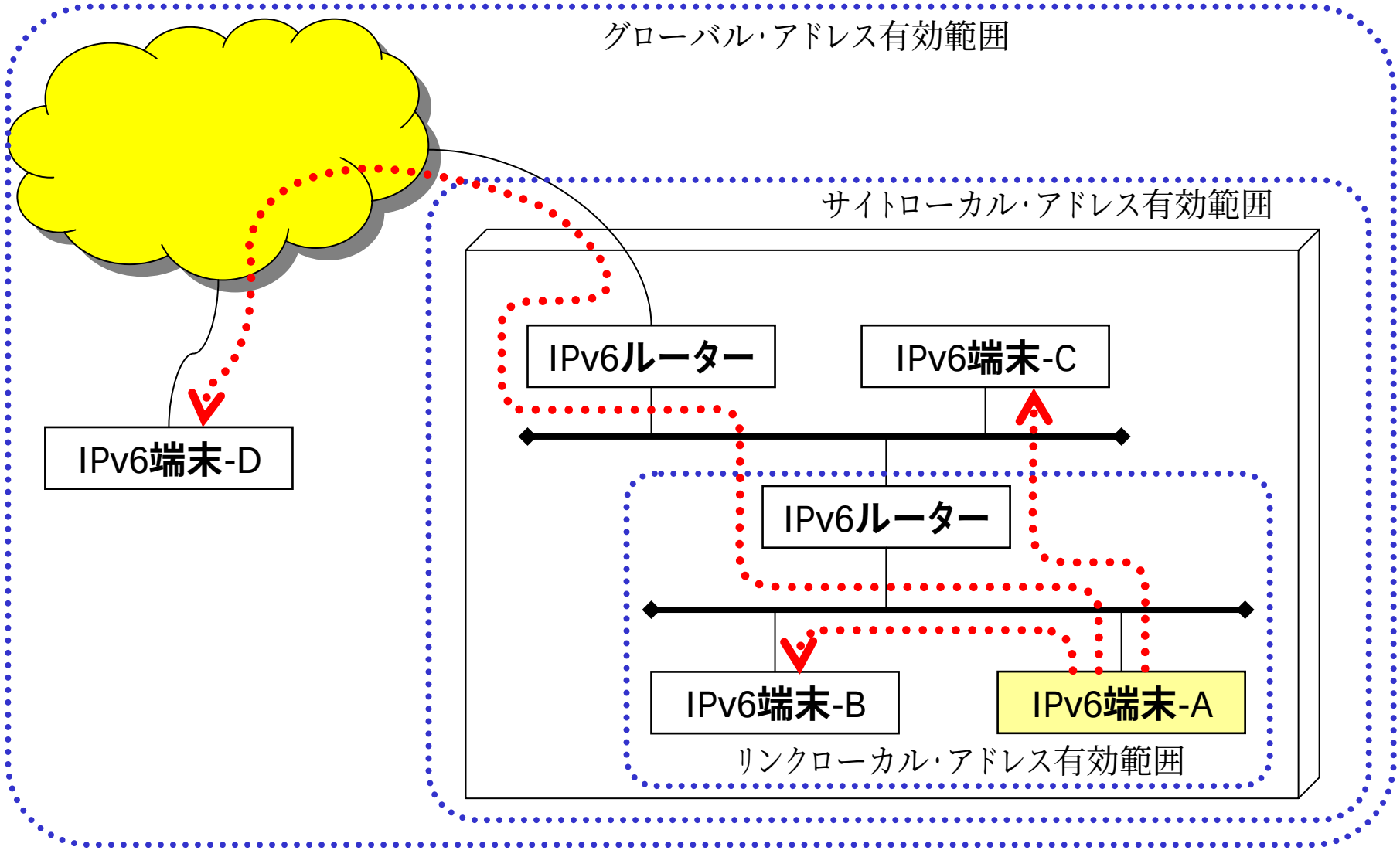
XXXX：XXXX：XXXX：XXXX：XXXX：XXXX：XXXX：XXXX

IPv6アドレスの種類

ユニキャスト・アドレス	グローバル・アドレス		0000000000 ～	・・・ ・	00000000 ～
		割り当て中	0010000000 ～ 0011111111	・・・ ・	00000000 ～ 11111111
			～	・・・	～
			0100000000 ～ 0111111111	・・・ ・	00000000 ～ 11111111
			～	・・・	～
	リンクローカル・アドレス fe80:…		1111111010 ～ 1111111010	・・・ ・	00000000 ～ 11111111
	サイトローカル・アドレス fec0:…		1111111011 ～ 1111111011	・・・ ・	00000000 ～ 11111111
マルチキャスト・アドレス			1111111100 ～ 1111111111	・・・ ・	00000000 ～ 11111111

他) エニーキャストアドレス、IPv4互換アドレス

IPv6アドレスの利用範囲



IPv6アドレスの用語

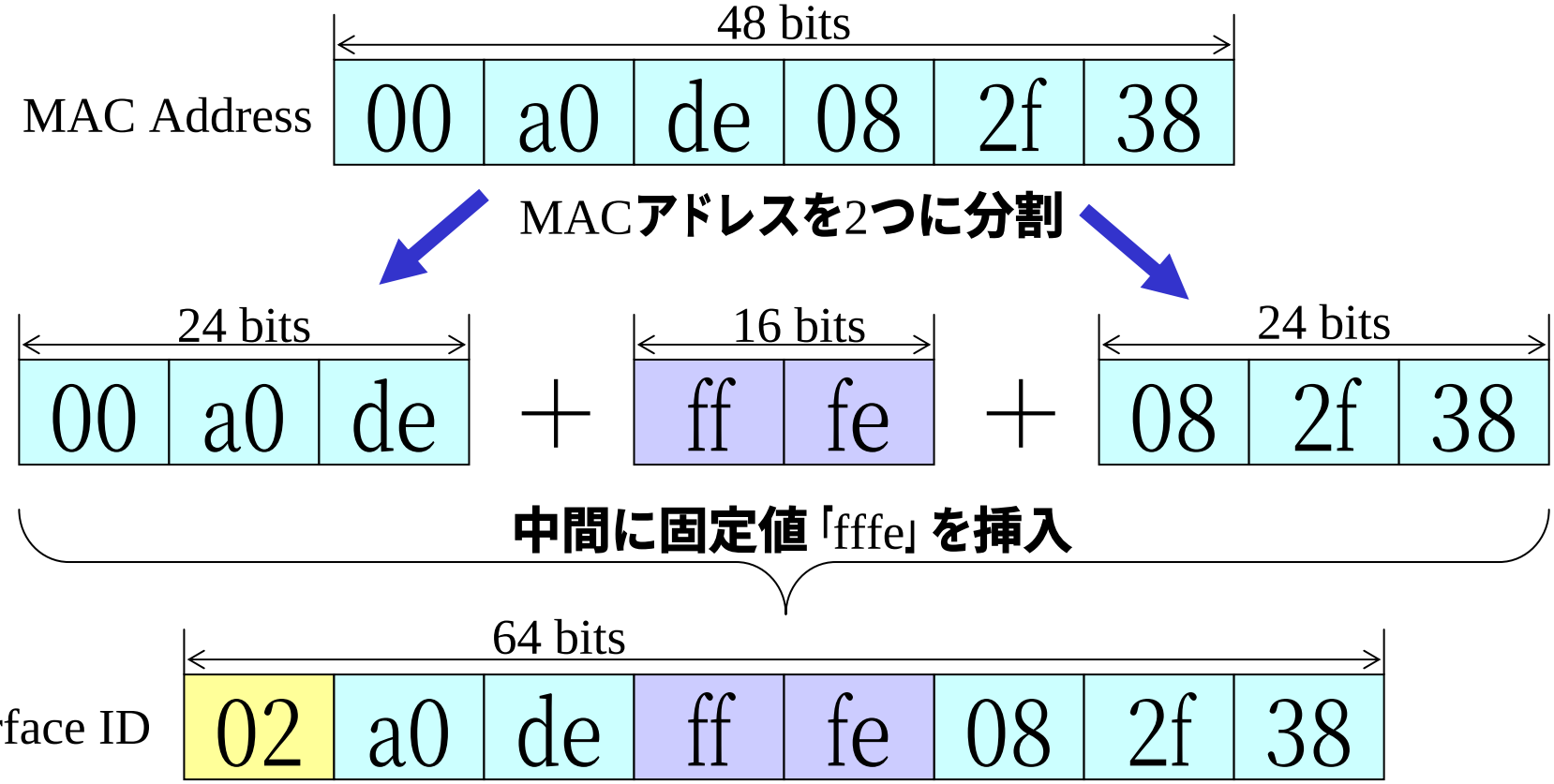
(16進数表記)

XXXX : XXXX : XXXX : XXXX : XXXX : XXXX : XXXX : XXXX

FP: アドレスフォーマット識別子
TLA ID: Top-Level Aggregation Identifier
(公共的にパケットを配送するサービス提供者)
RES: Reserved
NLA ID: Next-Level Aggregation Identifier
(TLAにパケットを配送してもらう組織の識別子)
SLA ID: Site-Level Aggregation Identifier
(組織内部のサブネットワークの識別子)
Interface ID: Interface Identifier (MACアドレス)

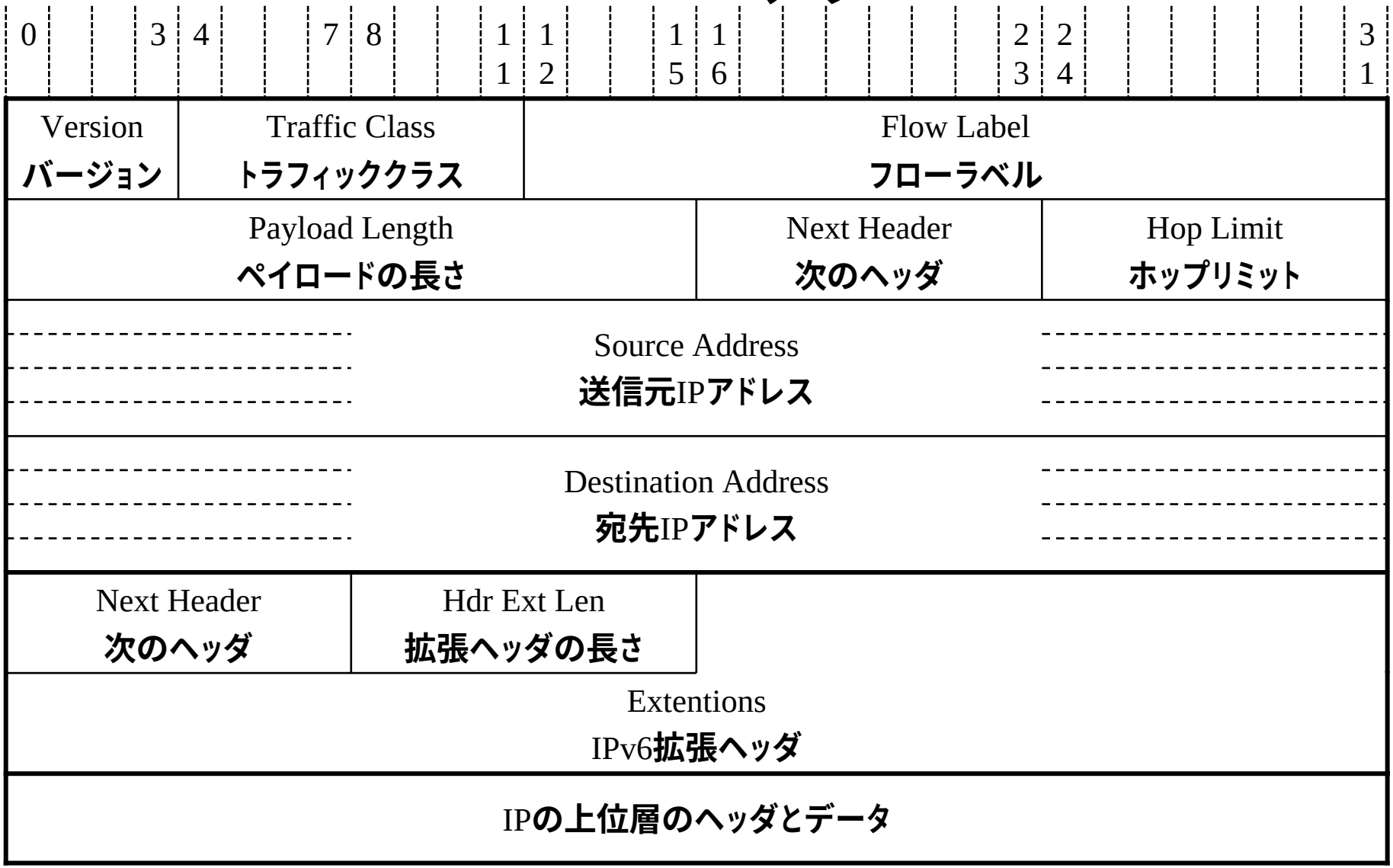
Interface ID

(MACアドレスから自動生成される情報…EUI-64という変換ルール)

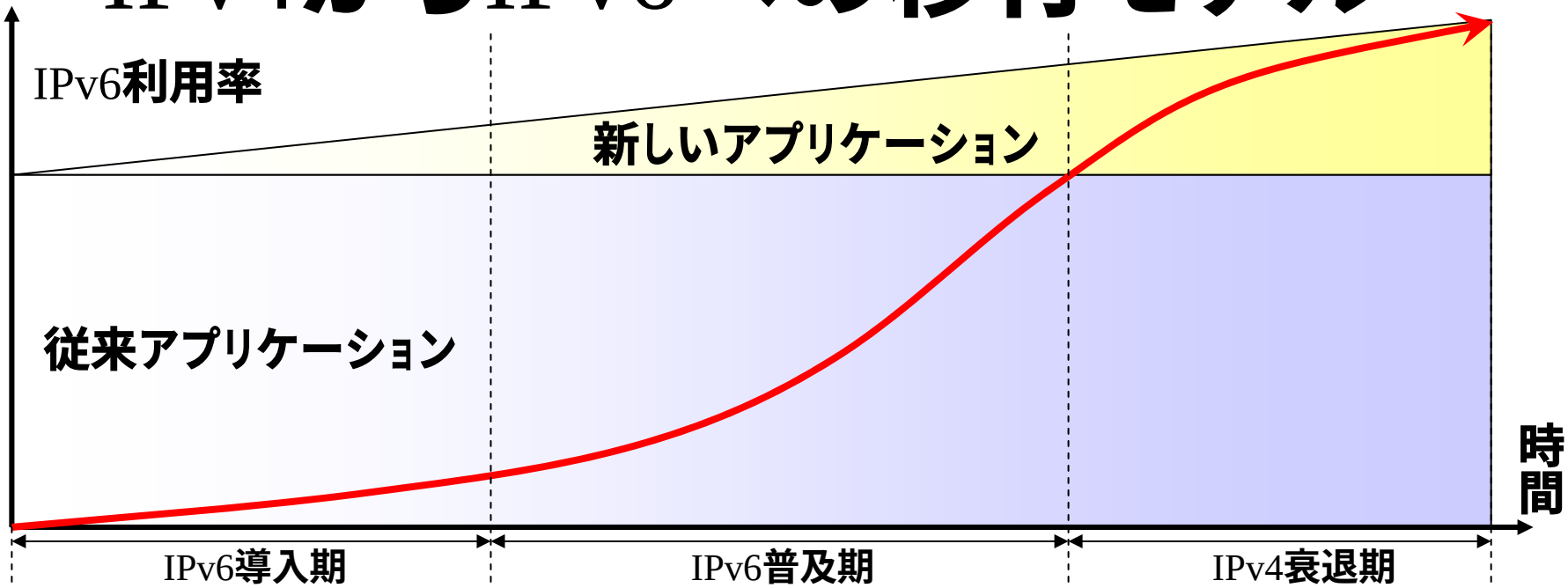


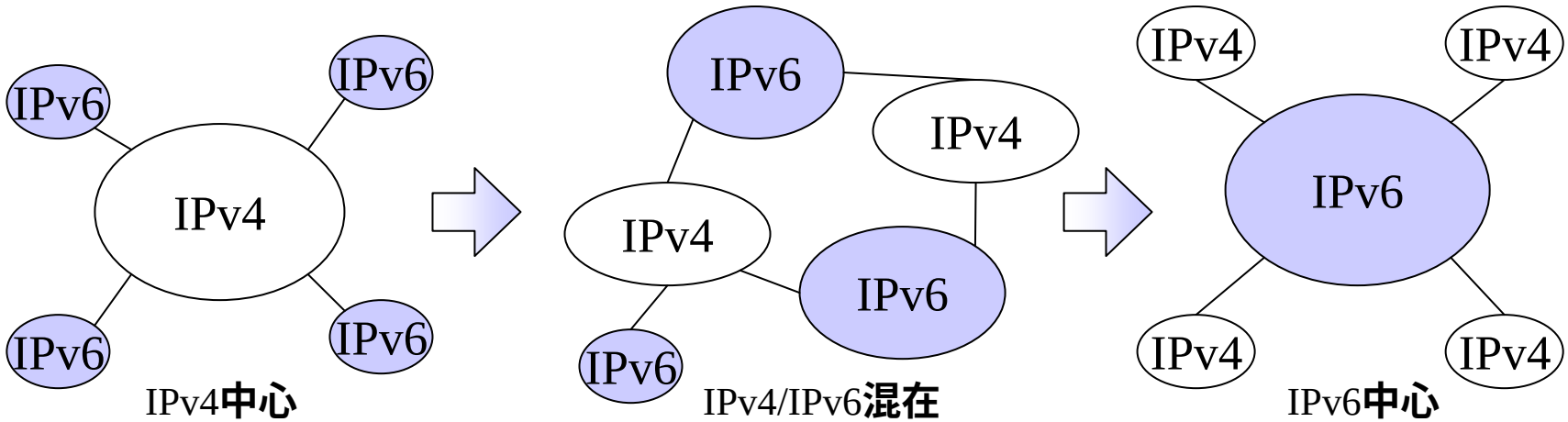
↑最初の1オクテットの最後の2ビットのみ値を反転

IPv6ヘッダ

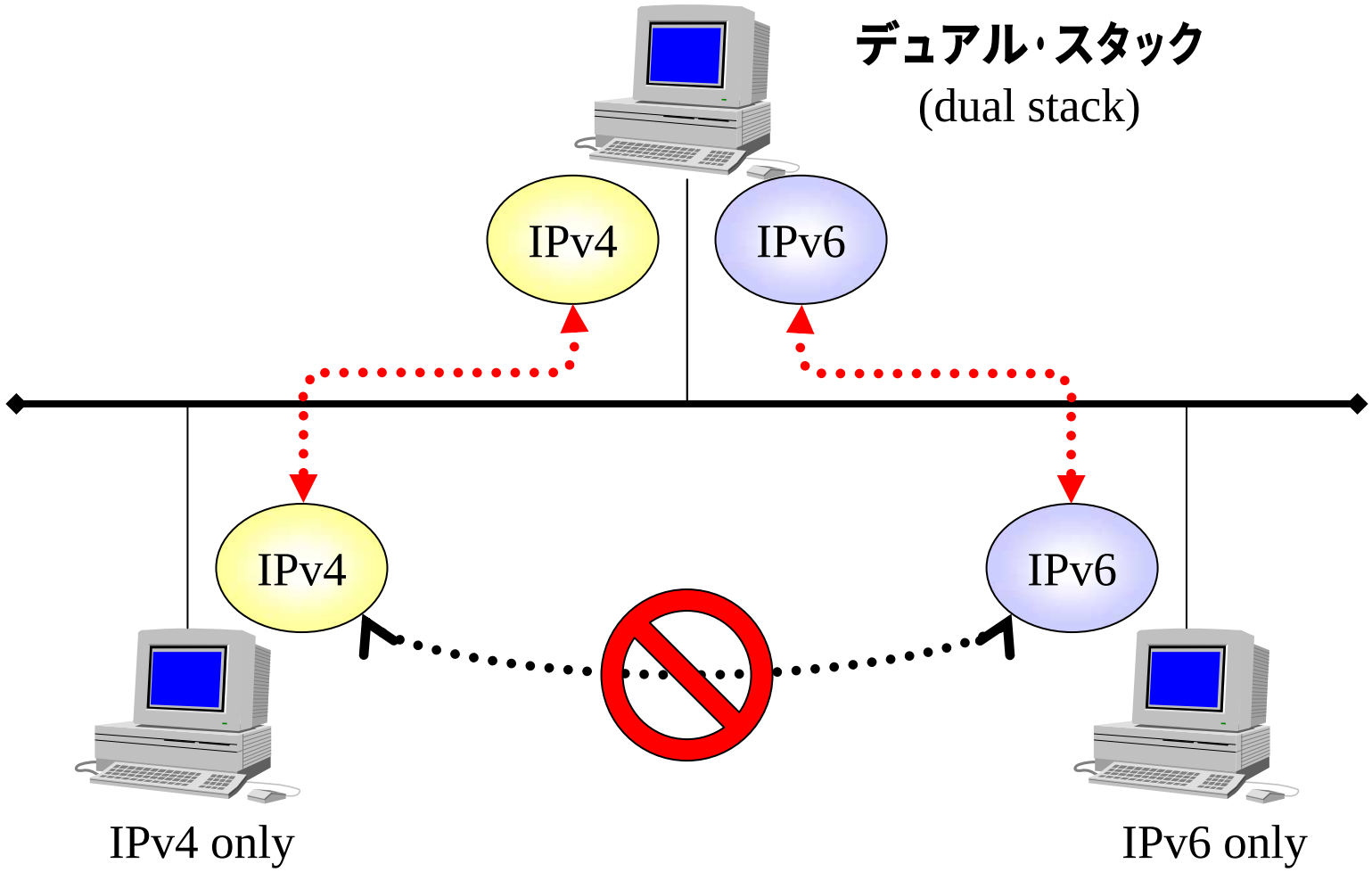


IPv4からIPv6への移行モデル

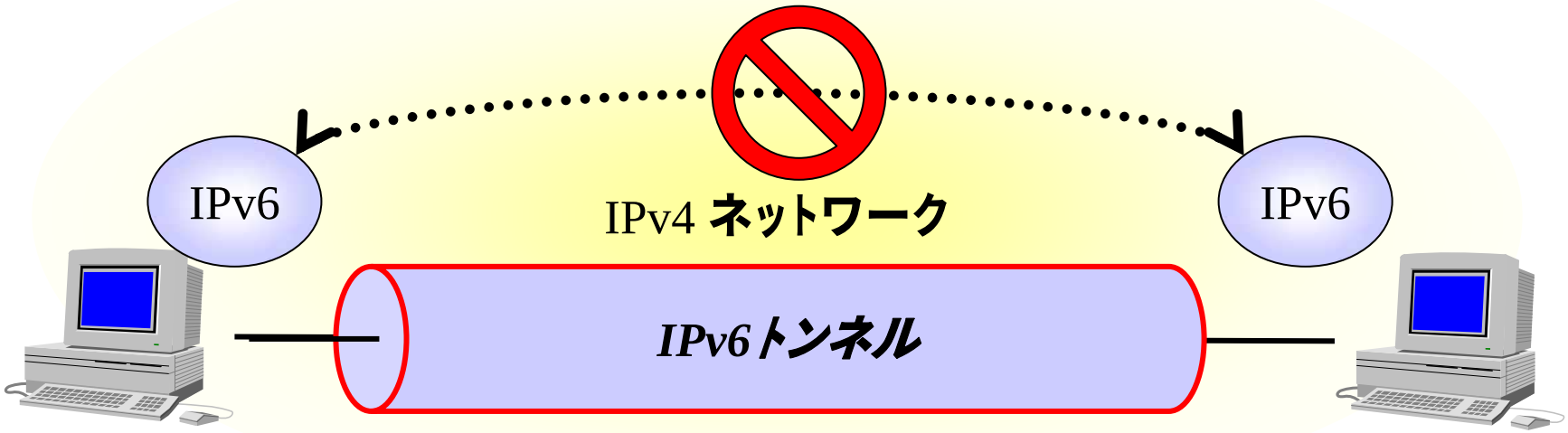




IPv4→IPv6移行技術(1)

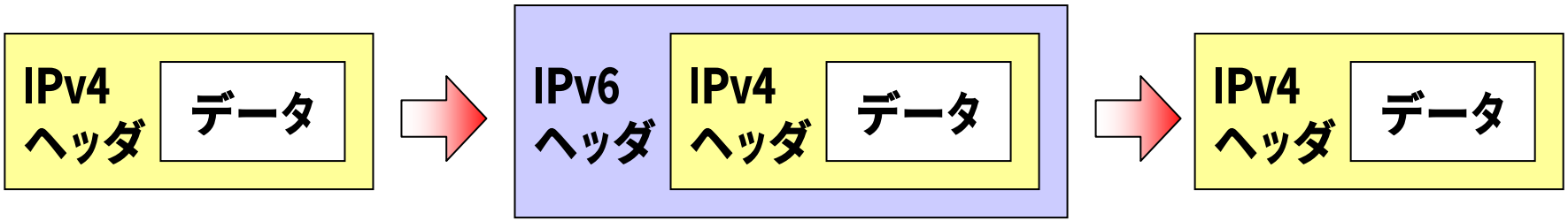


IPv4→IPv6移行技術(2)



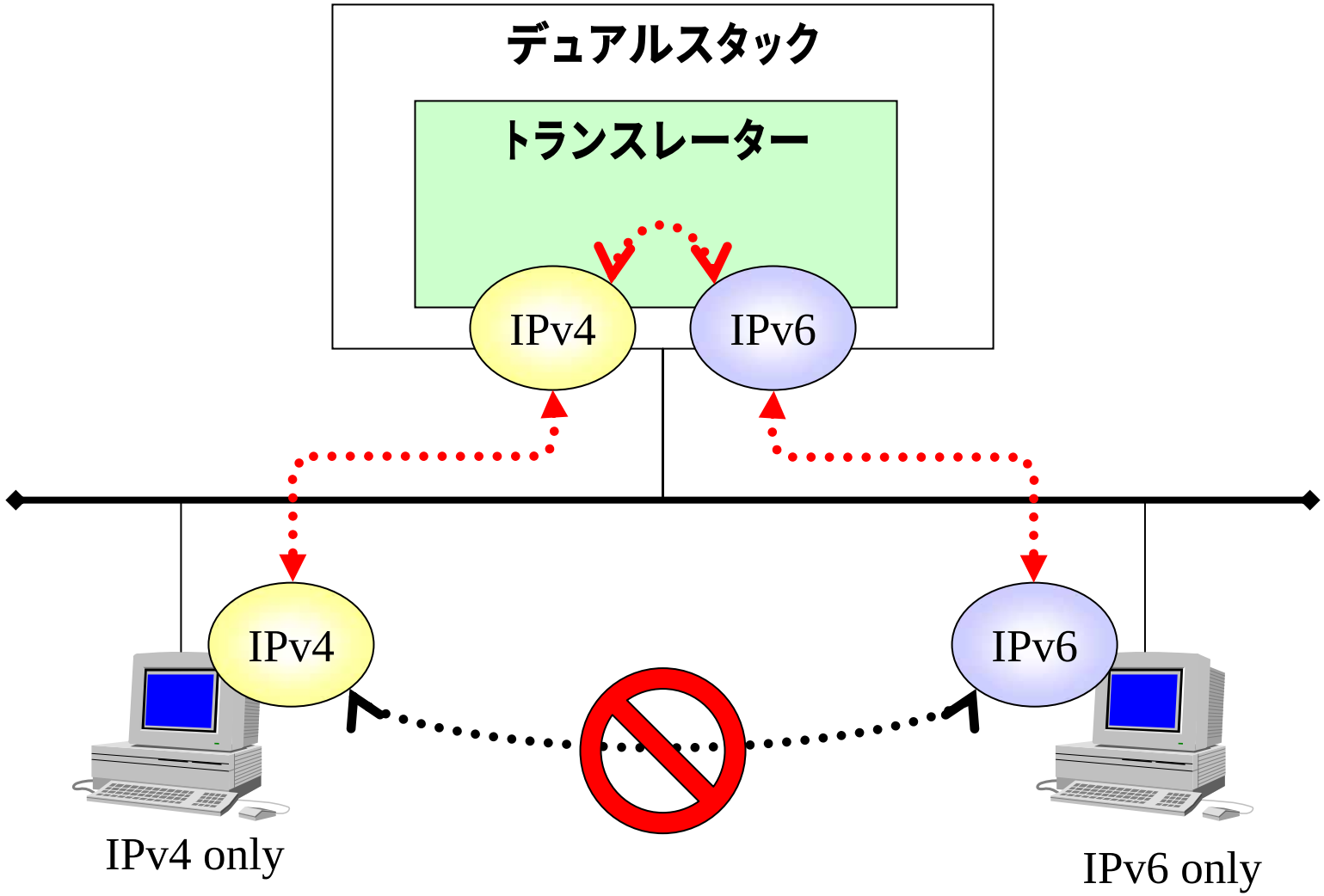
IPv4によるトンネリング
(IPv6パケットをIPv4でカプセル化)

IPv4→IPv6移行技術(3)

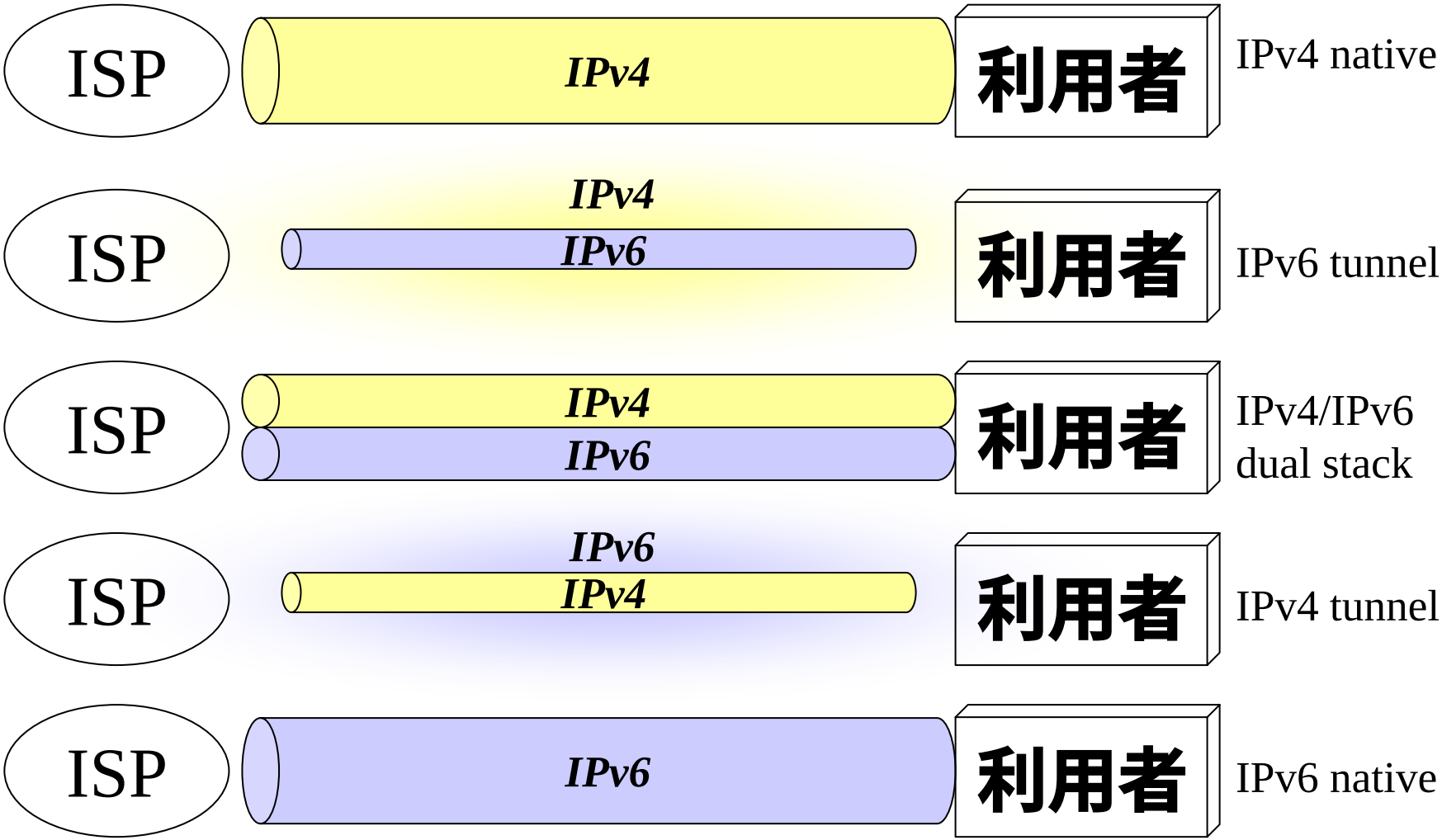


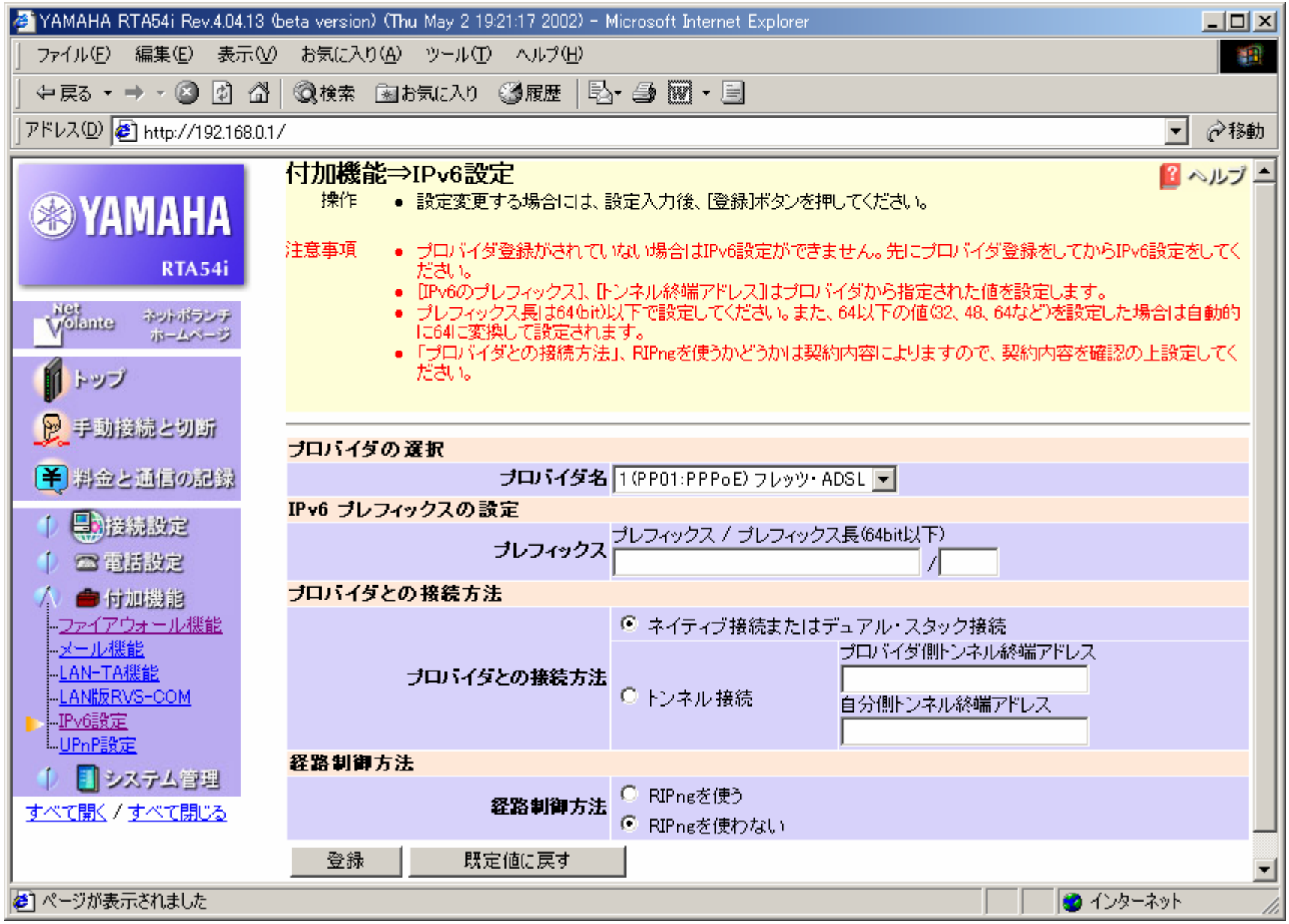
IPv6によるトンネリング
(IPv4パケットをIPv6でカプセル化)

IPv4→IPv6移行技術(4)



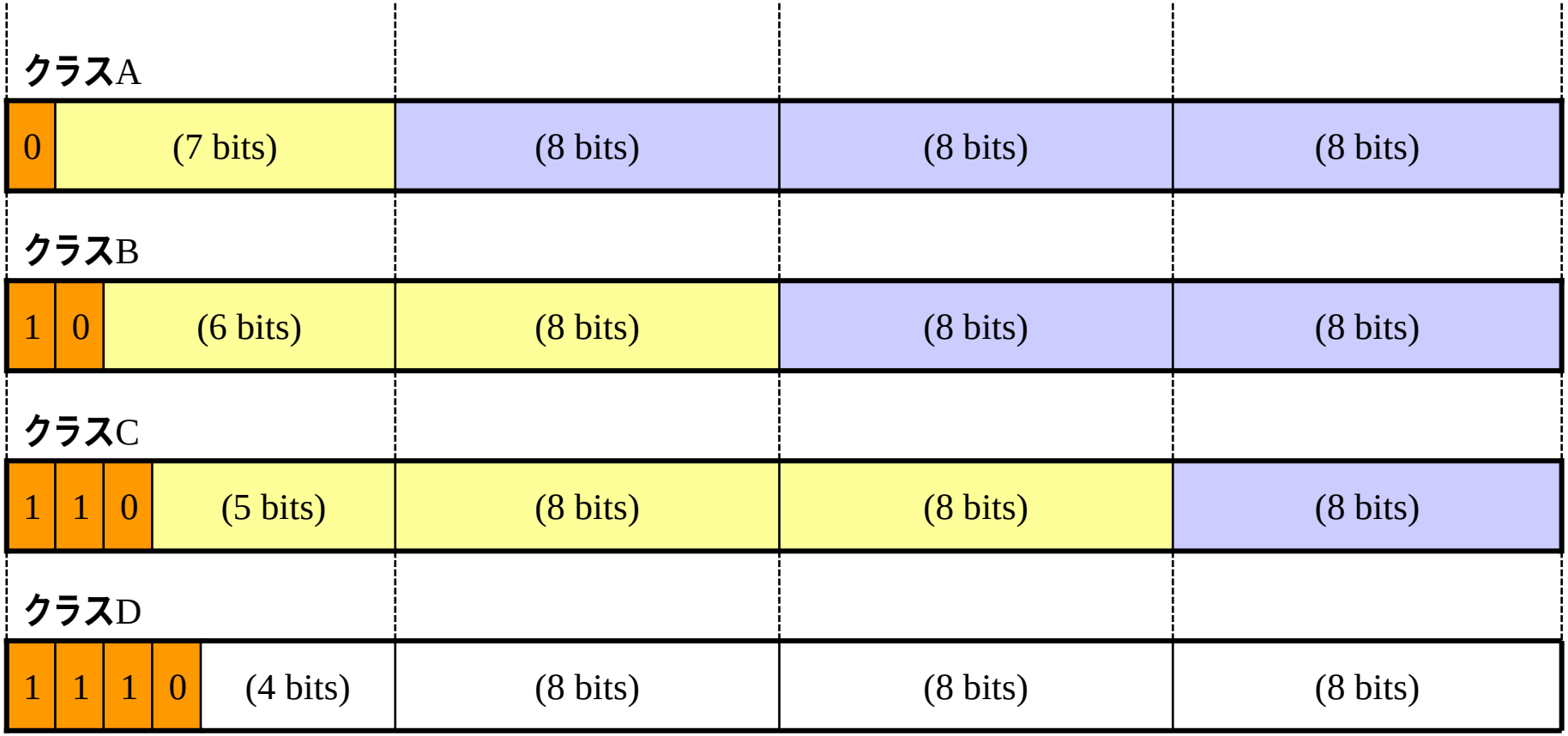
IPv6接続サービス





IPv4
～知識の整理～

IPv4アドレス



IPv4プライベート・アドレス

クラスA(10/8)

0	0	0	0	1	0	1	0	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

クラスB(172.16/12)

1	0	1	0	1	1	0	0	0	0	0	1	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

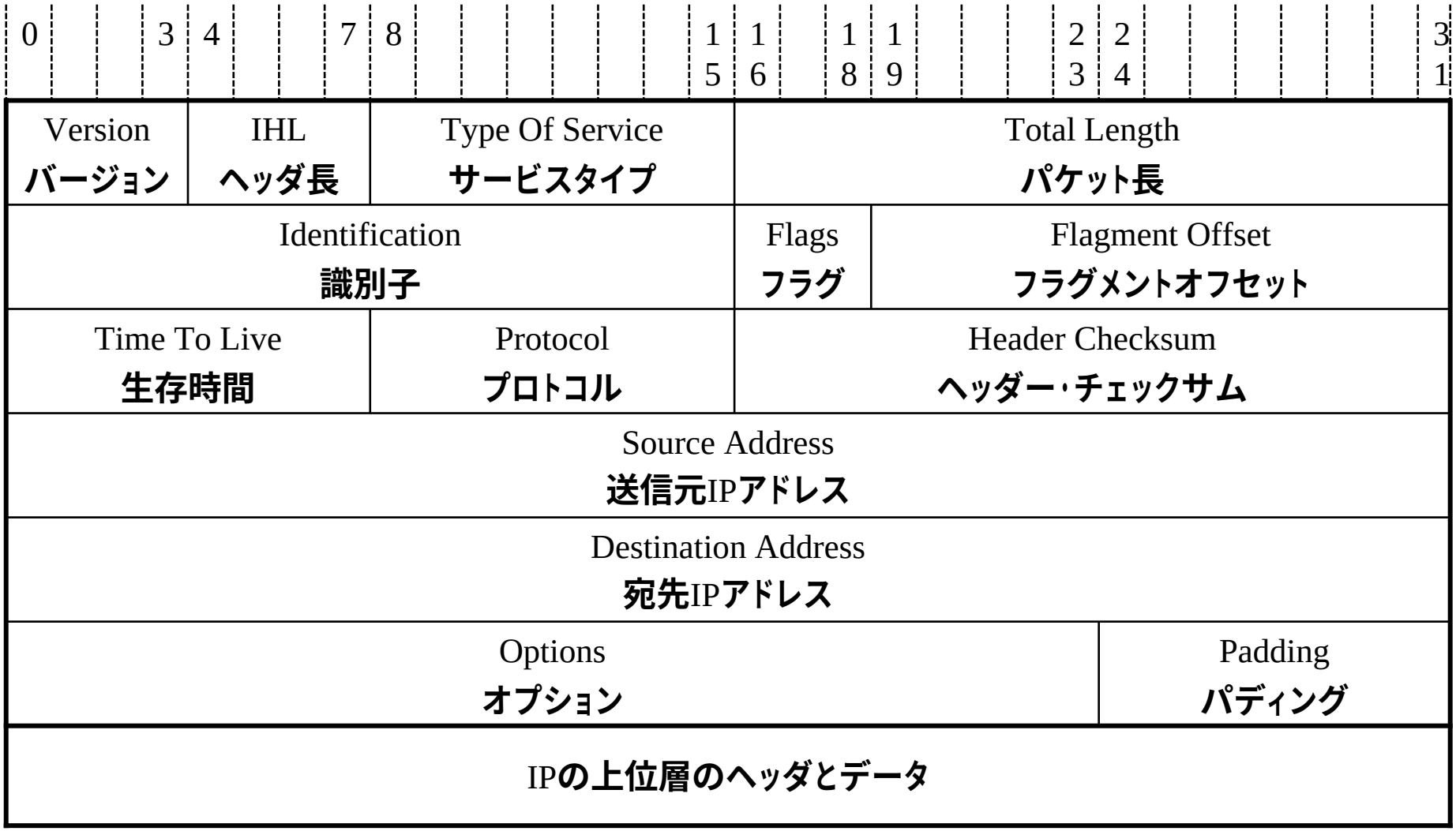
クラスC(192.168/16)

1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

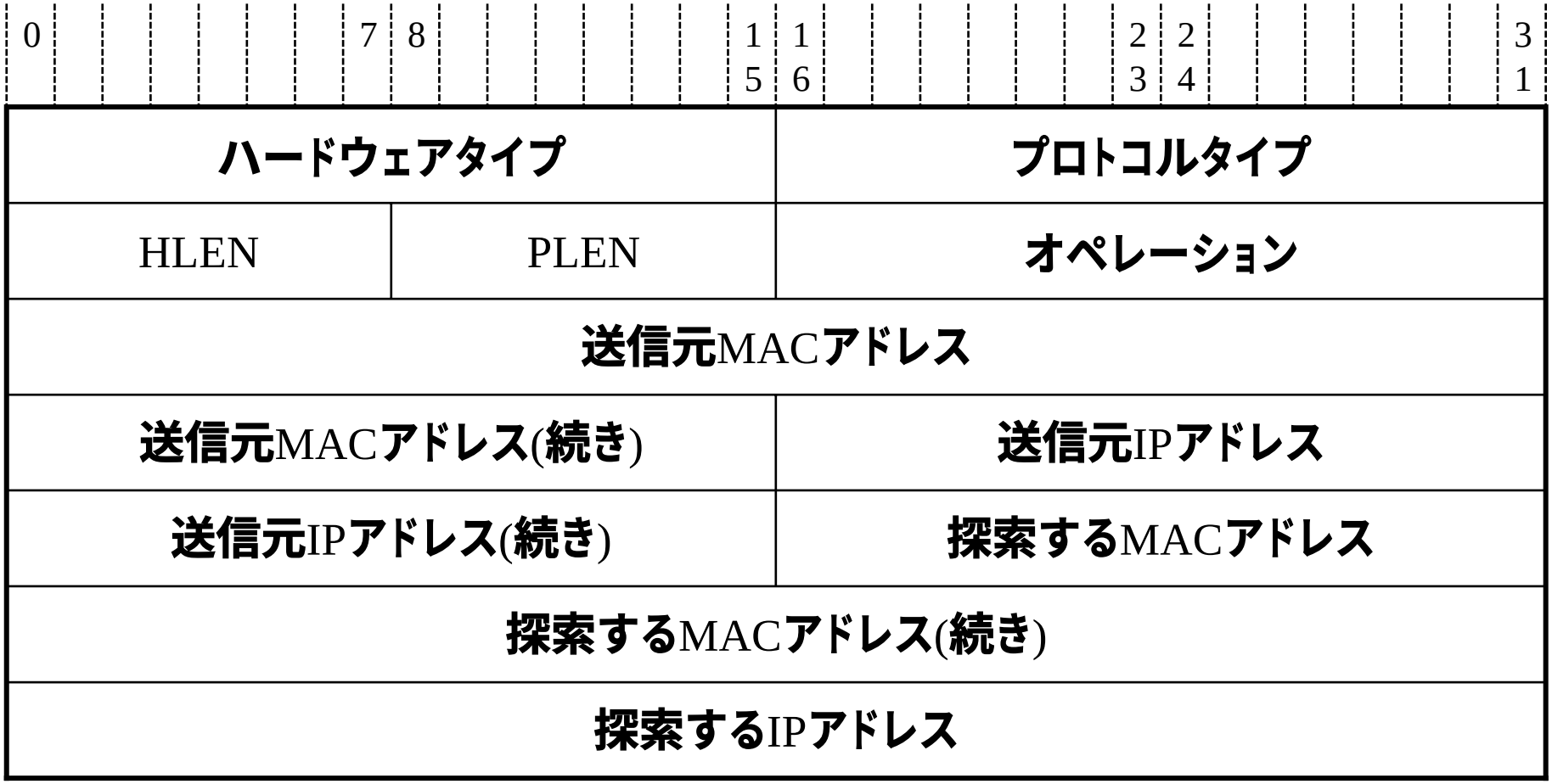
いろいろなアドレス(172.21.200.84/28)

IPアドレス																															
	172.							21.								200.								84							
1	0	1	0	1	1	0	0	0	0	0	1	0	1	0	1	1	1	0	0	1	0	0	0	0	1	0	1	0	1	0	0
サブネットマスク																															
	255.							255.								255.								192							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0
ネットワークアドレス																															
	172.							21.								200.								64							
1	0	1	0	1	1	0	0	0	0	0	1	0	1	0	1	1	1	0	0	1	0	0	0	0	1	0	1	0	0	0	0
ブロードキャストアドレス#1																															
	172.							21.								200.								95							
1	0	1	0	1	1	0	0	0	0	0	1	0	1	0	1	1	1	0	0	1	0	0	0	0	1	0	1	1	1	1	1
ブロードキャストアドレス#2																															
	255.							255.								255.								255							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

IPv4ヘッダ

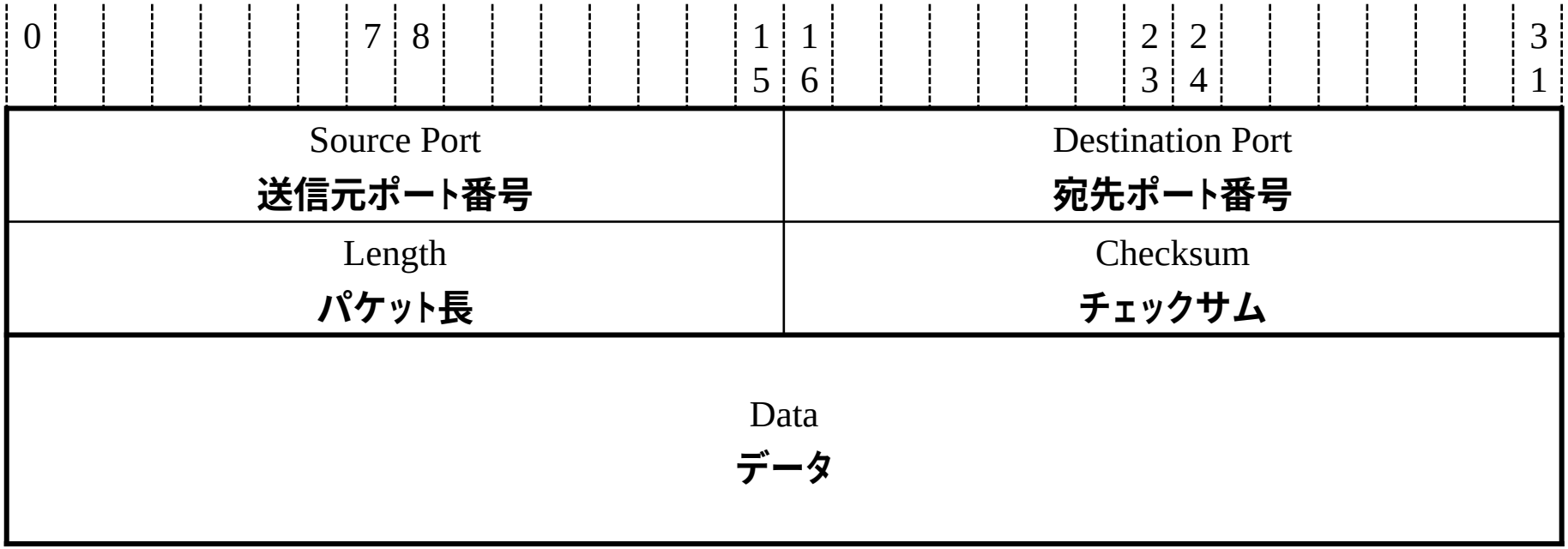


ARP(Address Resolution Protocol)

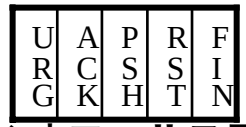


HLEN: MACアドレスの長さ=6 (オクテット)
PLEN: IPアドレスの長さ　　=4 (オクテット)

UDPヘッダ


0
7
8
15
16
23
24
31
Source Port
送信元ポート番号
Destination Port
宛先ポート番号
Length
パケット長
Checksum
チェックサム
Data
データ

TCPヘッダ

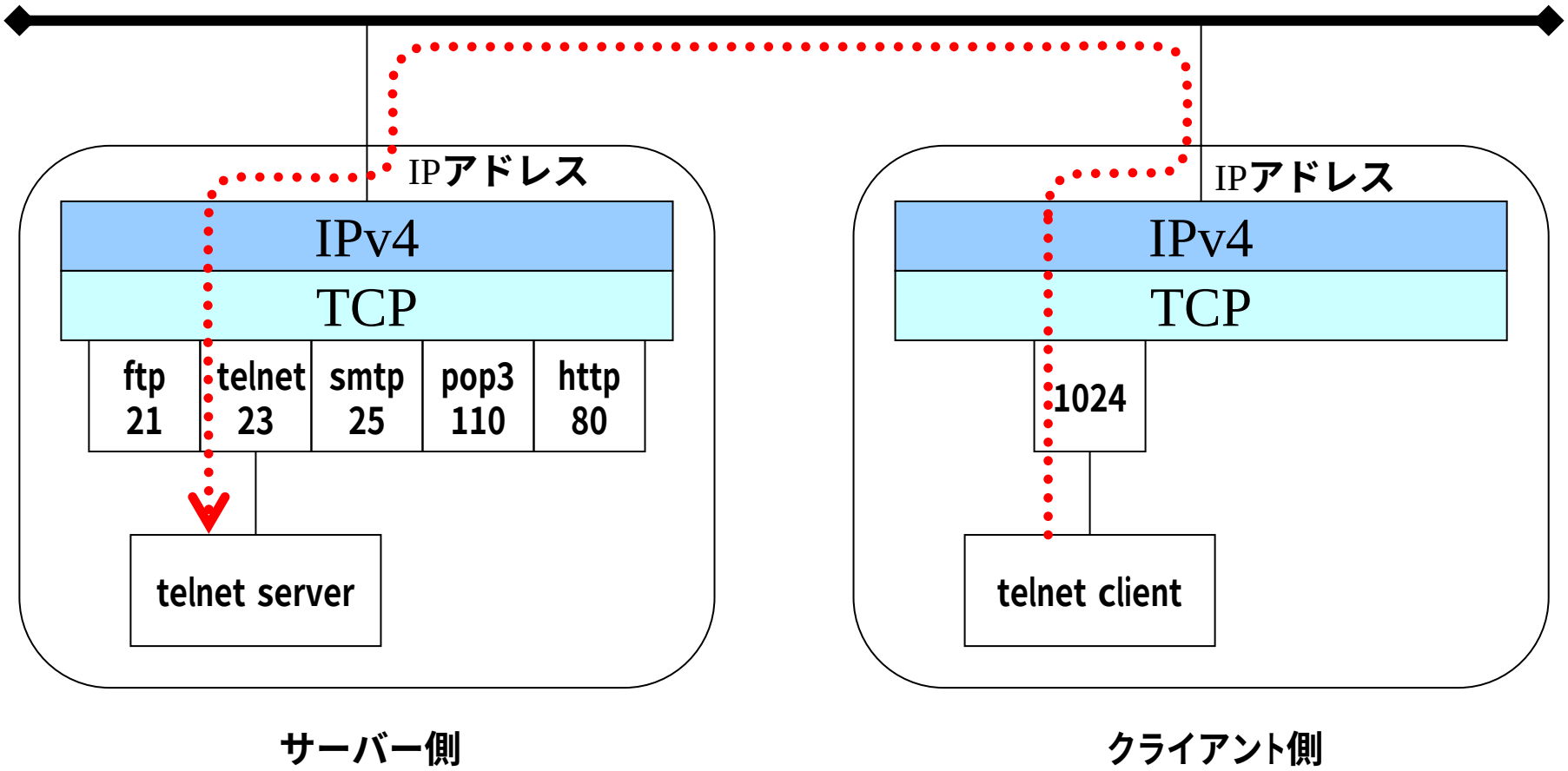


コントロールフラグ

0	3	4	7	8	9	10	15	16	23	24	31

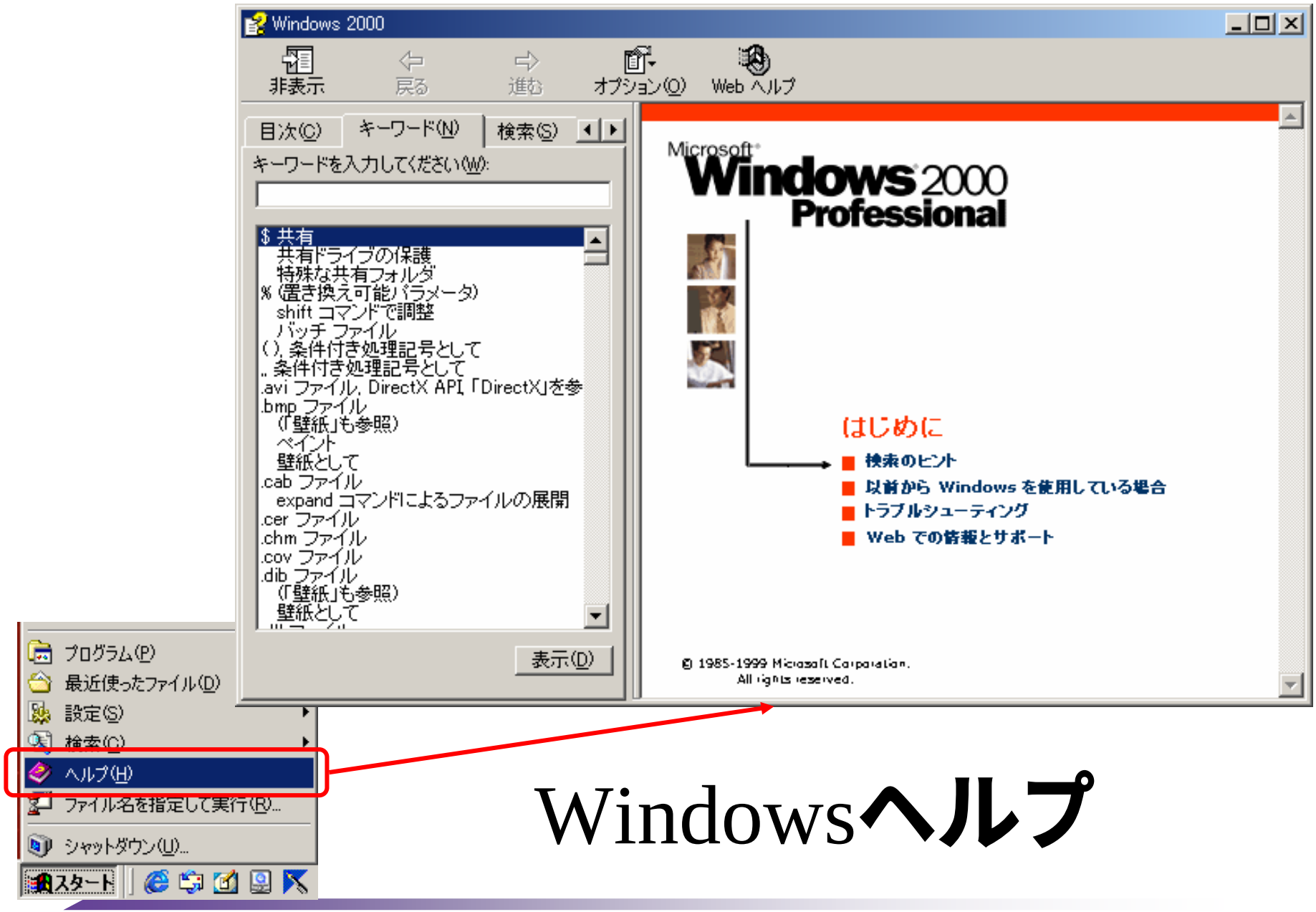
Source Port **送信元ポート番号**			Destination Port **宛先ポート**
Sequence Number **シーケンス番号**			
Acknowledgement Number **確認応答番号**			
Data Offset	Reserved **予約**	Control Flag **コントロールフラグ**	Window **ウィンドウサイズ**
Checksum **チェックサム**			Urgent Pointer **緊急ポインタ**
Options **オプション**			Padding **パディング**
Data..			

サーバーとクライアント



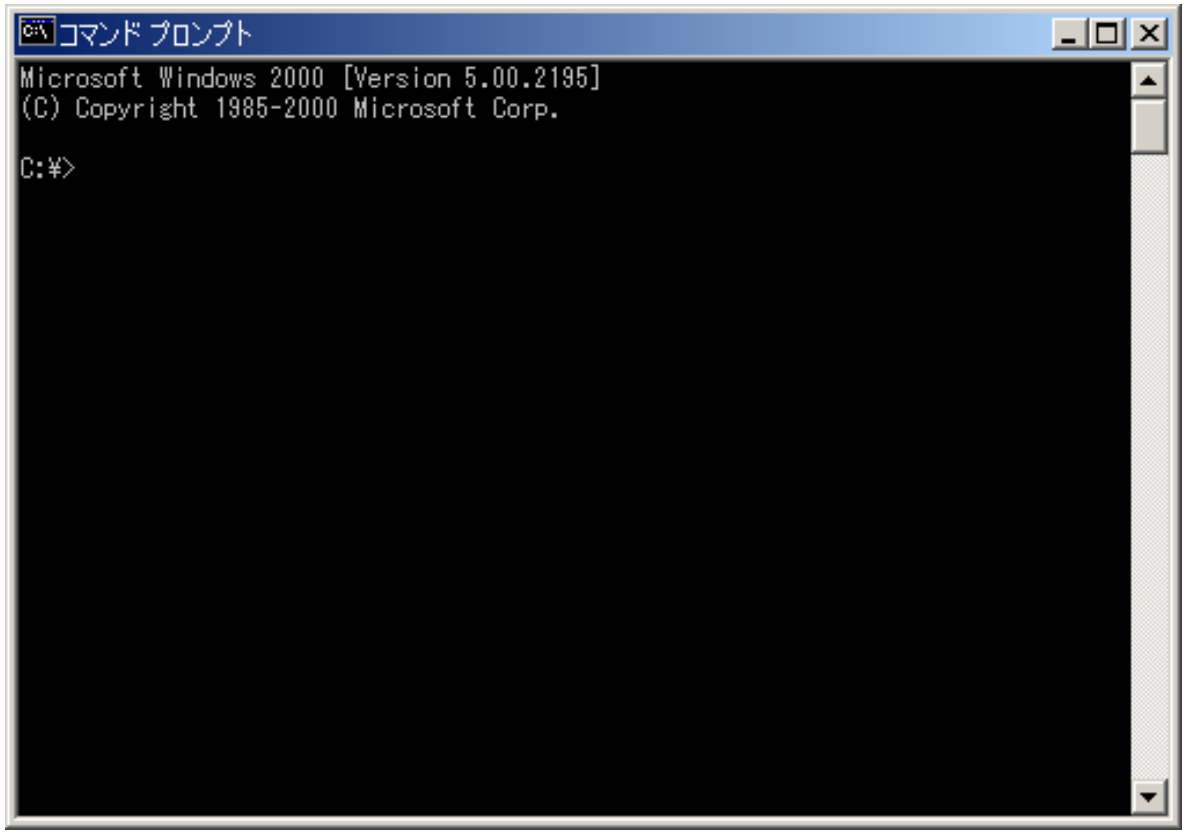
トラブル対策の道具(Windows)～知識の整理～

- Microsoft® Windows2000の標準ツール
- Windowsヘルプで検索してみよう!→[スタート]→[ヘルプ(H)]
- コマンド・プロンプト/MS-DOS プロンプト (cmd.exe)
- ping (ICMPエコーを利用したIPの到達性確認ツール)
- arp (ARPテーブルの確認や操作)
- ipconfig (IP設定と確認)
- tracert (ICMPエコーを利用した経路の確認ツール)
- netstat (統計情報や接続状態上などの表示)
- route (経路情報の確認や設定)
- telnet (telnetクライアント)
- ftp (ftpクライアント)
- tftp (tftpクライアント)
- (参考) net…NetBIOS,NetWareなどの操作や情報の確認



Windowsヘルプ

MS-DOS プロンプト



[スタート]
→[プログラム(P)]
→[アクセサリ]
→[コマンド プロンプト]

ステータスバーで、
マウスの右ボタンを
クリックするとでる
メニューのプロパティ
でカスタマイズできる。
・色、フォント、…
・ヒストリ
・スクロールバー

[ウィンドウのキャプチャー] Alt + PrtSc
[スクリーンのキャプチャー] Shift + PrtSc

pingコマンドのヘルプ

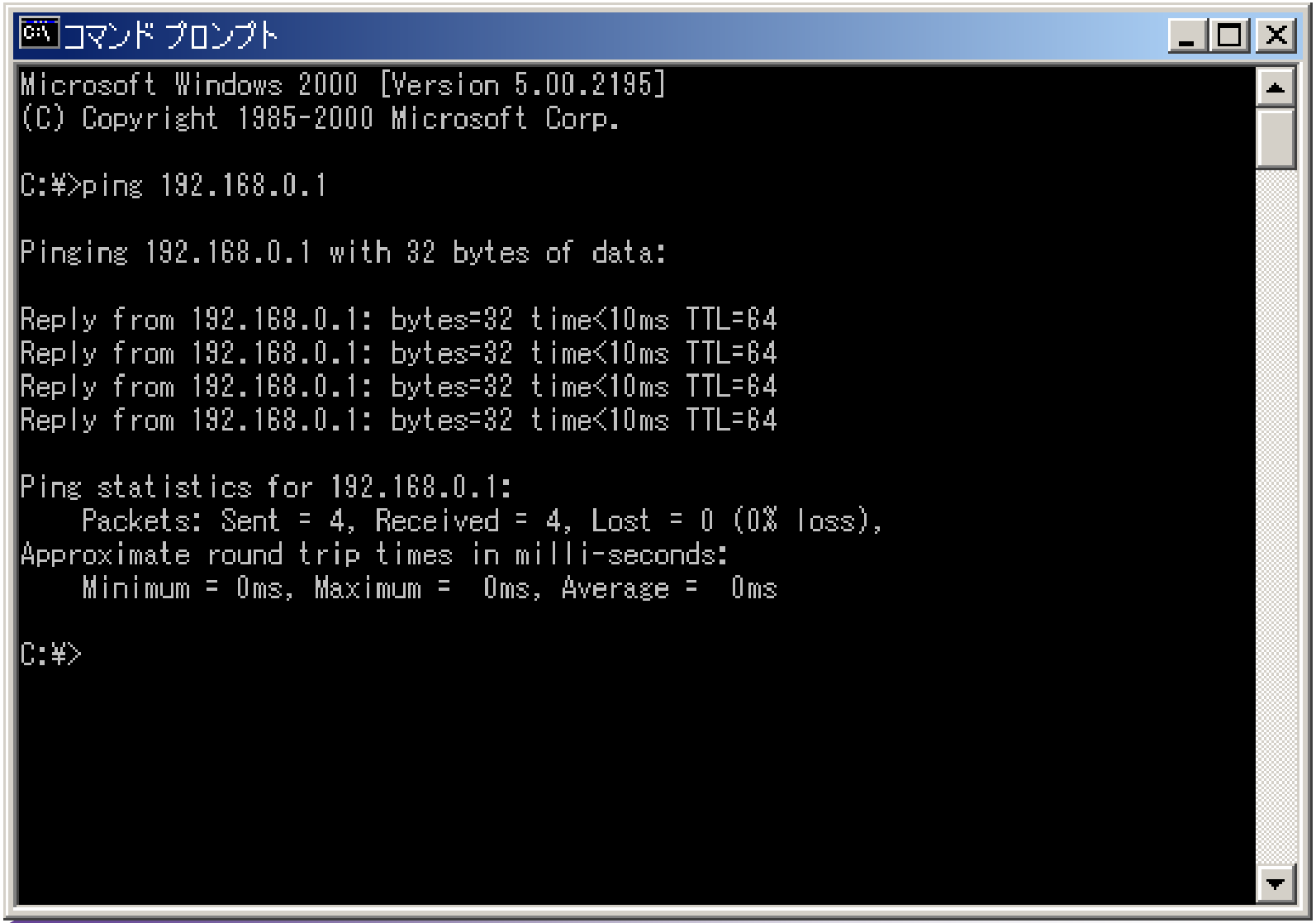
```
C:\>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] destination-list

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet.
    -i TTL         Time To Live.
    -v TOS         Type Of Service.
    -r count       Record route for count hops.
    -s count       Timestamp for count hops.
    -j host-list   Loose source route along host-list.
    -k host-list   Strict source route along host-list.
    -w timeout     Timeout in milliseconds to wait for each reply.
```

pingコマンドのオプション

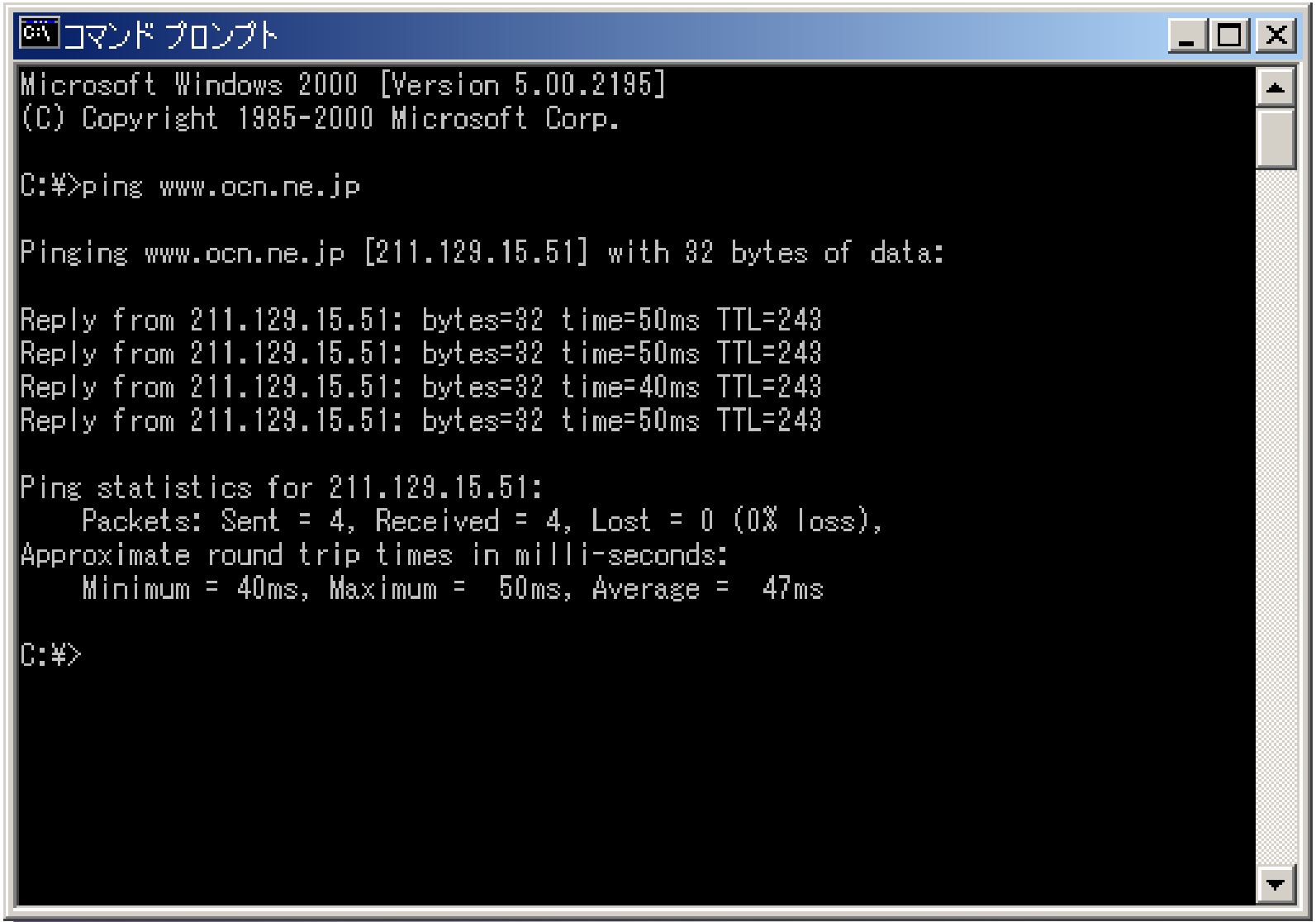
書式：ping ＜オプション＞ ホスト名またはIPアドレス

オプション	意味
-t	「Ctrl+C」キーが押されるまで送信を繰り返す
-a	IPアドレスの代わりに逆引きしたDNSホスト名の表示
-n count	指定した回数送信する。既定値は、4回。
-l size	送信パケットのサイズを指定する。既定値は32バイト。
-f	フラグメンテーション(パケットの分割)を禁止する。
-i TTL	パケットがルーターを通過できる最大数(ホップ数)の指定
-v TOS	IPパケットのTOS(type of service)フィールドに値を設定して送信する。
-r count	パケットが通過したルーターのIPアドレスを表示する。表示数も指定できる。
-s count	タイムスタンプを表示する。表示数も指定できる。
-j host-list	経路指定。指定されたホストがない場合は通常のルーティングをする。
-k host-list	経路指定。指定されたホストがない場合はエラーとする。
-w timeout	タイムアウト時間をミリ秒単位で指定する。

ping 192.168.0.1



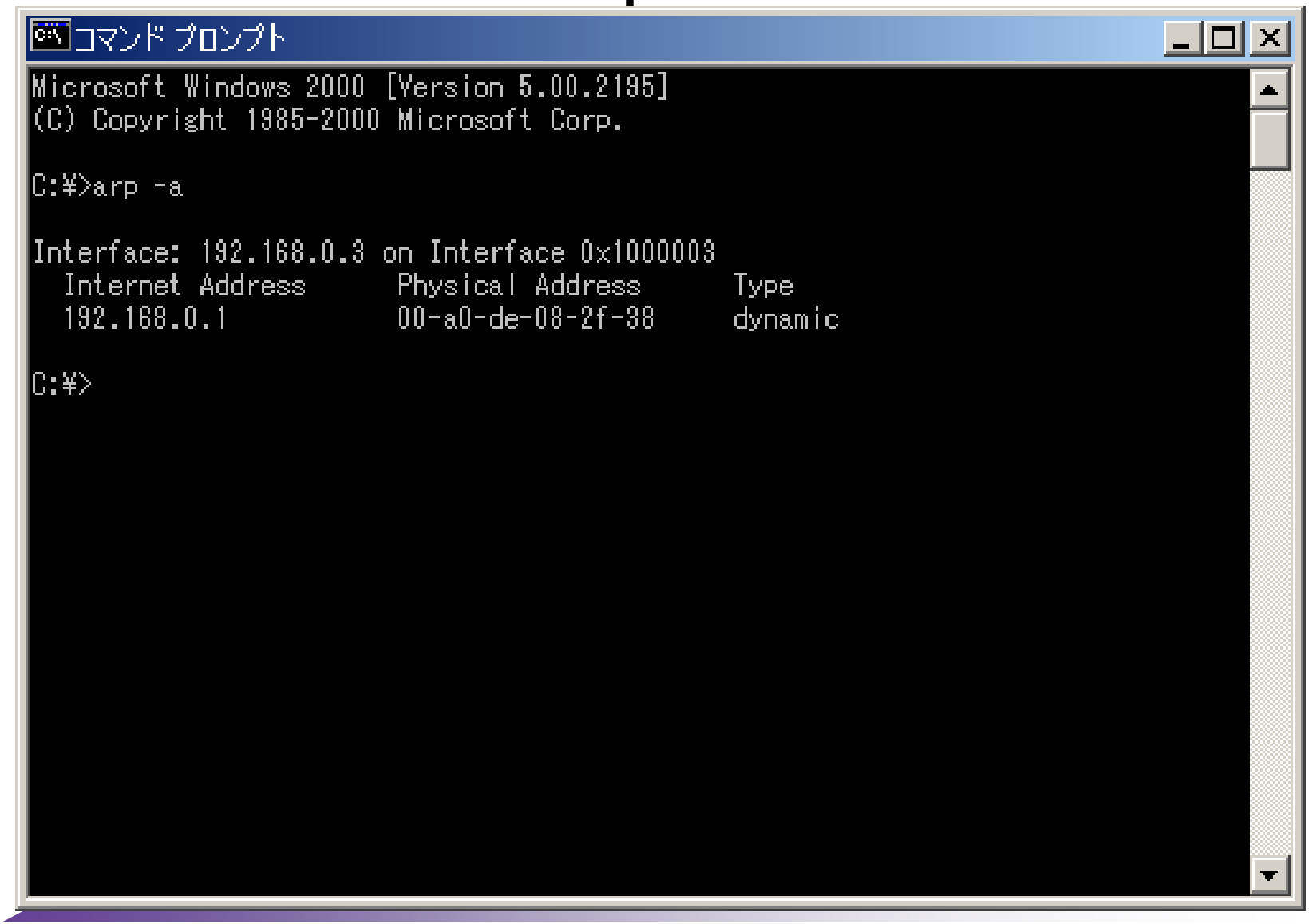
ping www.ocn.ne.jp



arpコマンド

```
C:\>arp

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.

Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.
```

arp -a



ipconfig コマンドのヘルプ

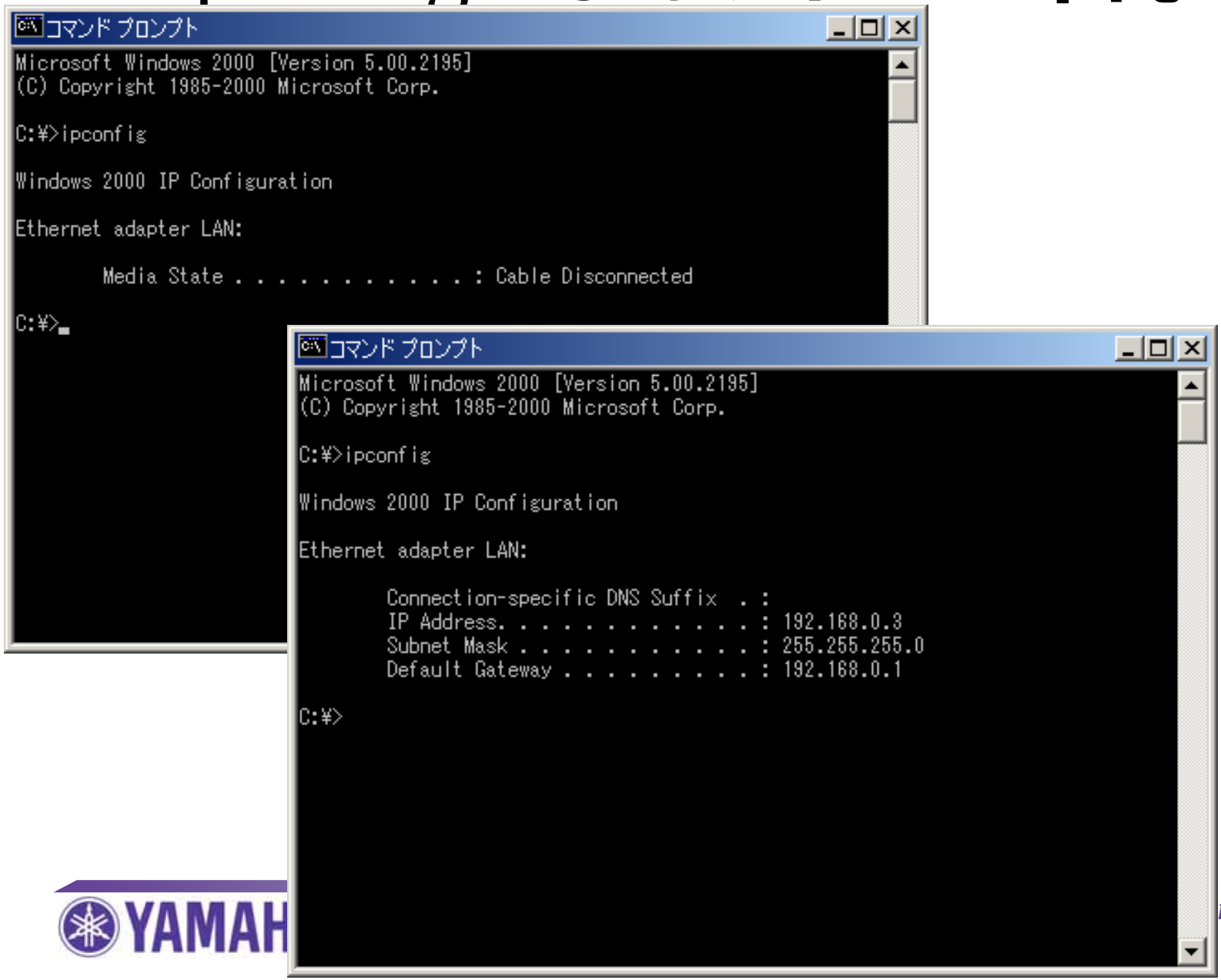
```
C:\>ipconfig -?

Windows 2000 IP Configuration

USAGE:
    ipconfig [/? | /all | /release [adapter] | /renew [adapter]
              | /flushdns | /registerdns
              | /showclassid adapter
              | /setclassid adapter [classidtoset] ]

    adapter    Full name or pattern with '*' and '?' to 'match',
               * matches any character, ? matches one character.
    Options
        /?           Display this help message.
        /all         Display full configuration information.
        /release     Release the IP address for the specified adapter.
        /renew       Renew the IP address for the specified adapter.
        /flushdns    Purges the DNS Resolver cache.
        /registerdns Refreshes all DHCP leases and re-registers DNS names
        /displaydns  Display the contents of the DNS Resolver Cache.
        /showclassid Displays all the dhcp class IDs allowed for adapter.
        /setclassid  Modifies the dhcp class id.

The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For SetClassID, if no class id is specified, then the classid is removed.

Examples:
    > ipconfig                        ... Show information.
    > ipconfig /all                   ... Show detailed information
    > ipconfig /renew                 ... renew all adapaters
    > ipconfig /renew EL*             ... renew adapters named EL....
    > ipconfig /release *ELINK?21*    ... release all matching adapters,
                                          eg. ELINK-21, myELELINKi21adapter.
```

ipconfig コマンドのオプション

書式: ipconfig ＜オプション＞

オプション	意味
/?	コマンドヘルプの表示
/all	全ての設定情報の表示
/release	アダプタの情報を開放する。
/renew	アダプタの情報を更新する。
/flushdns	Purges the DNS Resolver cache.
/registerdns	Refreshes all DHCP leases and re-registers DNS names
/displaydns	Display the contents of the DNS Resolver Cache.
/showclassid	Displays all the dhcp class IDs allowed for adapter.
/setclassid	Modifies the dhcp class id.

ipconfigによるアドレス確認



tracert コマンドのヘルプ

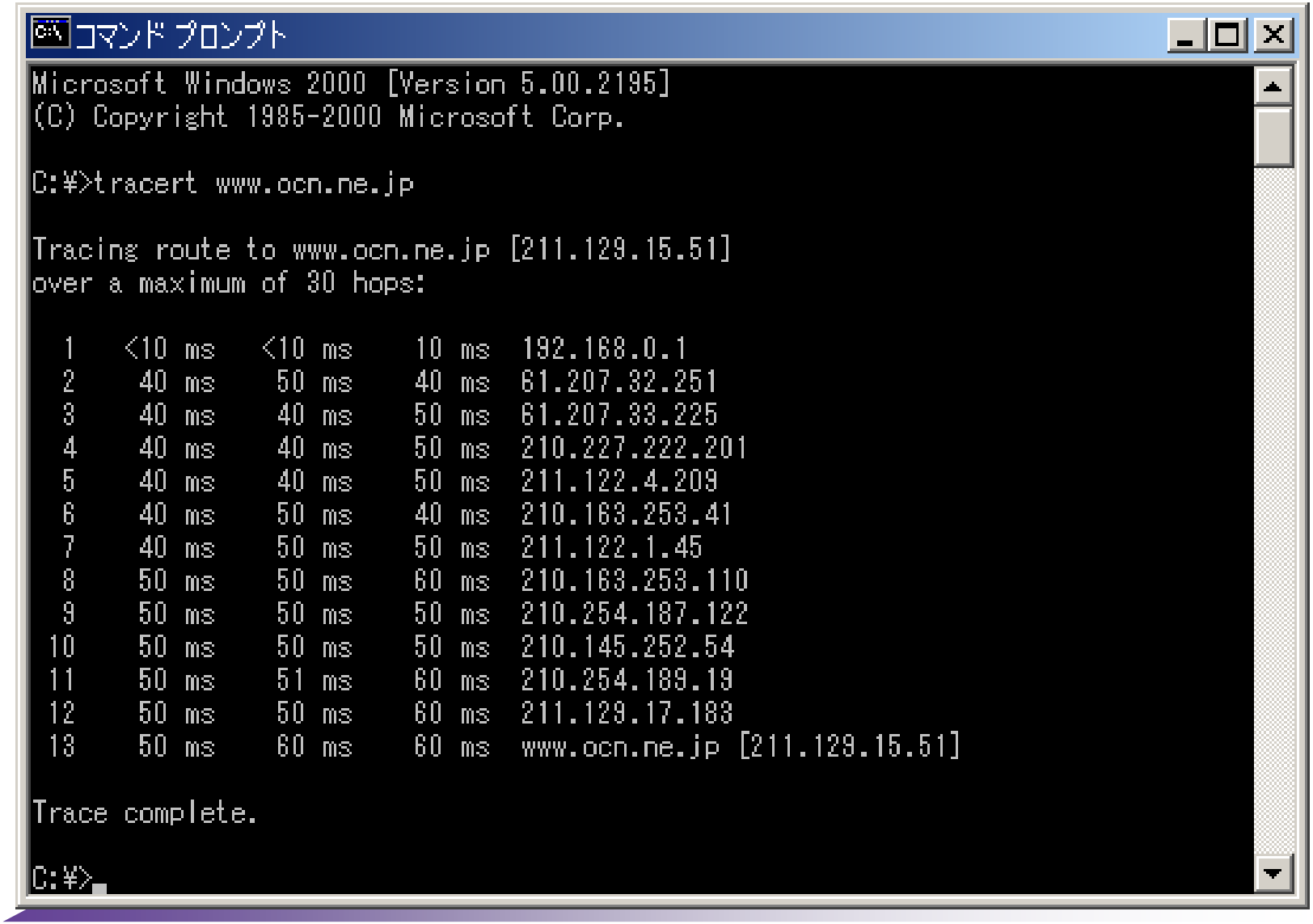
```
C:\>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list.
    -w timeout         Wait timeout milliseconds for each reply.
```

tracert コマンドのオプション

書式：tracert ＜オプション＞ ホスト名またはIPアドレス

オプション	意味
-d	IPアドレスだけ表示する (DNSホスト名の逆引きをしない)
-h maximum_hops	相手先までの最大ホスト数を指定する。
-j host-list	指定した経路で送信する。(なければ他の経路)
-w timeout	タイムアウト時間をミリ秒単位で指定する。

tracert www.ocn.ne.jp



netstat コマンドのヘルプ

```
C:\>netstat -?

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]

  -a            Displays all connections and listening ports.
  -e            Displays Ethernet statistics. This may be combined with the -s
                option.
  -n            Displays addresses and port numbers in numerical form.
  -p proto      Shows connections for the protocol specified by proto; proto
                may be TCP or UDP.  If used with the -s option to display
                per-protocol statistics, proto may be TCP, UDP, or IP.
  -r            Displays the routing table.
  -s            Displays per-protocol statistics.  By default, statistics are
                shown for TCP, UDP and IP; the -p option may be used to specify
                a subset of the default.
  interval      Redisplays selected statistics, pausing interval seconds
                between each display.  Press CTRL+C to stop redisplaying
                statistics.  If omitted, netstat will print the current
                configuration information once.
```

netstat コマンドのオプション

書式: netstat ＜オプション＞

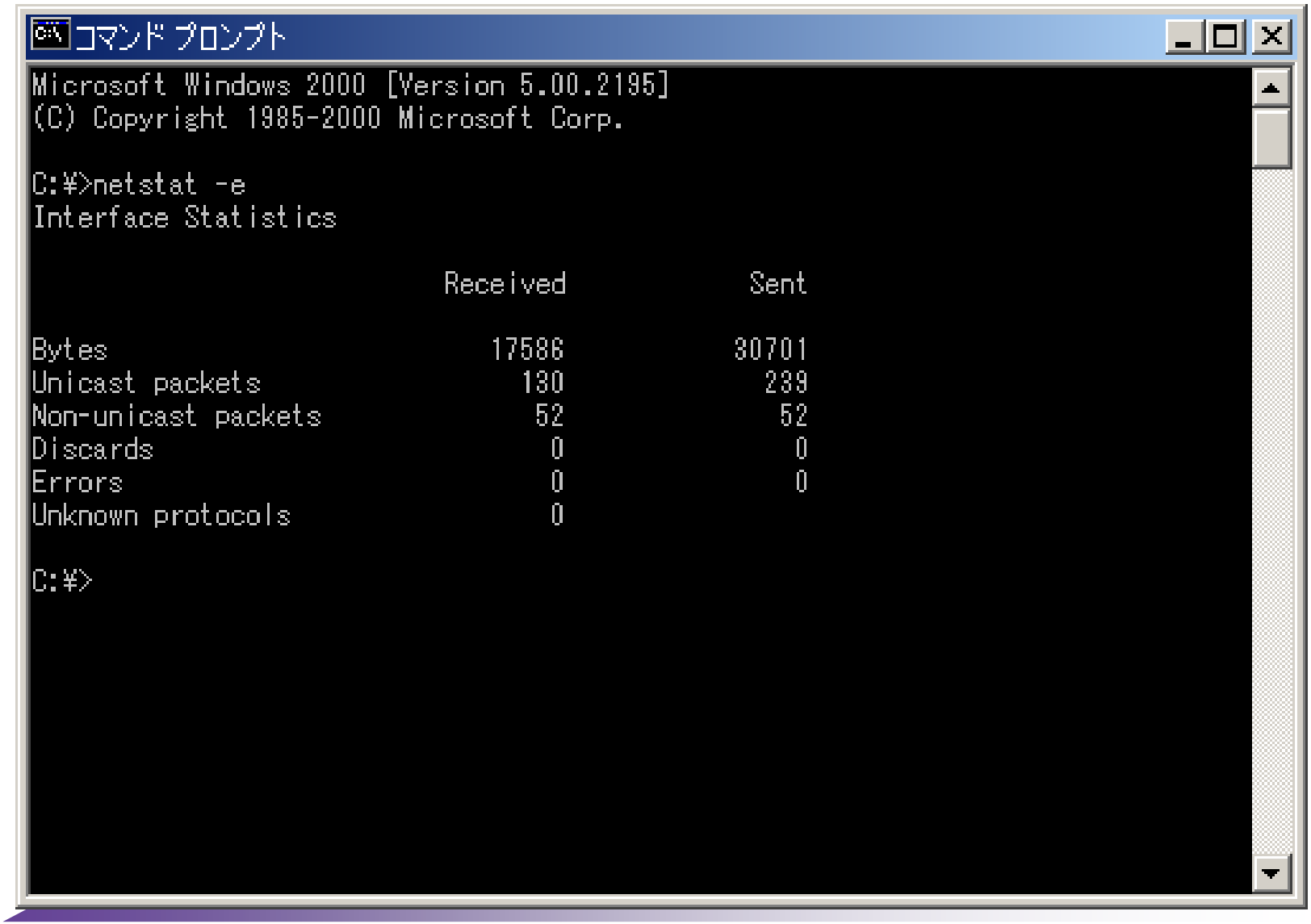
オプション	意味
-a	コネクションと待機ポートのすべてを表示する。(-nと合わせると数値表示)
-e	イーサネットの統計情報を表示する。
-n	アクティブなポートを接続先とともに表示する。
-s	IP, ICMP, TCP, UDPの統計情報を表示する。
-p proto	特定のプロトコル情報を表示する。-sオプションの代わりに利用する。 [proto]で、プロトコル名を指定する。
-r	ルーティング･テーブルを表示する。
interval	定期的に最新情報を更新して表示する。 [interval]で更新間隔を秒単位で指定

```
C:\>netstat –a
C:\>netstat –n
C:\>netstat –an 3
```

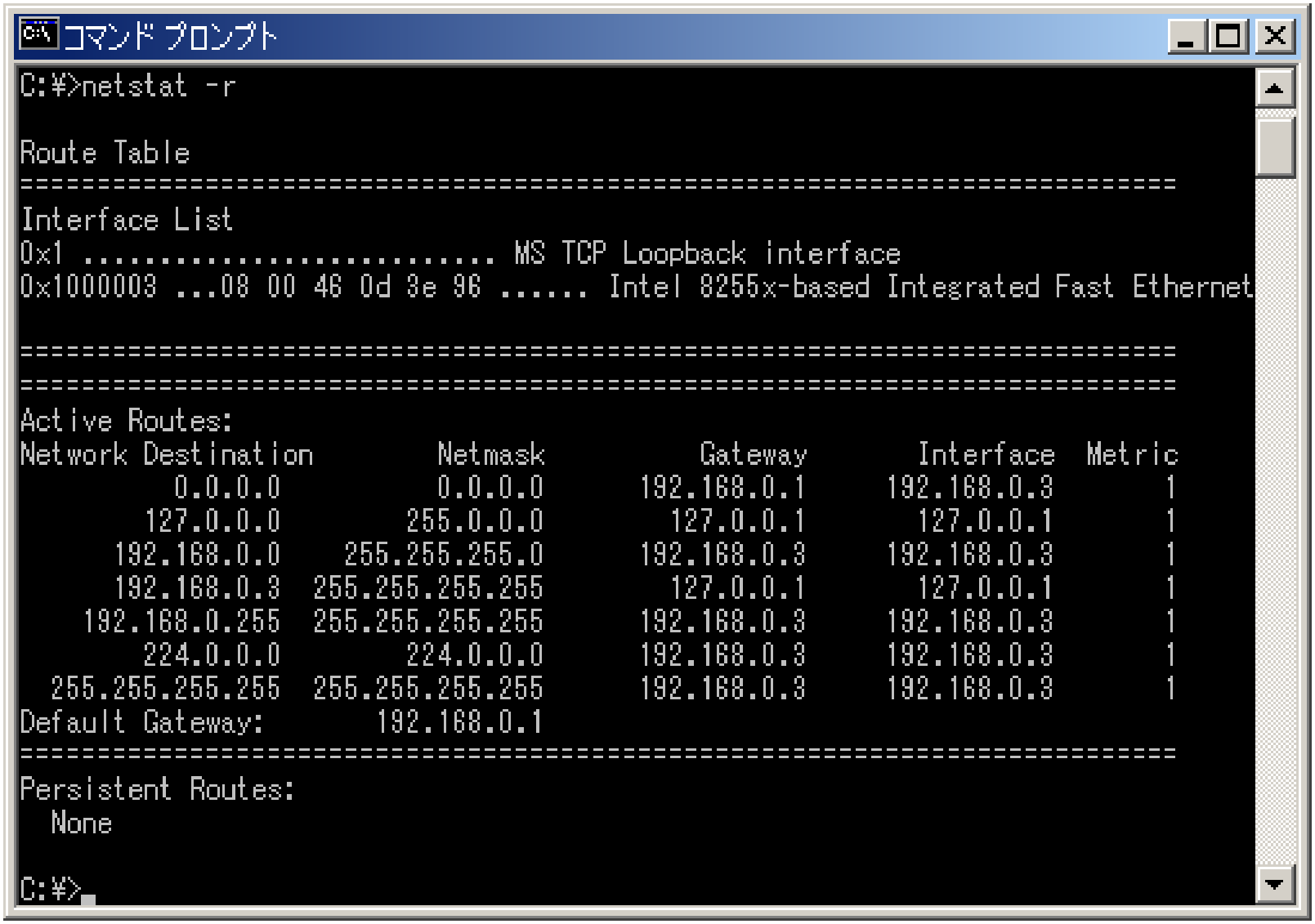
```
C:\>netstat -r
```

```
C:\>netstat –s
C:\>netstat –e
```

netsat –e



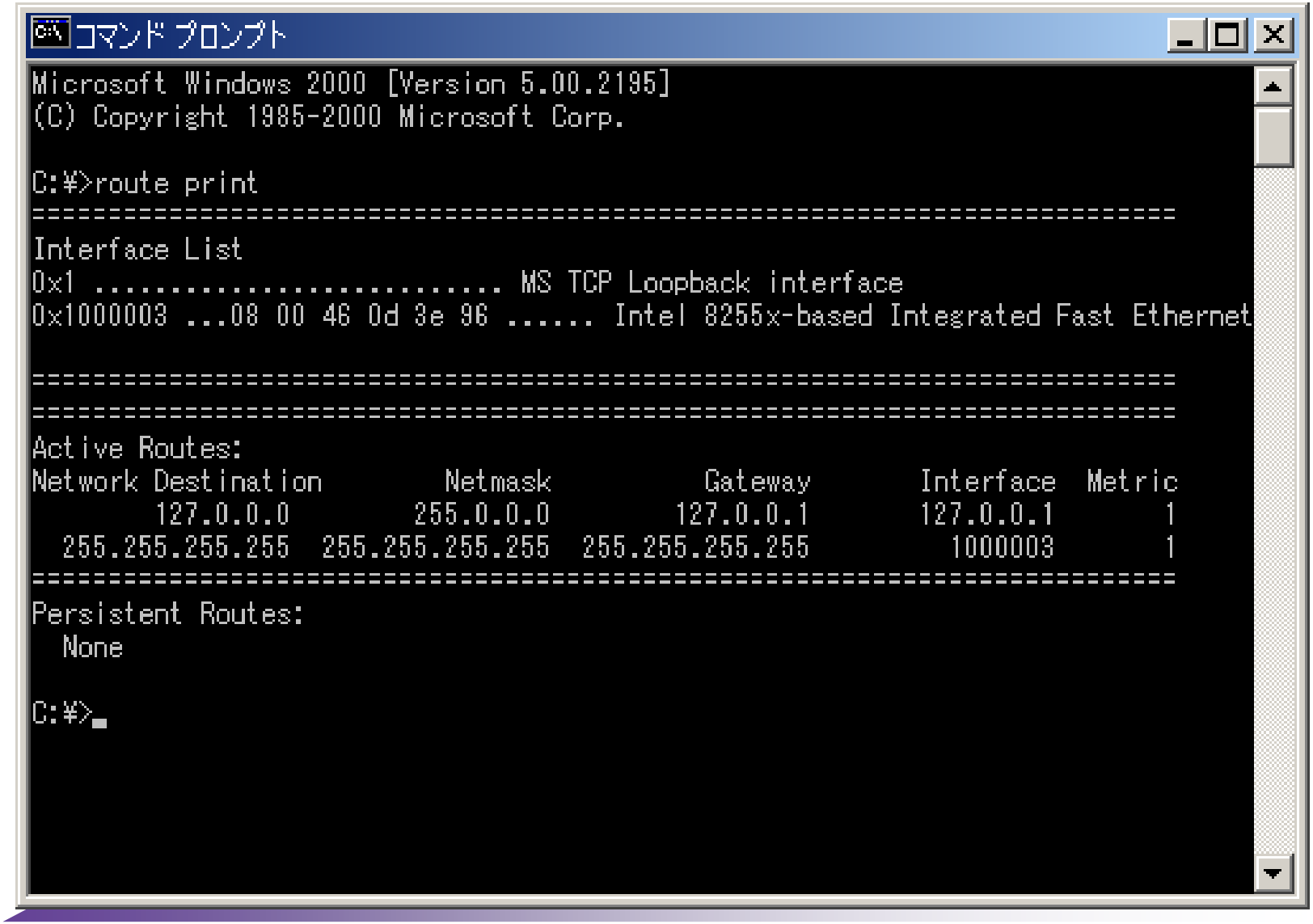
netsat –r



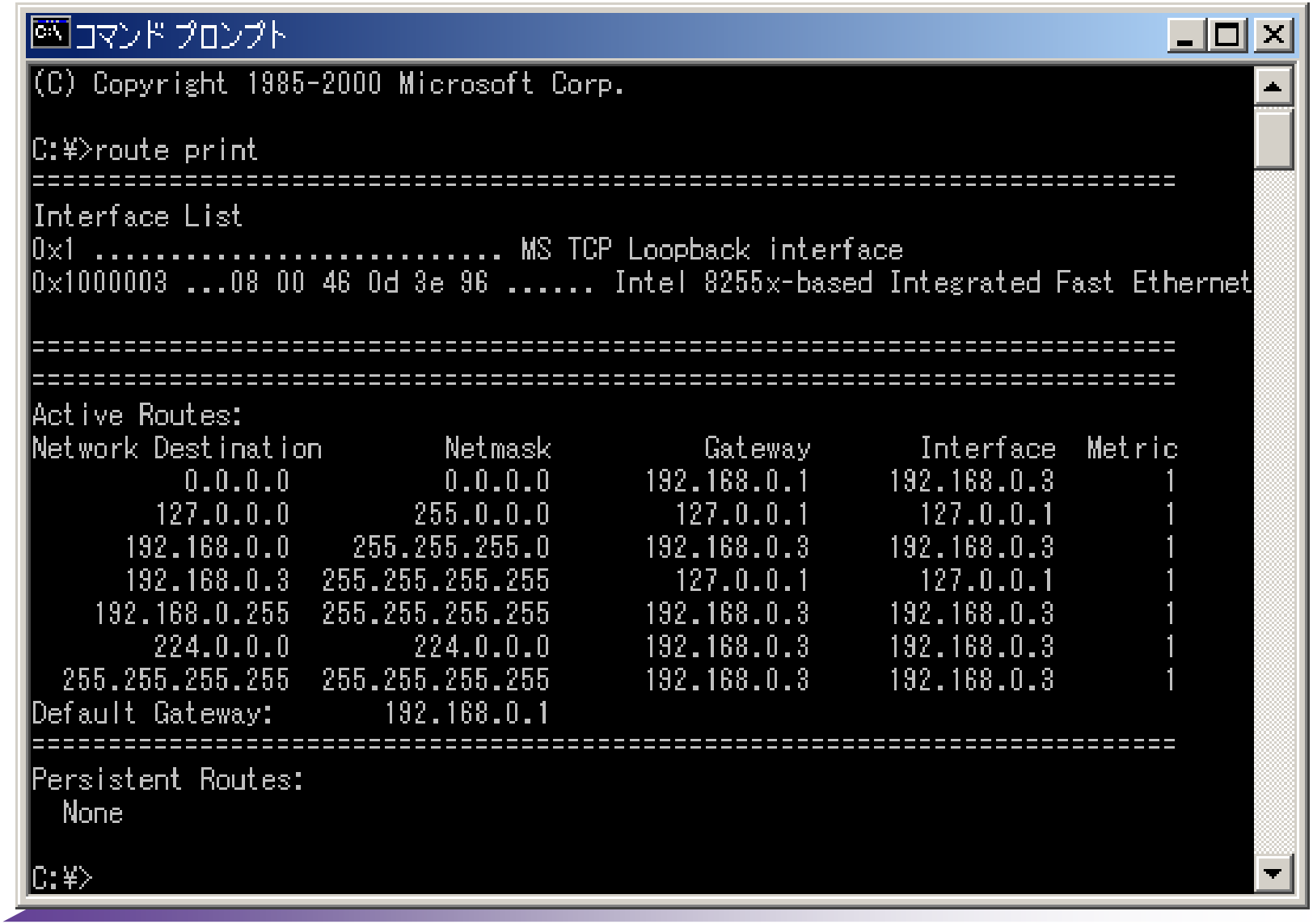
route コマンド

```
C:\>route
Manipulates network routing tables.
ROUTE [-f] [-p] [command [destination]
                  [MASK netmask]  [gateway] [METRIC metric]  [IF interface]
  -f            Clears the routing tables of all gateway entries.  If this is
                used in conjunction with one of the commands, the tables are
                cleared prior to running the command.
  -p            When used with the ADD command, makes a route persistent across
                boots of the system. By default, routes are not preserved
                when the system is restarted. Ignored for all other commands,
                which always affect the appropriate persistent routes. This
                option is not supported in Windows 95.
  command       One of these:
                  PRINT     Prints  a route
                  ADD       Adds    a route
                  DELETE    Deletes a route
                  CHANGE    Modifies an existing route
  destination   Specifies the host.
  MASK          Specifies that the next parameter is the 'netmask' value.
  netmask       Specifies a subnet mask value for this route entry.
                If not specified, it defaults to 255.255.255.255.
  gateway       Specifies gateway.
  interface     the interface number for the specified route.
  METRIC        specifies the metric, ie. cost for the destination.
All symbolic names used for destination are looked up in the network database
file NETWORKS. The symbolic names for gateway are looked up in the host name
database file HOSTS.
If the command is PRINT or DELETE. Destination or gateway can be a wildcard,
(wildcard is specified as a star '*'), or the gateway argument may be omitted.
If Dest contains a * or ?, it is treated as a shell pattern, and only
matching destination routes are printed. The '*' matches any string,
and '?' matches any one char. Examples: 157.*.1, 157.*, 127.*, *224*.
Diagnostic Notes:
    Invalid MASK generates an error, that is when (DEST & MASK) != DEST.
    Example> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
             The route addition failed: The specified mask parameter is invalid.
 (Destination & Mask) != Destination.
Examples:
    > route PRINT
    > route ADD 157.0.0.0 MASK 255.0.0.0  157.55.80.1 METRIC 3 IF 2
              destination^      ^mask      ^gateway     metric^    ^
                                                        Interface^
      If IF is not given, it tries to find the best interface for a given
      gateway.
    > route PRINT
    > route PRINT 157*          .... Only prints those matching 157*
    > route DELETE 157.0.0.0
    > route PRINT
```

route (未接続)

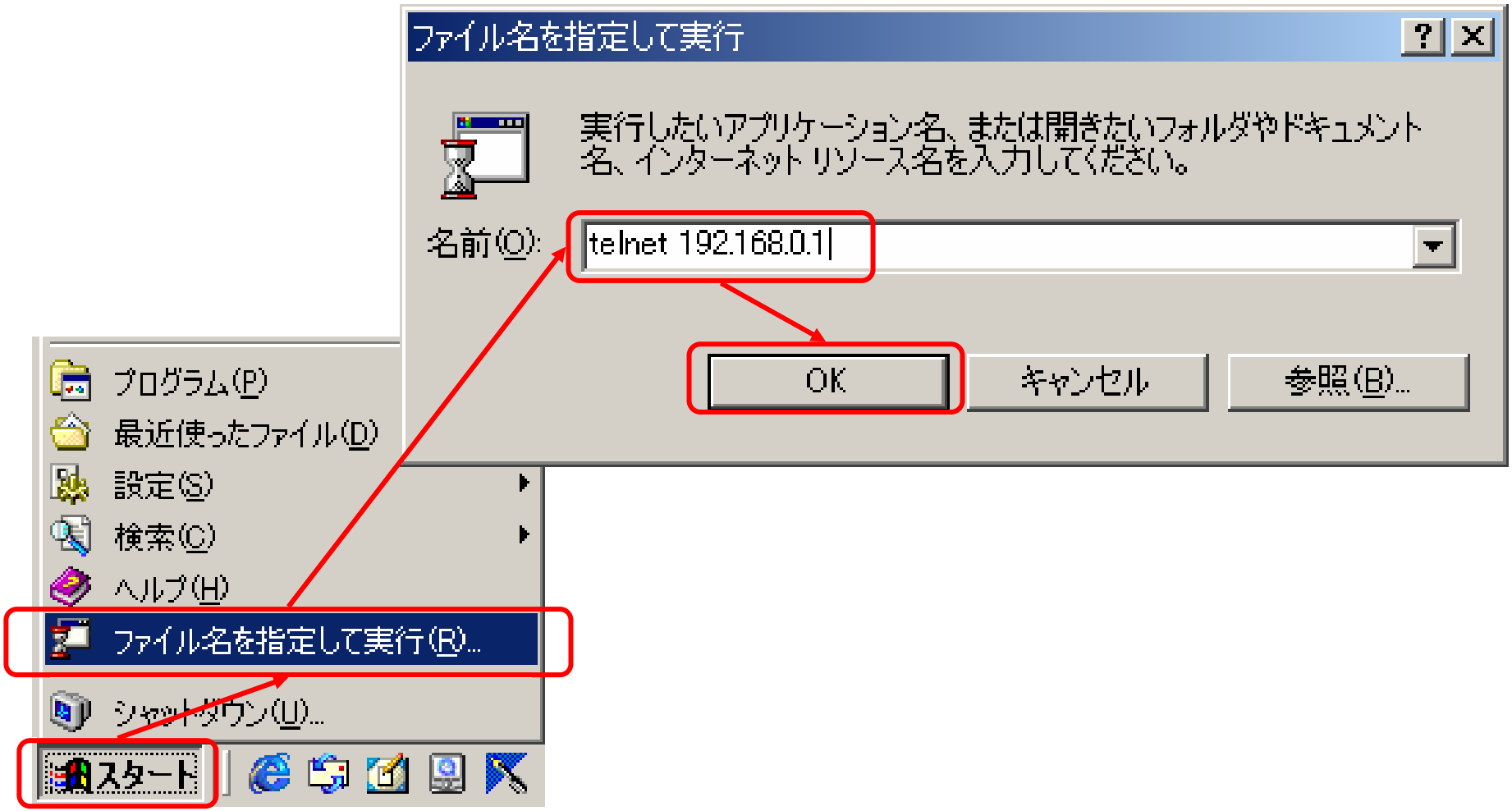


route (192.168.0.3/24)

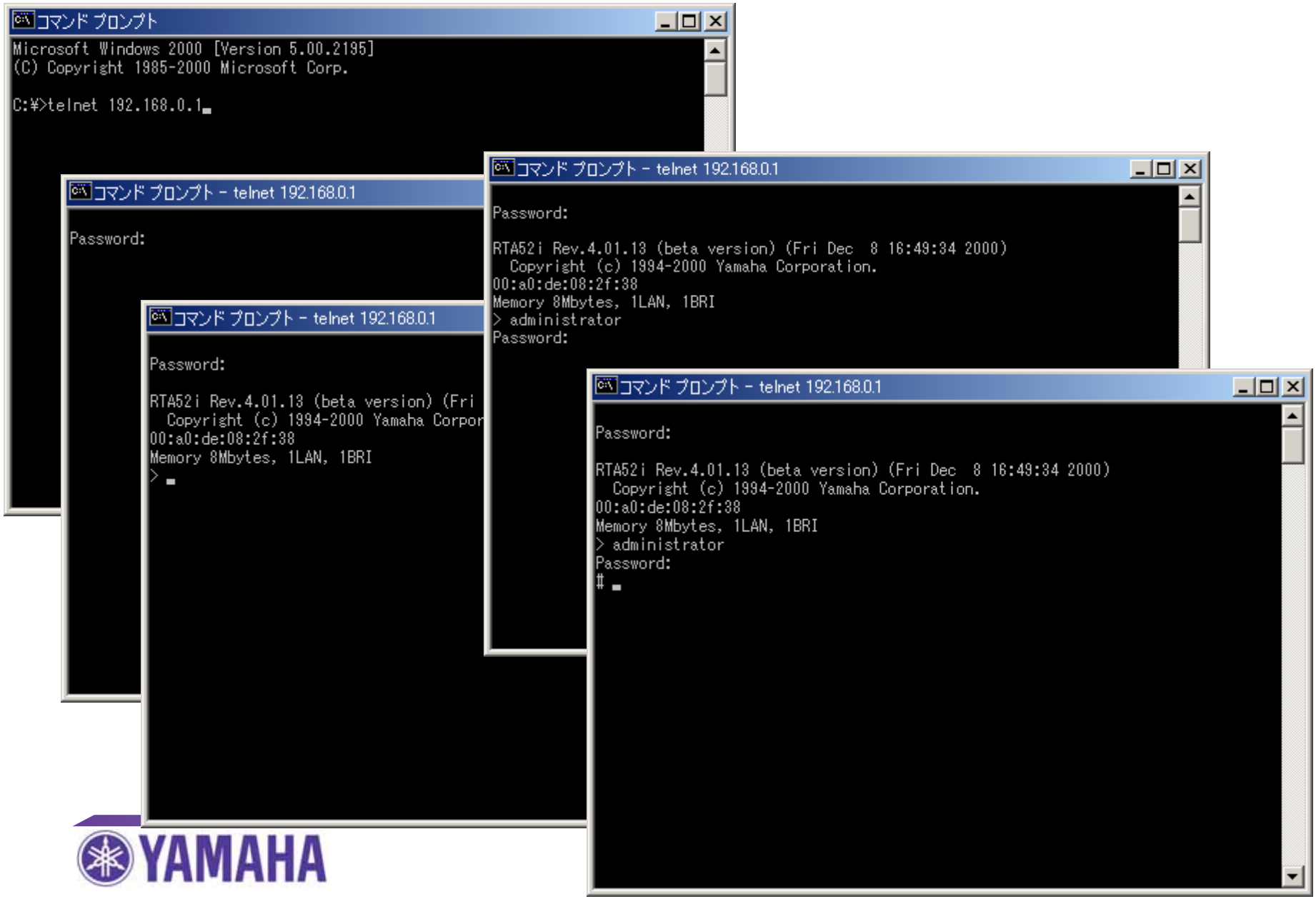


telnet コマンド

書式：telnet IPアドレスまたはホスト名 ポート番号



telnet コマンド

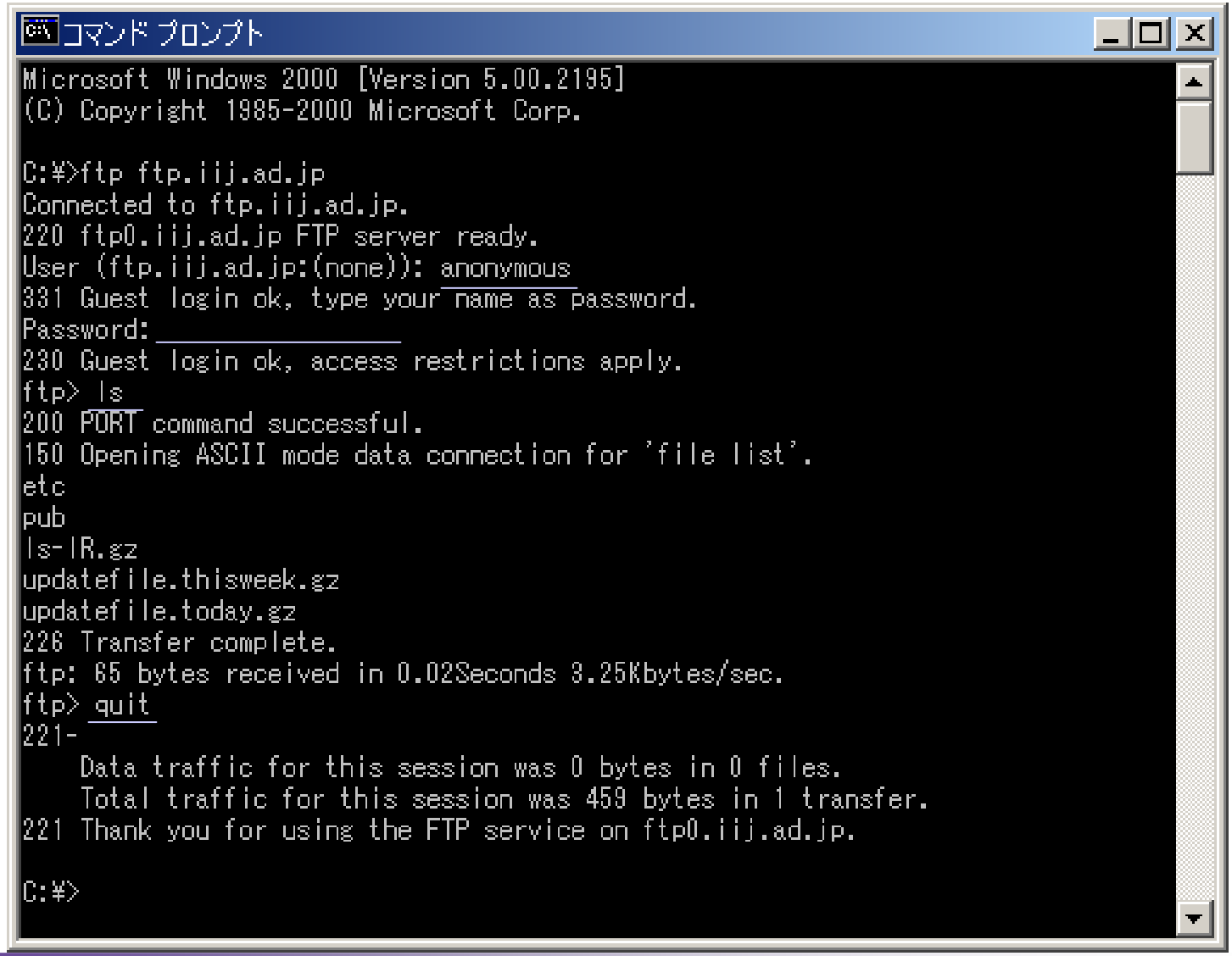


YAMAHA

ftp コマンド

```
C:\>ftp -?

Transfers files to and from a computer running an FTP server service
(sometimes called a daemon). Ftp can be used interactively.

FTP [-v] [-d] [-i] [-n] [-g] [-s:filename] [-a] [-w:windowsize] [-A] [host]

  -v              Suppresses display of remote server responses.
  -n              Suppresses auto-login upon initial connection.
  -i              Turns off interactive prompting during multiple file
                  transfers.
  -d              Enables debugging.
  -g              Disables filename globbing (see GLOB command).
  -s:filename     Specifies a text file containing FTP commands; the
                  commands will automatically run after FTP starts.
  -a              Use any local interface when binding data connection.
  -A              login as anonymous.
  -w:buffersize   Overrides the default transfer buffer size of 4096.
  host            Specifies the host name or IP address of the remote
                  host to connect to.

Notes:
  - mget and mput commands take y/n/q for yes/no/quit.
  - Use Control-C to abort commands.
```

ftp コマンド



tftp コマンド

ルーターのファームウェアを更新したり、設定の取得や
更新に利用する。(利用する場合がある)

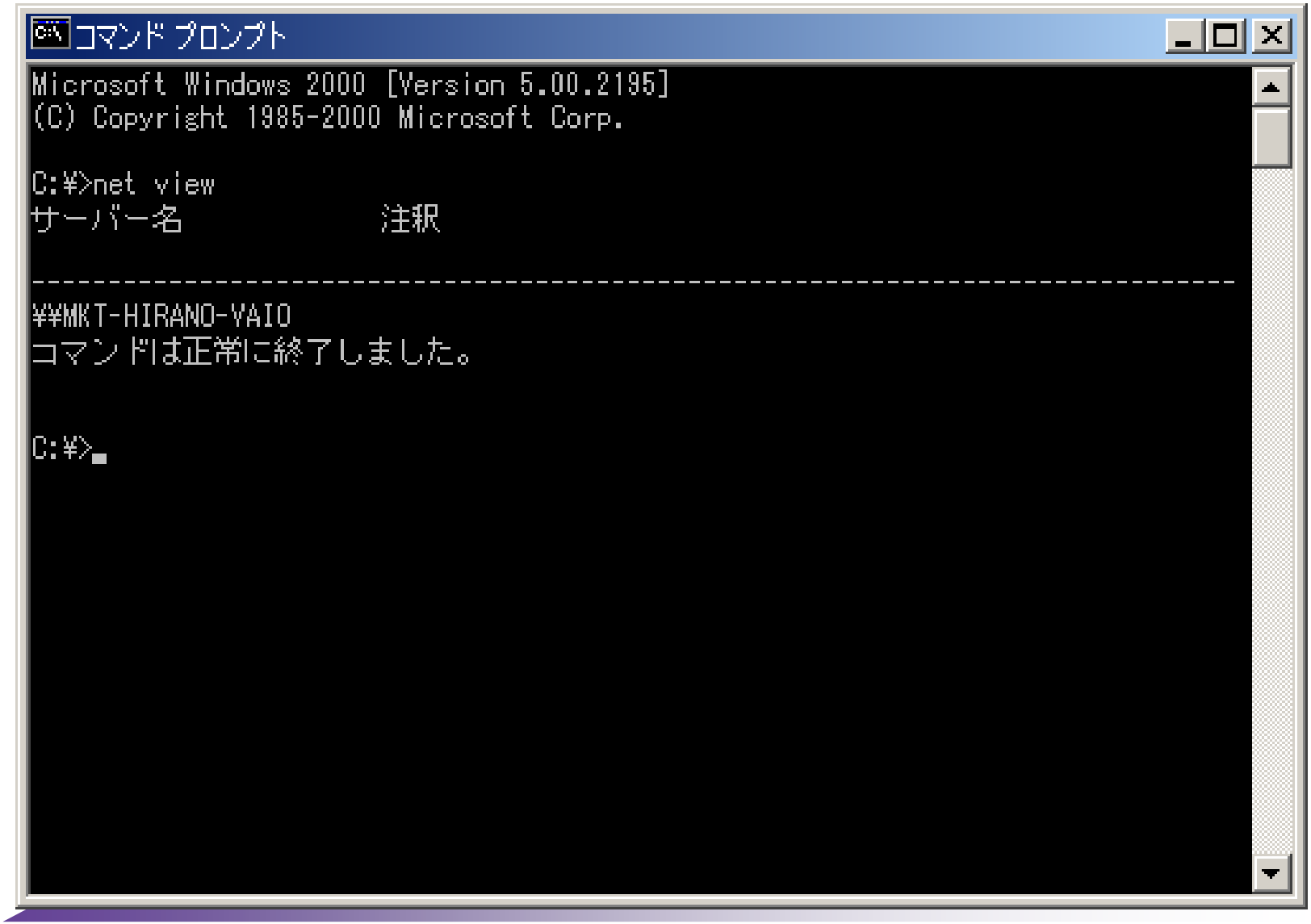
```
C:\>tftp

Transfers files to and from a remote computer running the TFTP service.

TFTP [-i] host [GET | PUT] source [destination]

  -i              Specifies binary image transfer mode (also called
                  octet). In binary image mode the file is moved
                  literally, byte by byte. Use this mode when
                  transferring binary files.
  host            Specifies the local or remote host.
  GET             Transfers the file destination on the remote host to
                  the file source on the local host.
  PUT             Transfers the file source on the local host to
                  the file destination on the remote host.
  source          Specifies the file to transfer.
  destination     Specifies where to transfer the file.
```

※Windowsの場合、tftpコマンドより、RT-RevUpperが便利。

net コマンドのヘルプ

```
C:\>net help
このコマンドの構文は次のとおりです:


NET HELP コマンド
      -または-
NET コマンド /HELP

指定できるコマンドは、次のとおりです。

NET ACCOUNTS              NET HELP              NET SHARE
NET COMPUTER              NET HELPMSG           NET START
NET CONFIG                NET LOCALGROUP        NET STATISTICS
NET CONFIG SERVER         NET NAME              NET STOP
NET CONFIG WORKSTATION    NET PAUSE             NET TIME
NET CONTINUE              NET PRINT             NET USE
NET FILE                  NET SEND              NET USER
NET GROUP                 NET SESSION           NET VIEW

NET HELP SERVICES は、開始することができるネットワーク サービスの一覧
を表示します。
NET HELP SYNTAX は、NET HELP の構文の表記規則を表示します。
NET HELP コマンド | MORE で、ヘルプを 1 画面ずつ表示します。
```

net view



トラブル対策の道具(そのほか)
～知識の整理～

- TeraTerm Pro (**ターミナルソフト**、telnet**クライアント**)
- ethereal + WinPcap (**パケットキャプチャ**)
- Macintosh**用**ping,tracertoute,nslookup**ツール→**WhatRoute
- RT-Utility (RT-Tftp Clients)
- RT-RevUpper (**リビジョンアップ・ユーティリティ**)
- **ユーザーさんが作ってくれたユーティリティ**

TeraTerm Pro

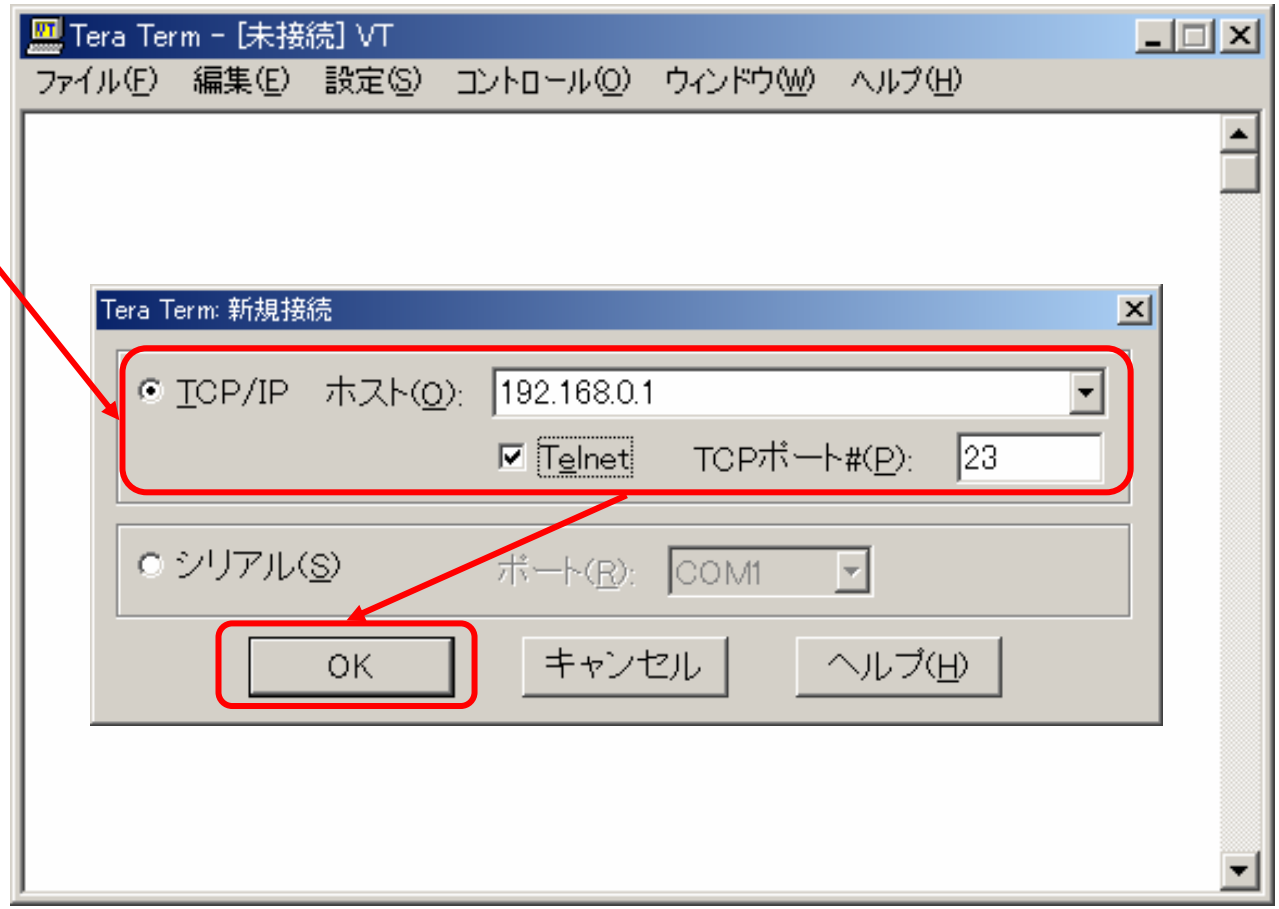
Tera Term Pro

Windows用のフリーソフトウェアのターミナルエミュレータ(通信ソフト)です。VT100エミュレーション、telnet接続、シリアル接続などが可能です。
また、第三者によるTeraTermを拡張するモジュールもいくつか公開されています。
http://hp.vector.co.jp/authors/VA002416/

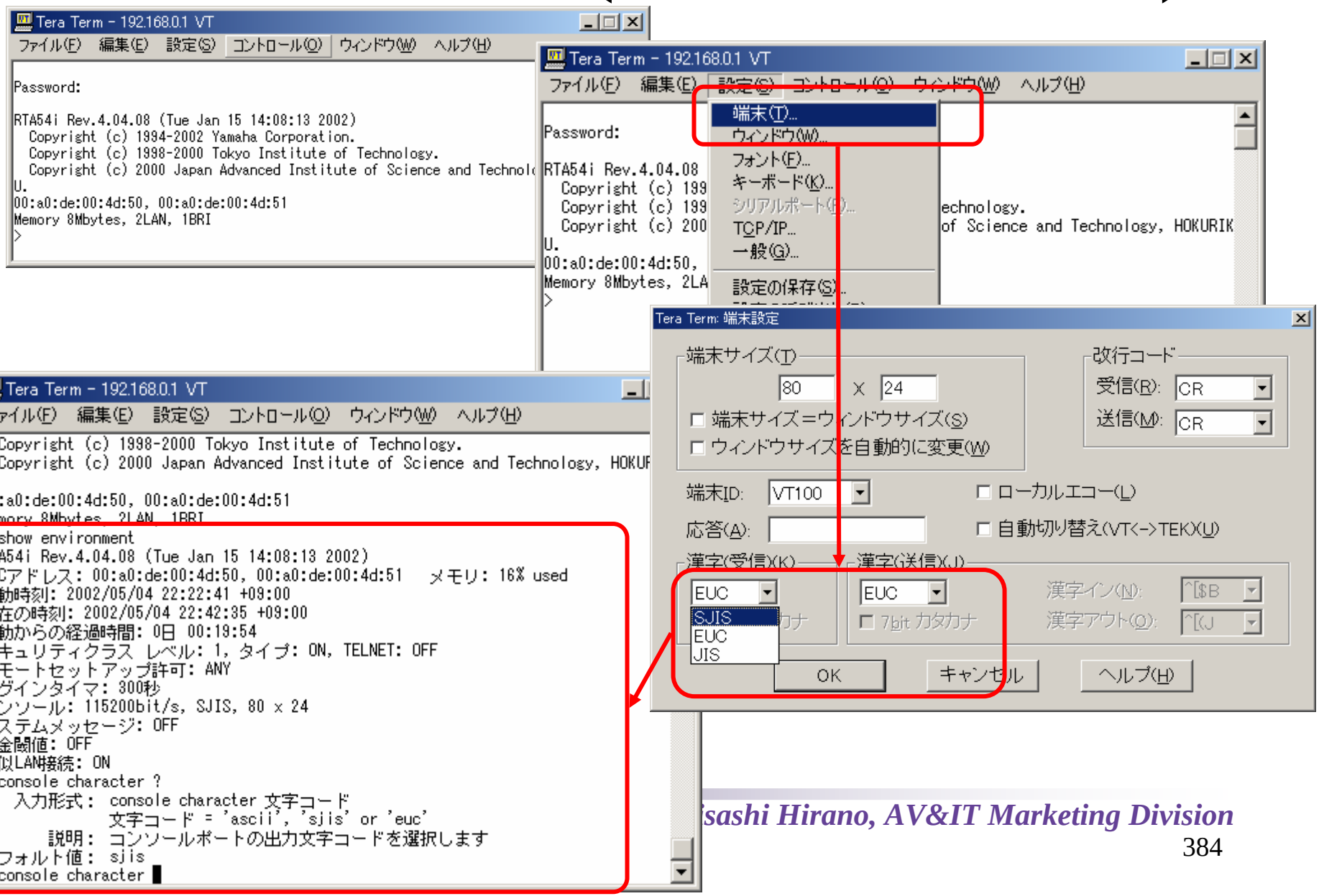
http://www.sakurachan.org/soft/teraterm-j/files/ttermp23.zip
ftp://www.sakurachan.org/pub/windows/net/term/teraterm/ttermp23.zip
http://www.vector.co.jp/authors/VA002416/ttermp23.zip
ftp://riksun.riken.go.jp/pub/pc/misc/terminal/teraterm/ttermp23.zip
ftp://ftp.forest.impress.co.jp/pub/win/winsock/apps/teraterm/ttermp23.zip
ftp://ftp.s.u-tokyo.ac.jp/PC/terminal/teraterm/ttermp23.zip

TeraTerm Pro (telnetで接続)

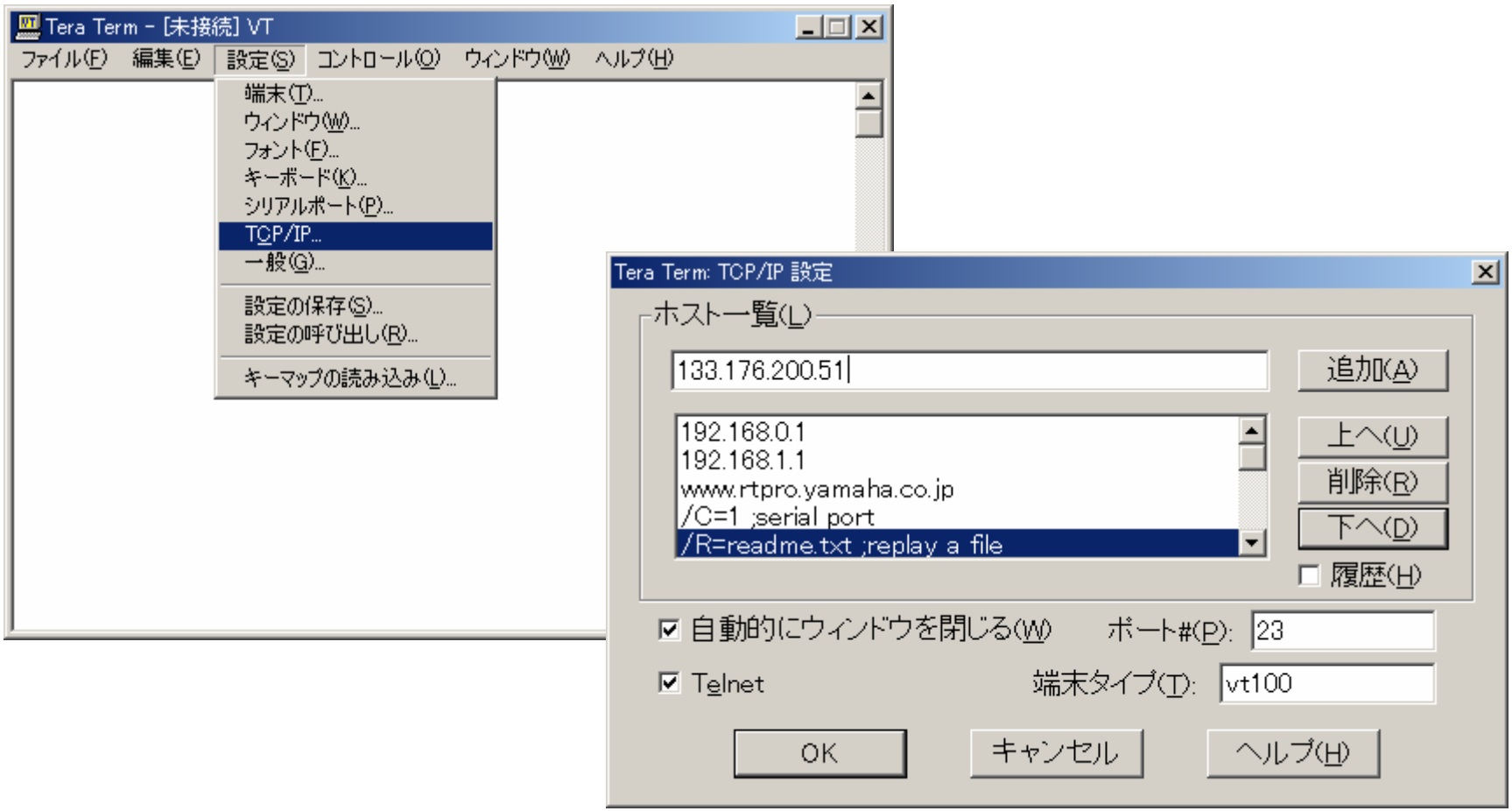
[スタート]
→[プログラム(P)]
→[Tera Term Pro]
→[Tera Term Pro]



TeraTerm Pro (漢字コード選択)



TeraTerm Pro (**接続先の登録**)



ethereal + WinPcap

ethereal

フリーのLANアナライザー(プロトコルアナライザー)
→いろいろなOSで利用できる
Windows2000/XPなど: WinPcapを併用する。
FreeBSD…ports
フィルタリングの書式は、UNIXのtcpdump準拠
http://www.ethereal.com/

WinPcap

Windows用キャプチャードライバー
http://netgroup-serv.polito.it/winpcap/install/default.htm

apache

apache

「NCSA httpdのパッチ」でスタートしたフリーのHTTP server
→元々、UNIX系だったが、現在では、Windowsでも利用可能
http://www.apache.org/
http://www.apache.jp/

→ C:¥Program Files¥Apache Group¥Apache

netperf

netperf

UNIX用のパフォーマンス測定ツール
→元々、UNIX系だったが、現在では、Windowsでも利用可能
http://www.netperf.org/

ftp://ftp.cup.hp.com/dist/networking/benchmarks/netperf/
(binaries**→**2.1**や**2.1pl1**などに**Win**版がある**)

[ネットで見つけた利用例紹介ページ]
http://trylan.fc2web.com/
http://trylan.fc2web.com/tools/tools_6.html

Macintosh用ping,tracerouteツール

Macintoshには、ping,traceroute,nslookupなどの確認をするツールが標準装備されていない。

WhatRoute

フリーソフトウェアのMacintosh用ping,traceroute,nslookupツールです。
WhatRoute無名時代にネットボランチRTA50iのCD-ROMに添付していました。
今では、代表的なツールになっています。
http://www.rtpro.yamaha.co.jp/RT/FAQ/Macintosh/ping.html
http://crash.ihug.co.nz/~bryanc/

RT-Utility

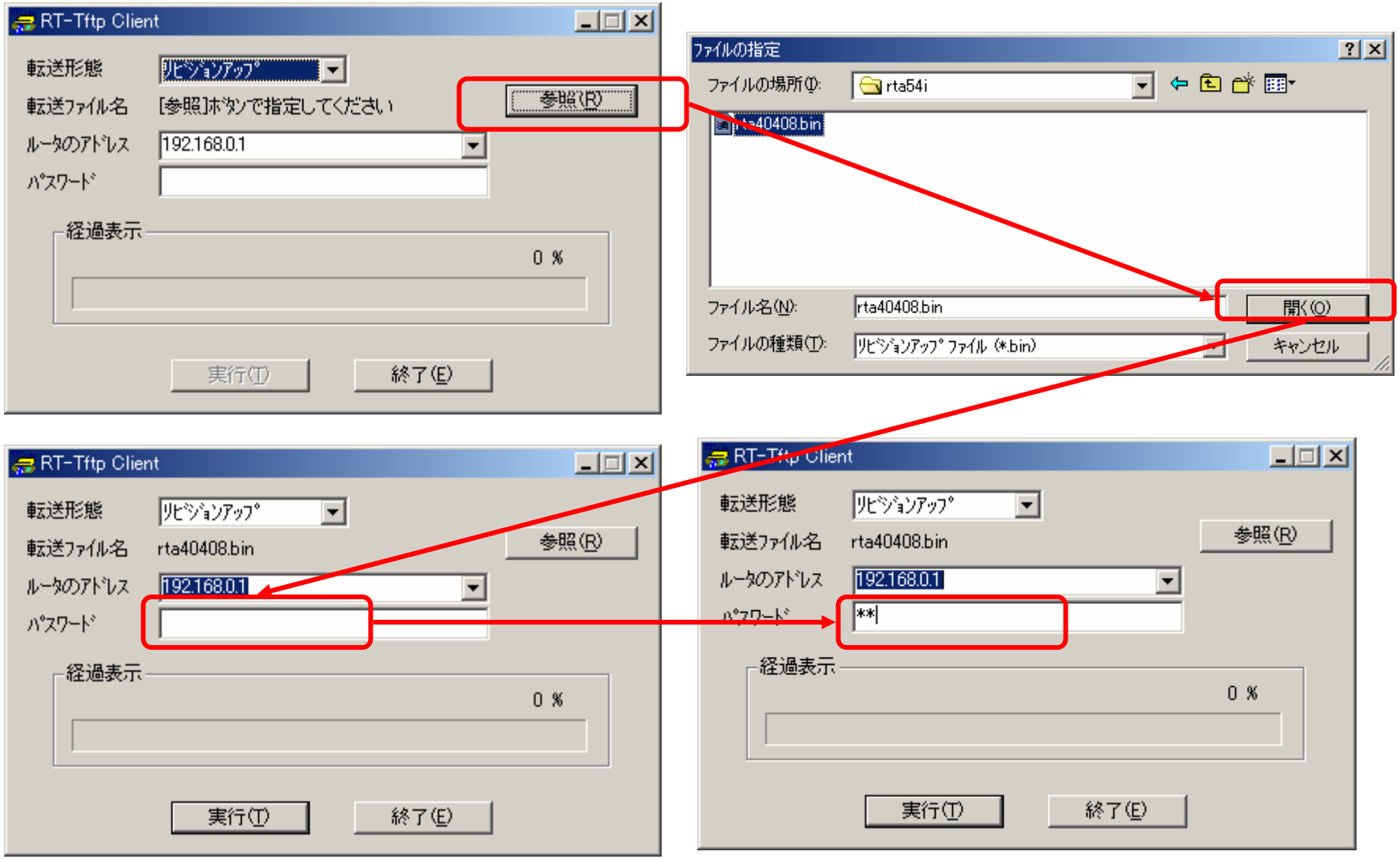
RT-Utility

ヤマハが提供するフリーのヤマハルーター用ユーティリティ
ファームウェアの更新、設定の取得・更新、接続や切断の
管理などを行うツールがある。

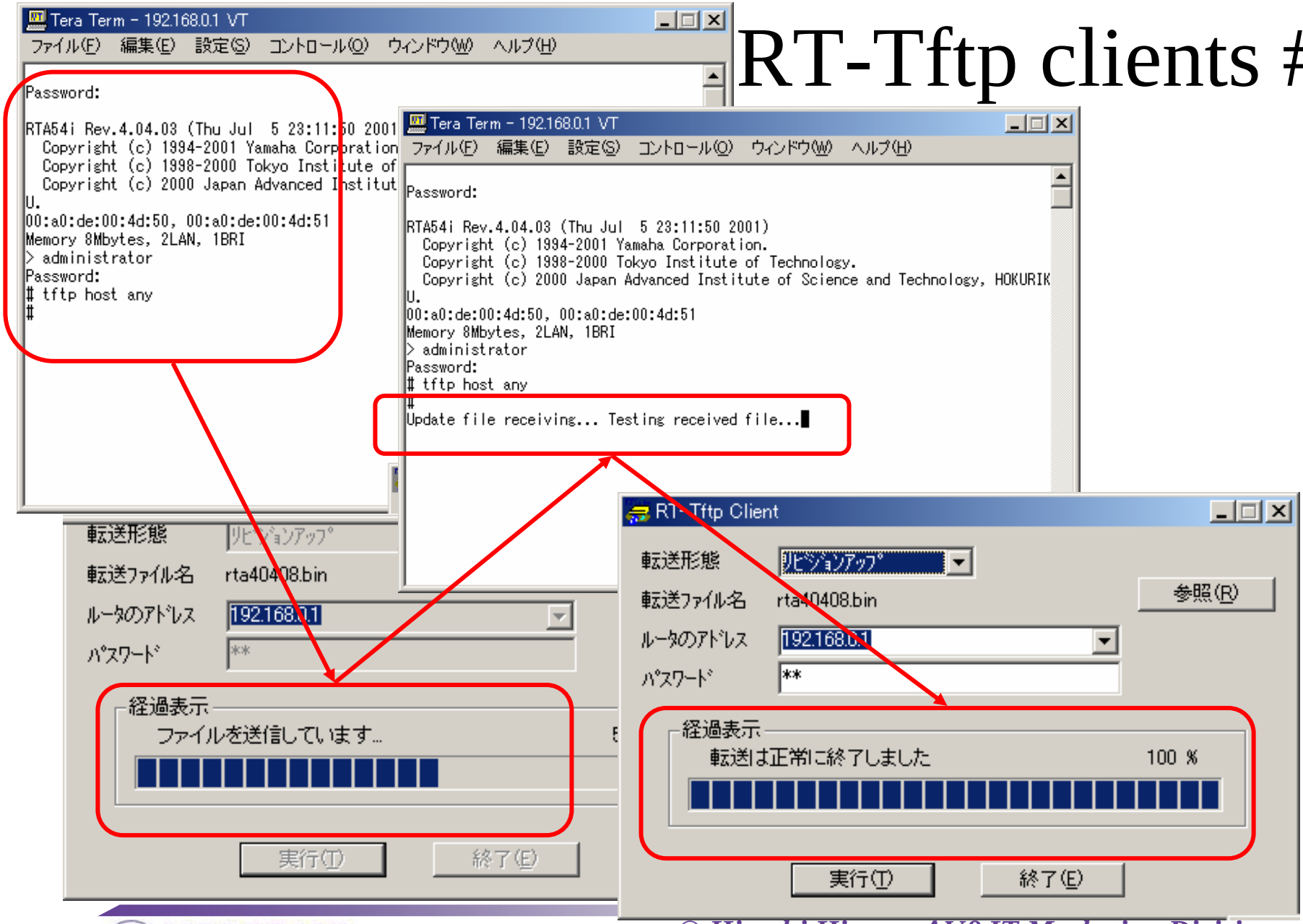
RT-Monitor: 接続切断の管理
RT-Tftp:ファームウェアの更新、設定の取得・更新
RT-Switch: 設定の切替

http://www.rtpro.yamaha.co.jp/RT/utility/index.html
http://www.rtpro.yamaha.co.jp/RT/utility/win32.html
http://www.rtpro.yamaha.co.jp/RT/utility/mac.html

RT-Tftp clients #1

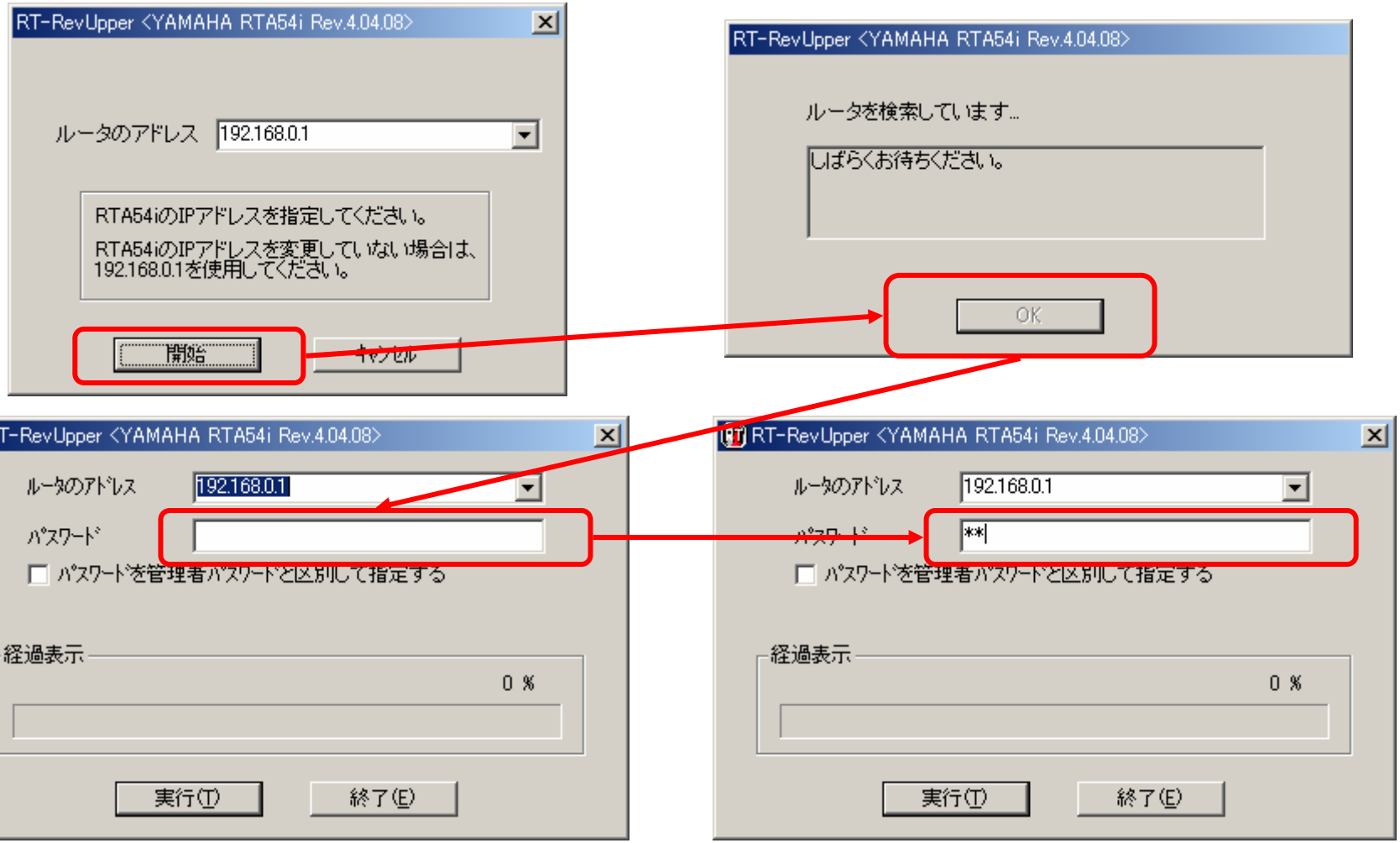


RT-Tftp clients #2

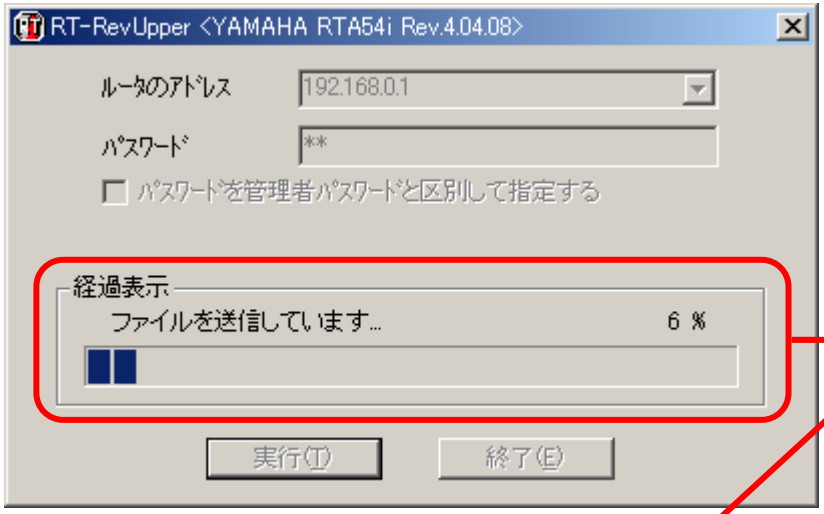


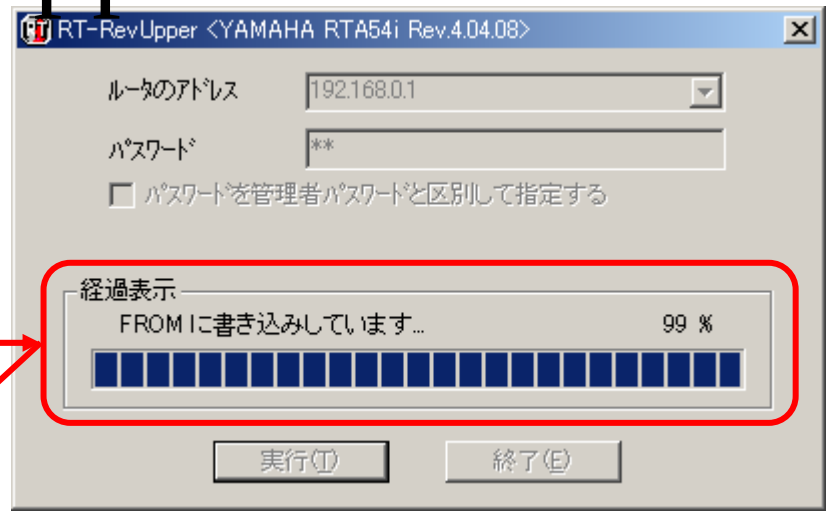
RT-RevUpper #1

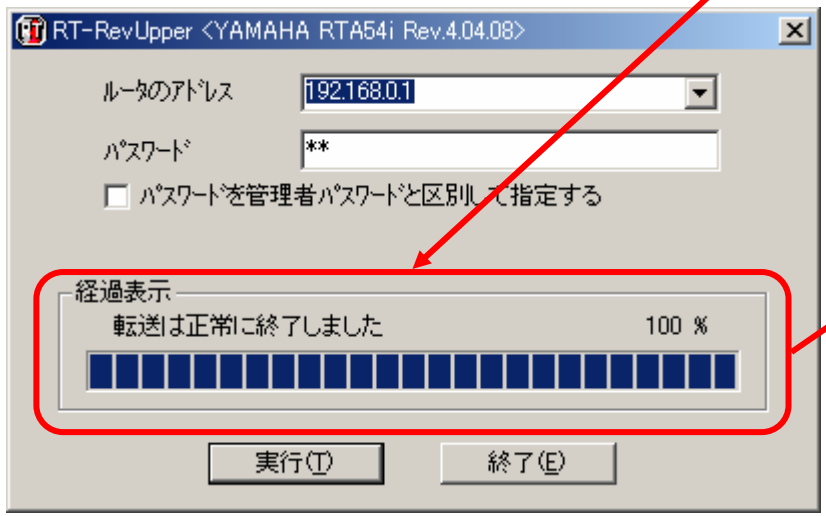
RT-Tftpクライアントとルーターのプログラムが一体になったアプリケーション

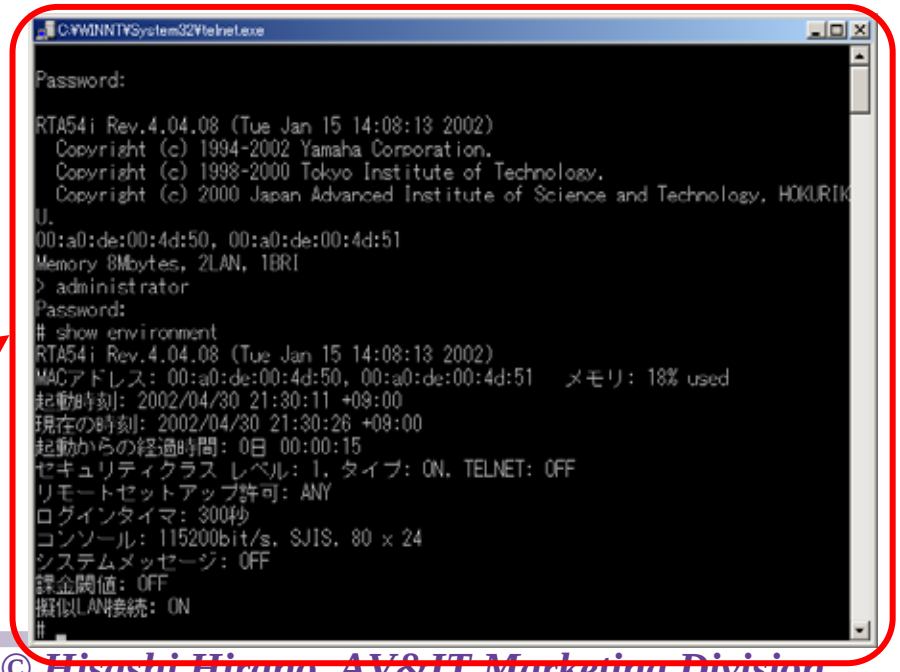


RT-RevUpper #2









転送終了後、自動的に再起動が始まる。LEDの点滅の後、ブザーが鳴り(再)起動...リビジョンアップが完了する。

ユーザーさんによるユーティリティ

kzsyslogd

ヤマハルーターのユーザーさんが開発してくれたルーターの出力するsyslogの情報をwindowsで受信してくれる。
http://www.gin.or.jp/users/bato/kzsyslog/index.html

RTCon

ヤマハルーターのユーザーさんが開発してくれた
ネットボランチを統合管理するユーティリティ
http://www.genesissoft.com/software/rtcon/

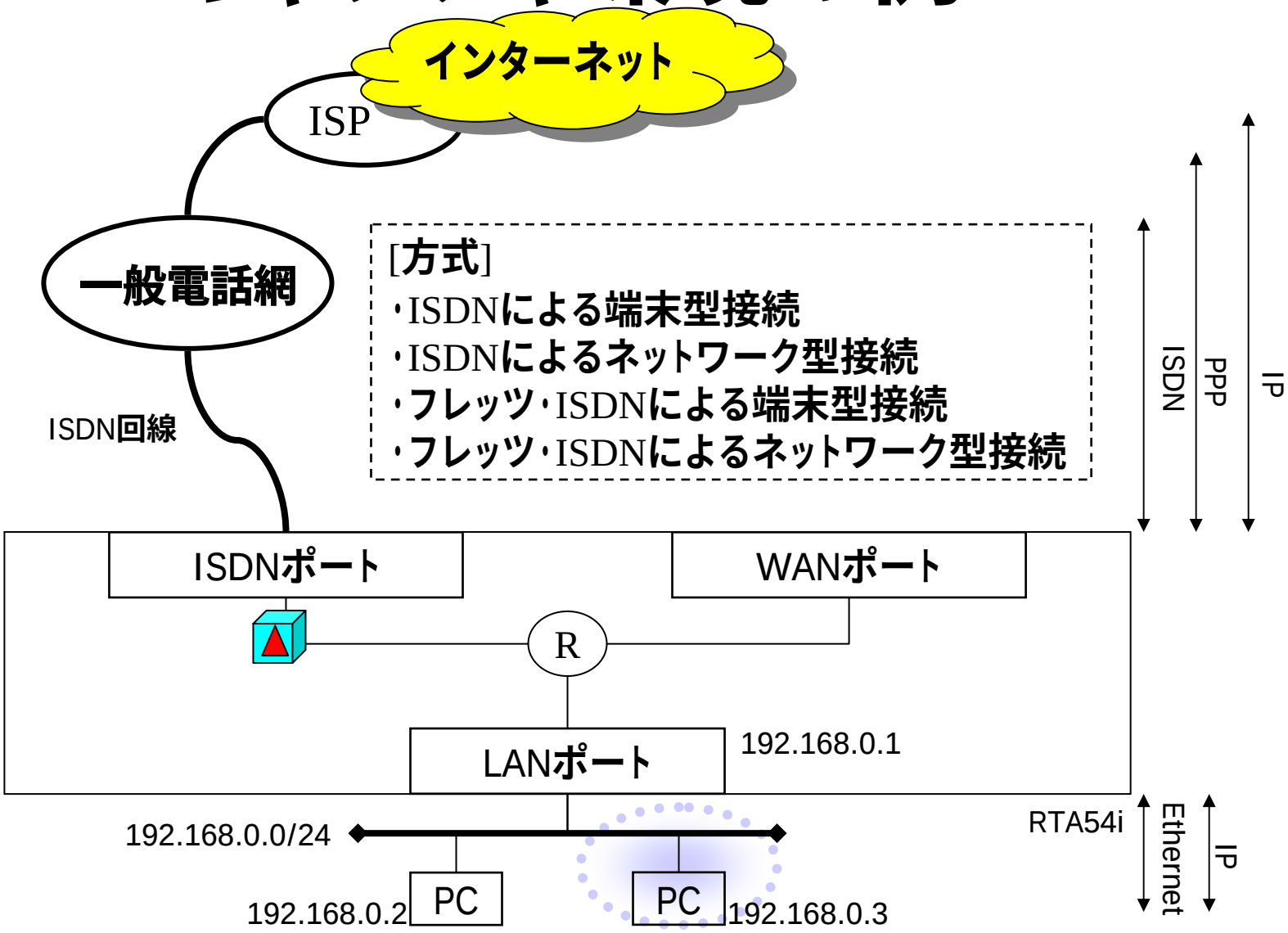
他にも色々

ヤマハルーターユーザーさんが開発してくれたユーティリティを紹介しています。
http://www.rtpro.yamaha.co.jp/RT/utility/of-by-for-win32.html
http://www.rtpro.yamaha.co.jp/RT/utility/of-by-for-mac.html
http://www.rtpro.yamaha.co.jp/RT/utility/of-by-for-unix.html

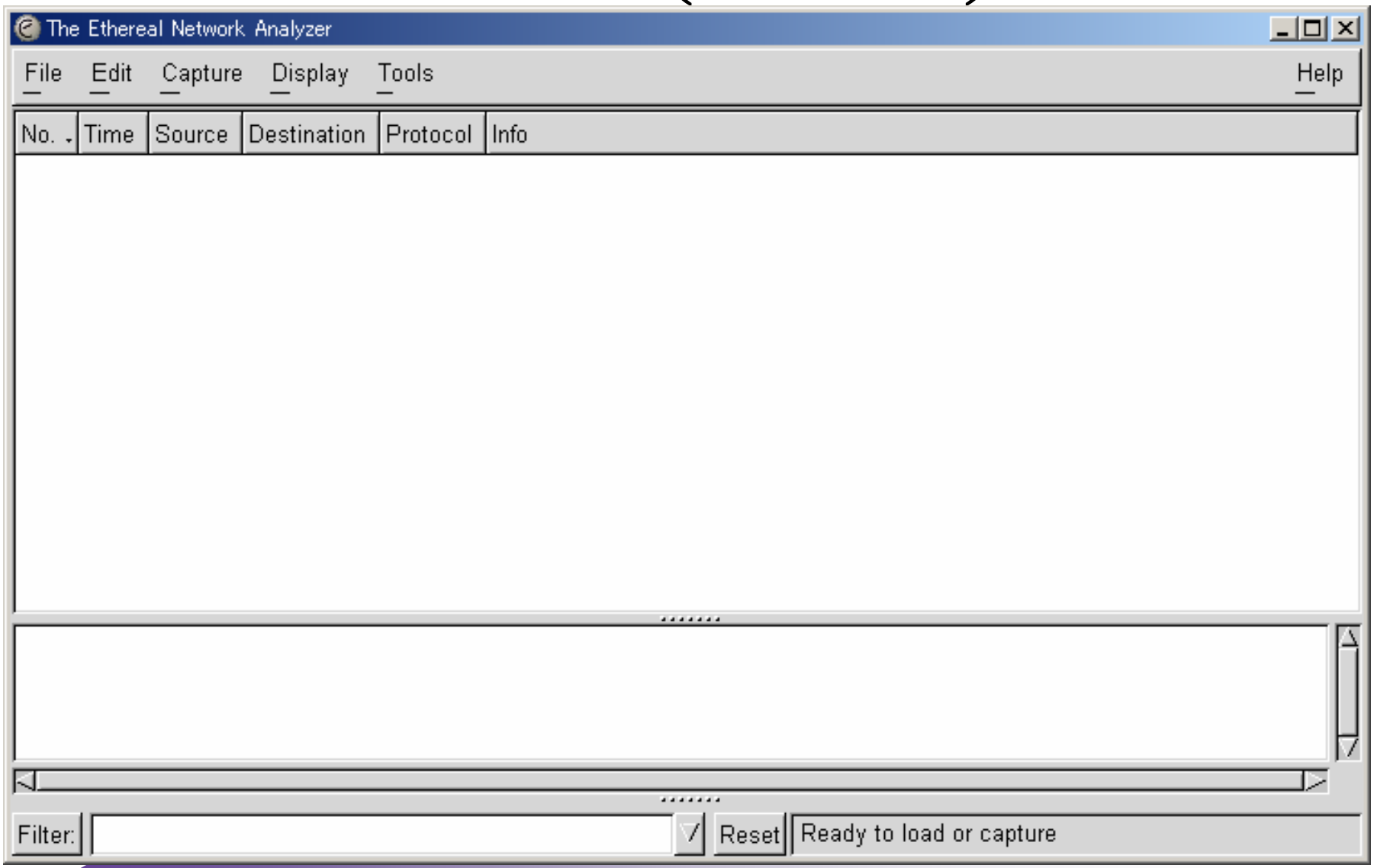
パケットのキャプチャ
～知識の整理～

- ethereal**の起動、キャプチャ**
  キャプチャ開始
  キャプチャ終了
- ping**の実行とパケットキャプチャ**
  ARP request/ARP reply
  ICMP echo request/echo reply
  arp**テーブルの確認**
- DNS**への問い合わせ**
  UDP**パケット**
- DHCP**パケットの観測**
  UDP**パケット**
- WWW**サーバへのアクセスとパケットキャプチャ**
  TCP**の**SYN**パケット**
  TCP**の最初のパケット**

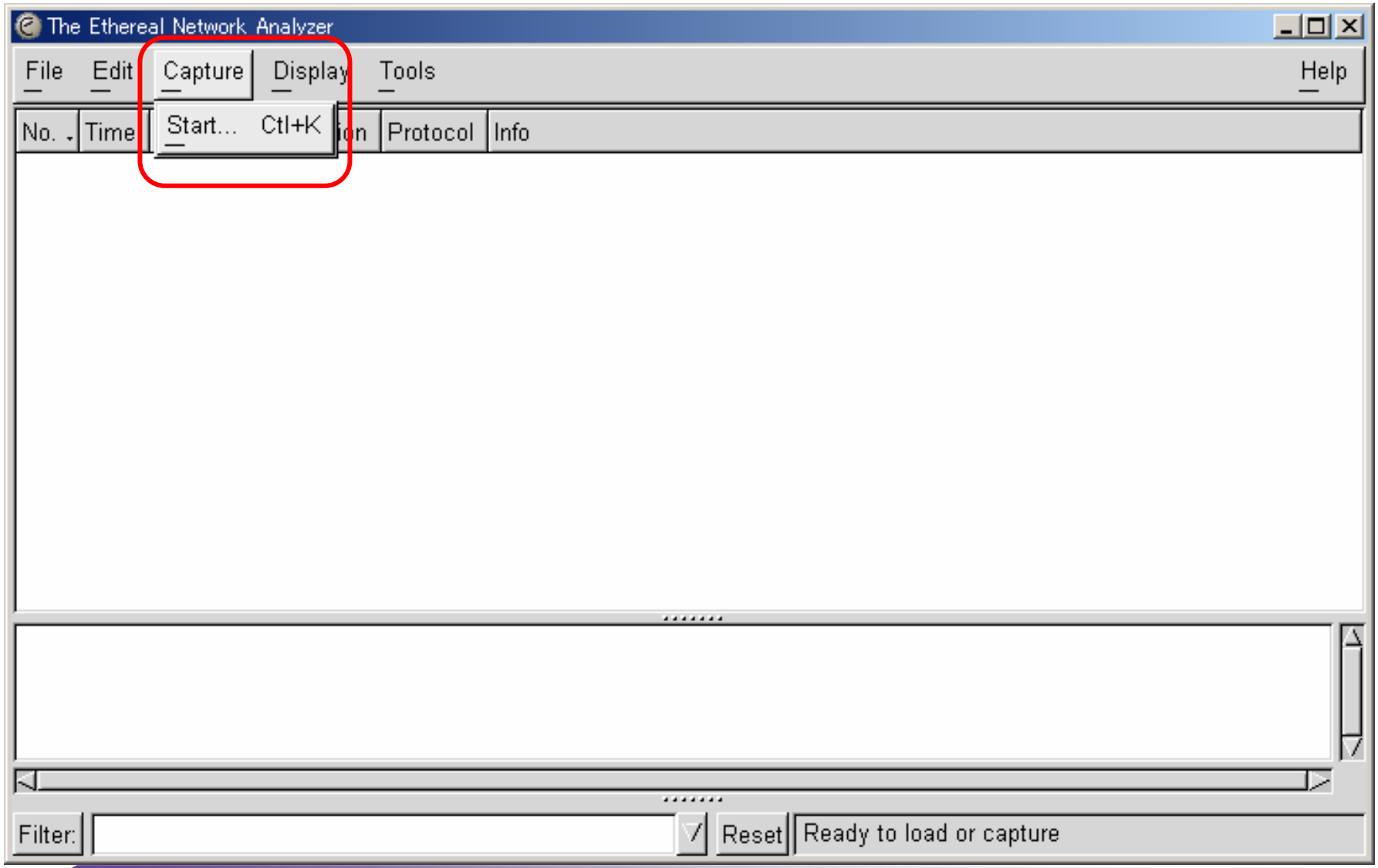
キャプチャ環境の例



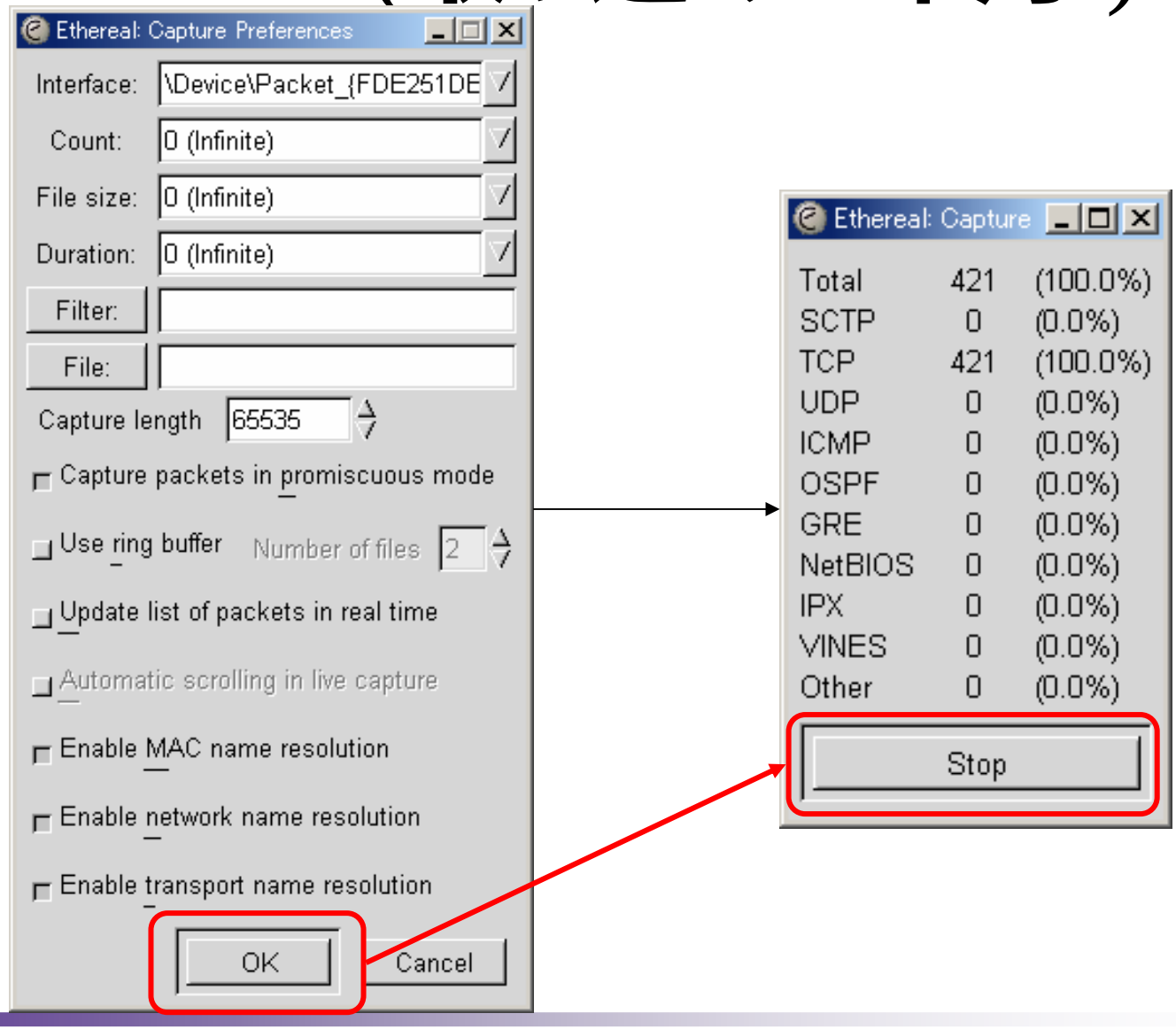
ethereal(**起動時**)



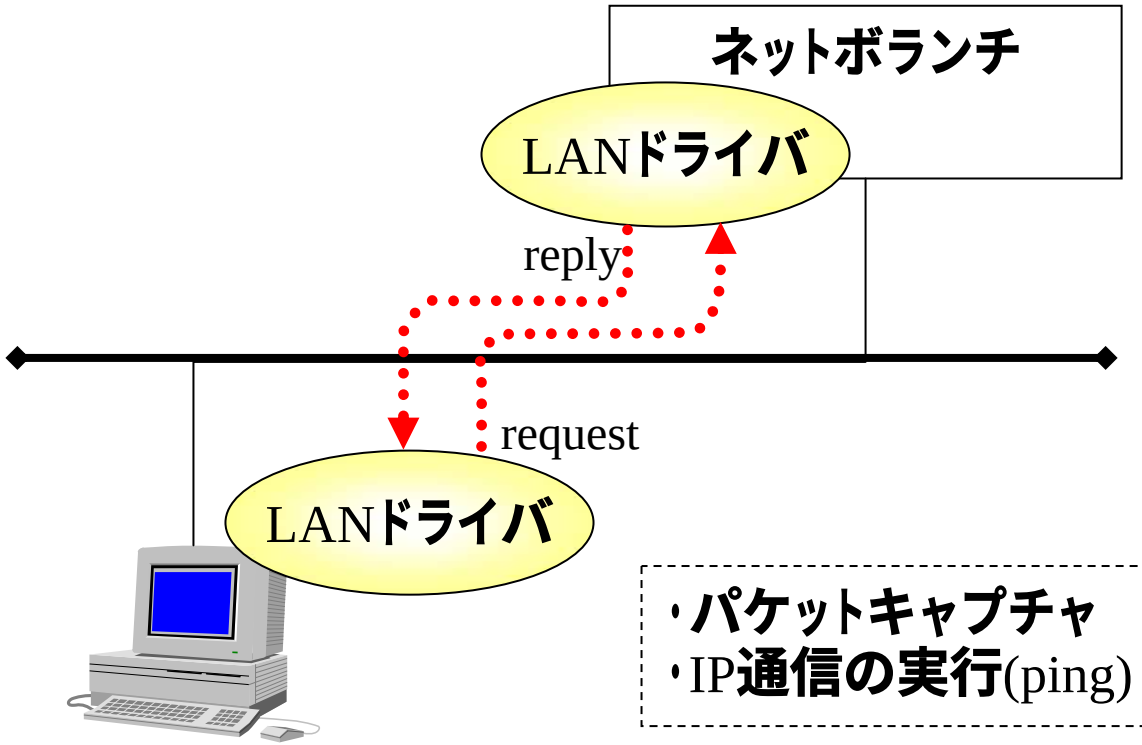
ethereal(キャプチャ開始)



ethereal(取り込み→終了)

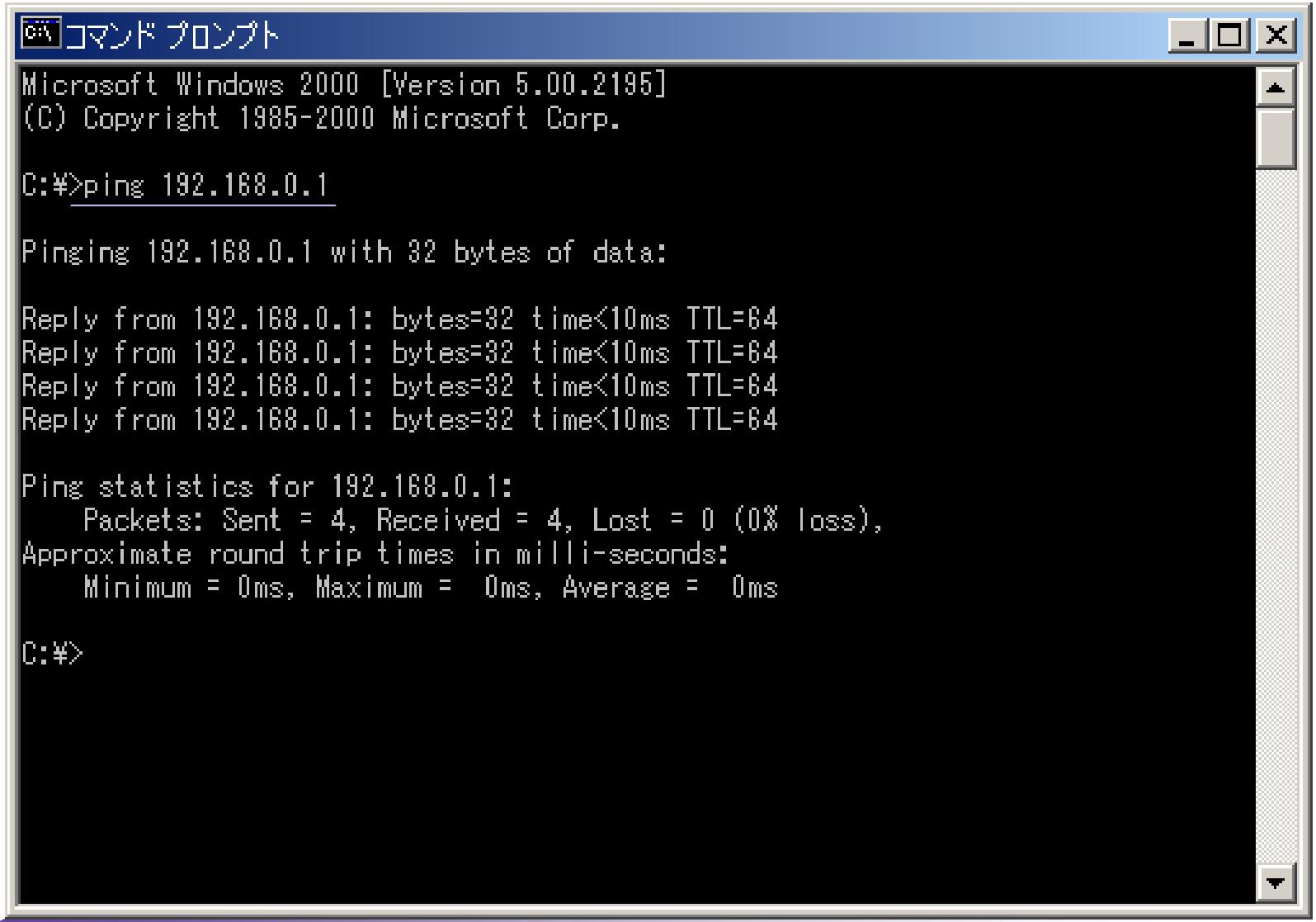


ARPパケットの観測環境

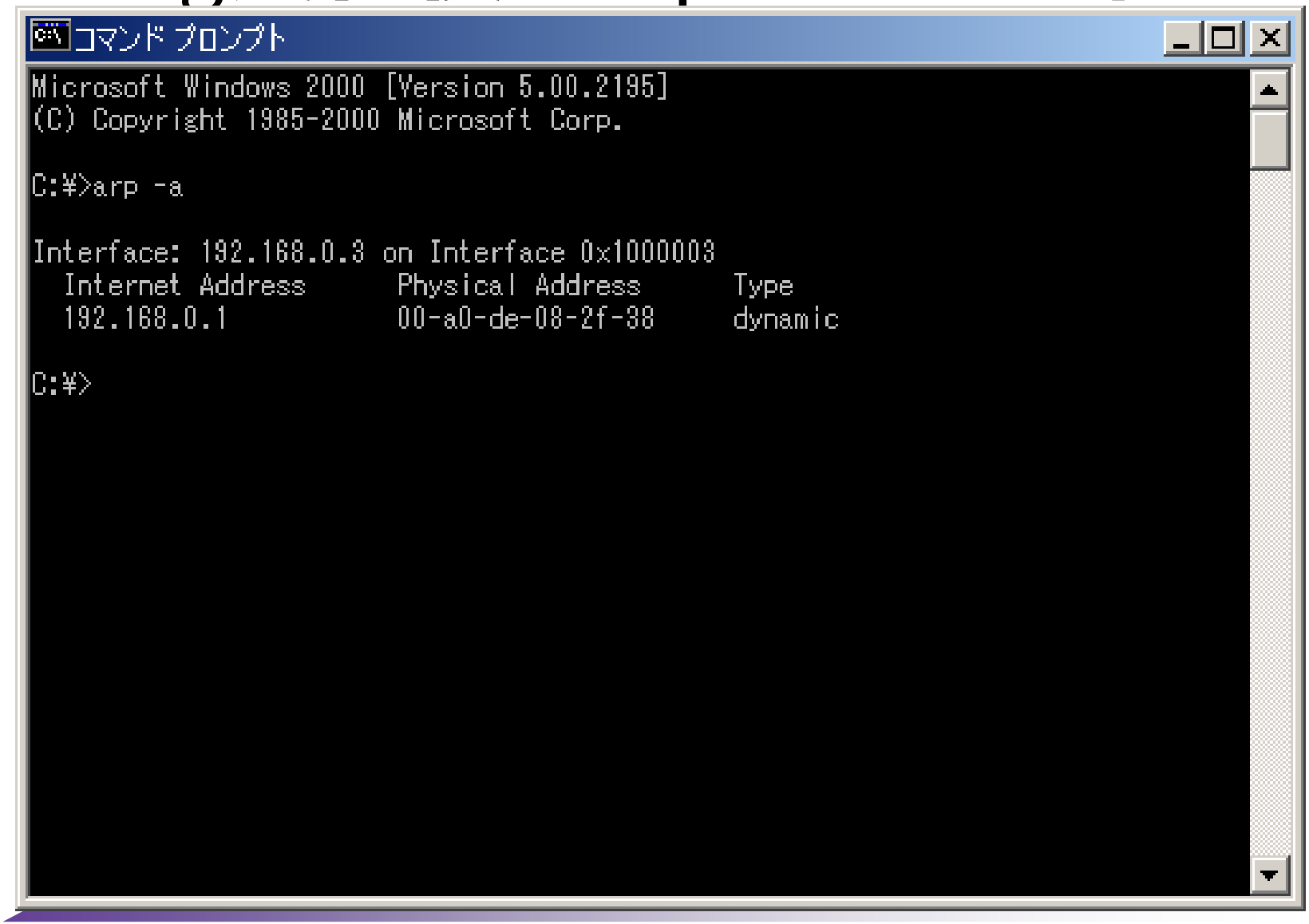


- パケットキャプチャ
- IP通信の実行(ping)

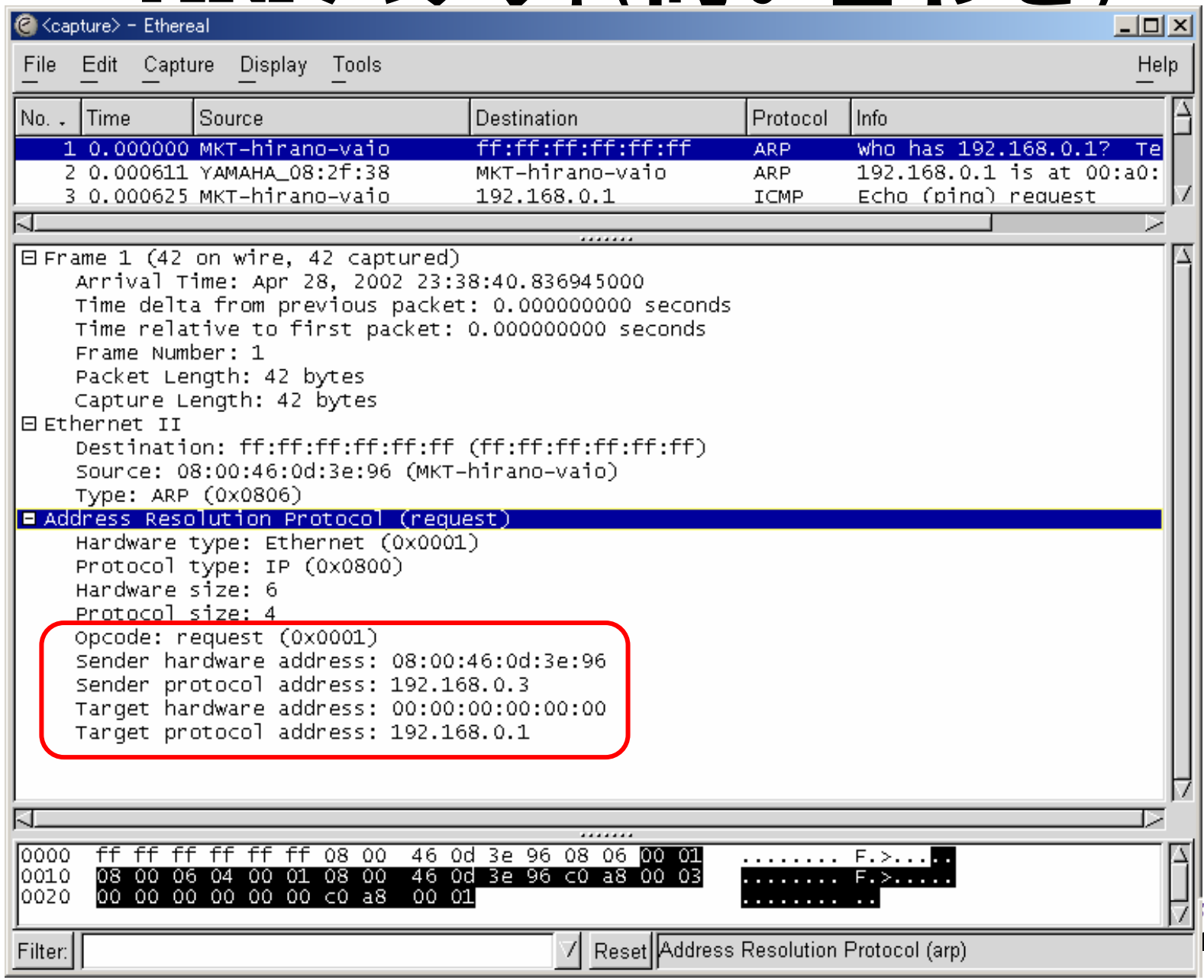
pingの実行とパケットキャプチャ



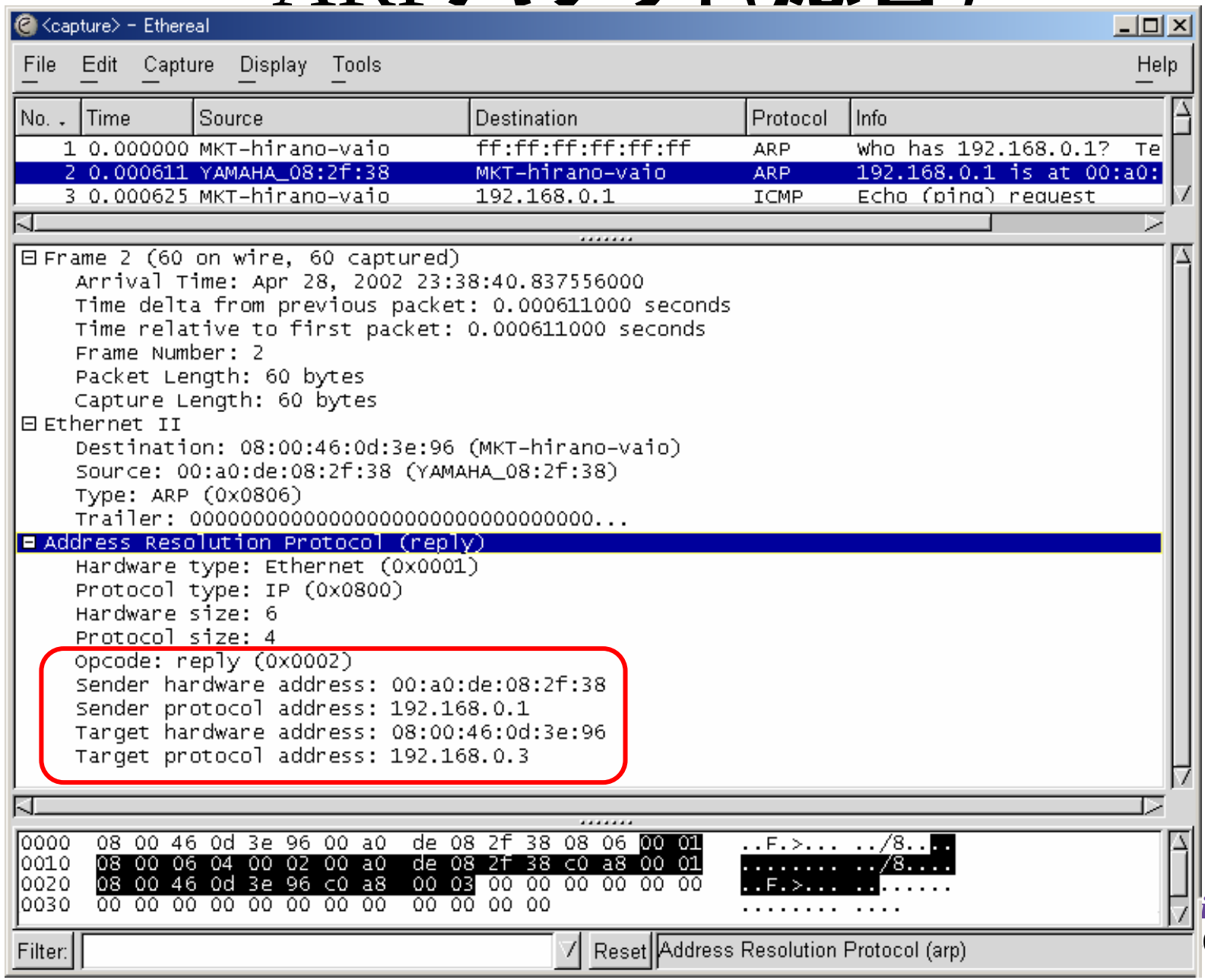
Ping実行後のarpテーブル確認



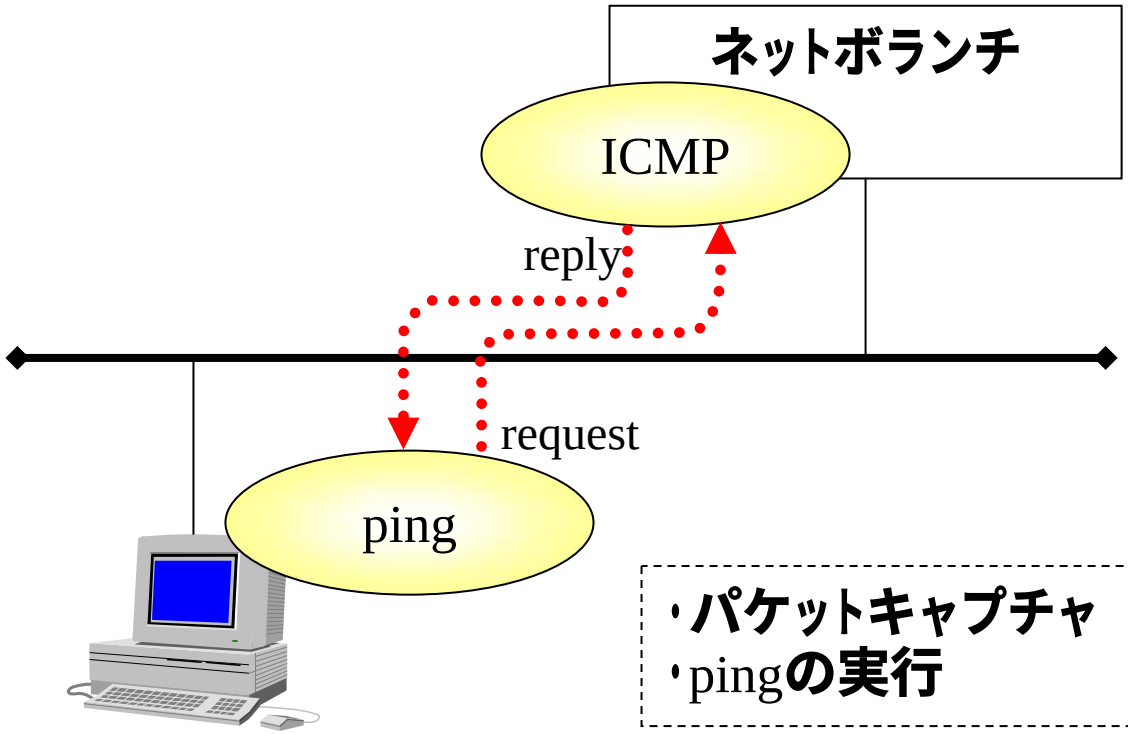
ARPパケット(問い合わせ)



ARPパケット(応答)

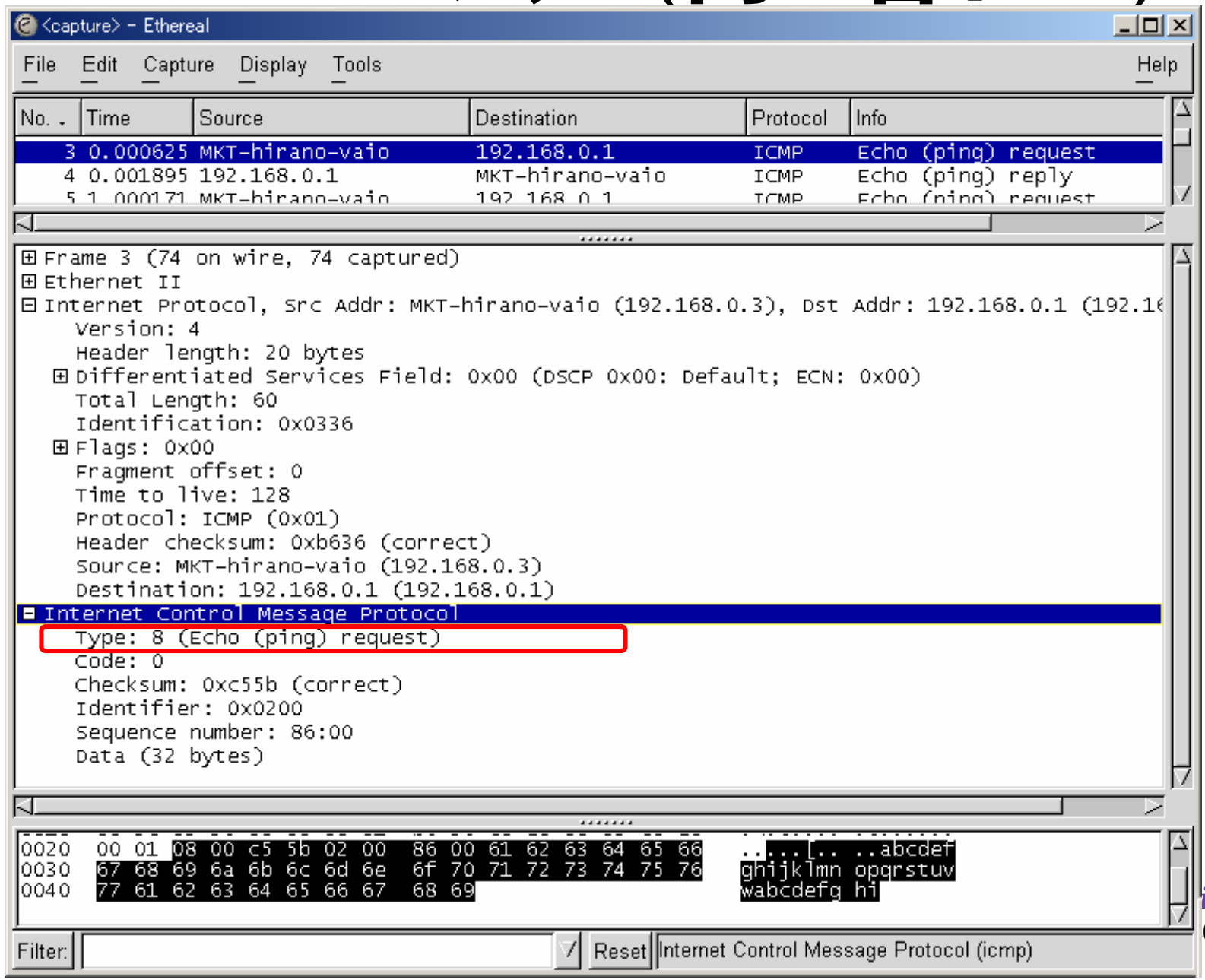

<capture> - Ethereal
File Edit Capture Display Tools Help
No. Time Source Destination Protocol Info
1 0.000000 MKT-hirano-vaio ff:ff:ff:ff:ff:ff ARP Who has 192.168.0.1? Te
2 0.000611 YAMAHA_08:2f:38 MKT-hirano-vaio ARP 192.168.0.1 is at 00:a0:
3 0.000625 MKT-hirano-vaio 192.168.0.1 ICMP Echo (ping) request
Frame 2 (60 on wire, 60 captured)
Arrival Time: Apr 28, 2002 23:38:40.837556000
Time delta from previous packet: 0.000611000 seconds
Time relative to first packet: 0.000611000 seconds
Frame Number: 2
Packet Length: 60 bytes
Capture Length: 60 bytes
Ethernet II
Destination: 08:00:46:0d:3e:96 (MKT-hirano-vaio)
Source: 00:a0:de:08:2f:38 (YAMAHA_08:2f:38)
Type: ARP (0x0806)
Trailer: 00000000000000000000000000000000...
Address Resolution Protocol (reply)
Hardware type: Ethernet (0x0001)
Protocol type: IP (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (0x0002)
Sender hardware address: 00:a0:de:08:2f:38
Sender protocol address: 192.168.0.1
Target hardware address: 08:00:46:0d:3e:96
Target protocol address: 192.168.0.3
0000 08 00 46 0d 3e 96 00 a0 de 08 2f 38 08 06 00 01
0010 08 00 06 04 00 02 00 a0 de 08 2f 38 c0 a8 00 01
0020 08 00 46 0d 3e 96 c0 a8 00 03 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
Filter:
Reset
Address Resolution Protocol (arp)

ICMPパケットの観測環境

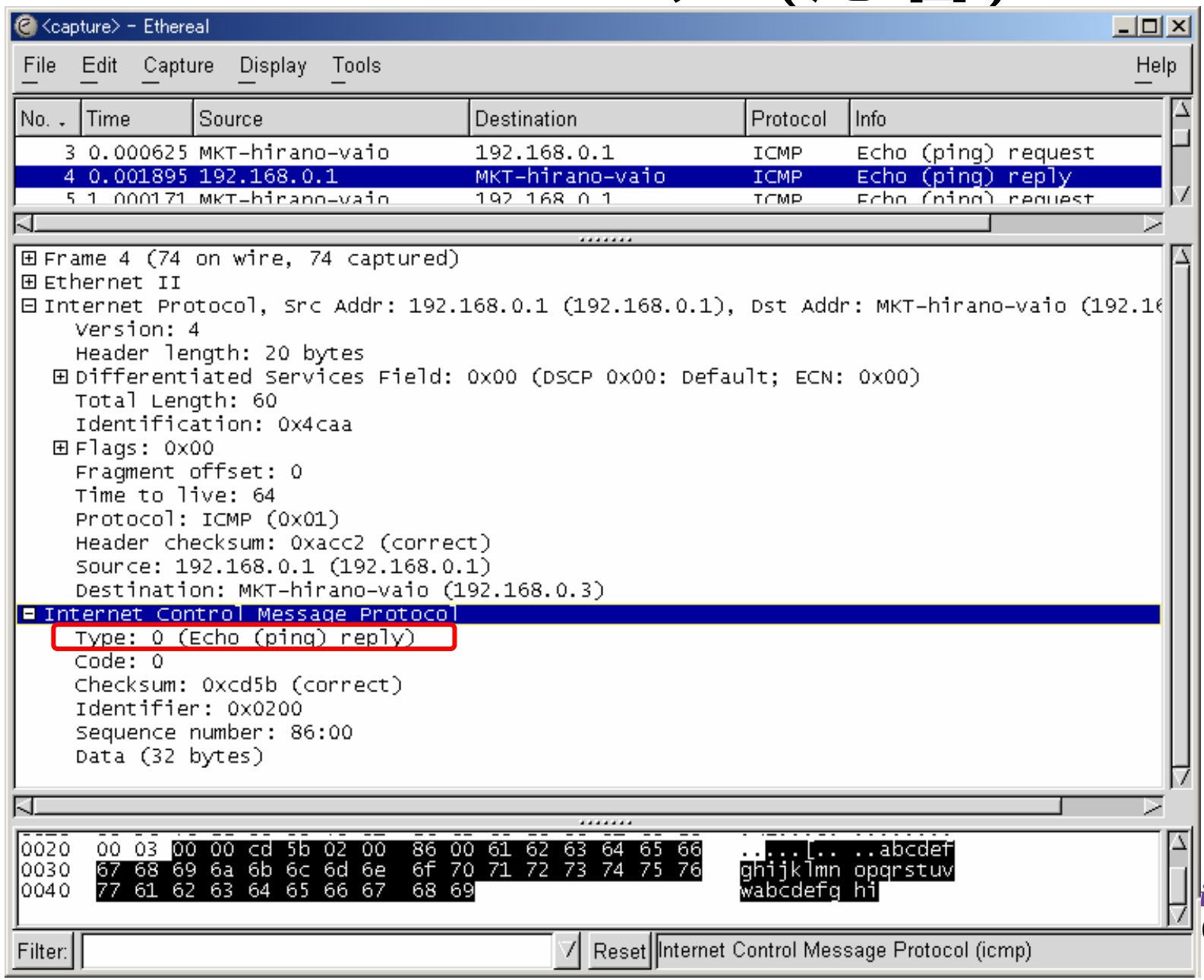


・パケットキャプチャ
・pingの実行

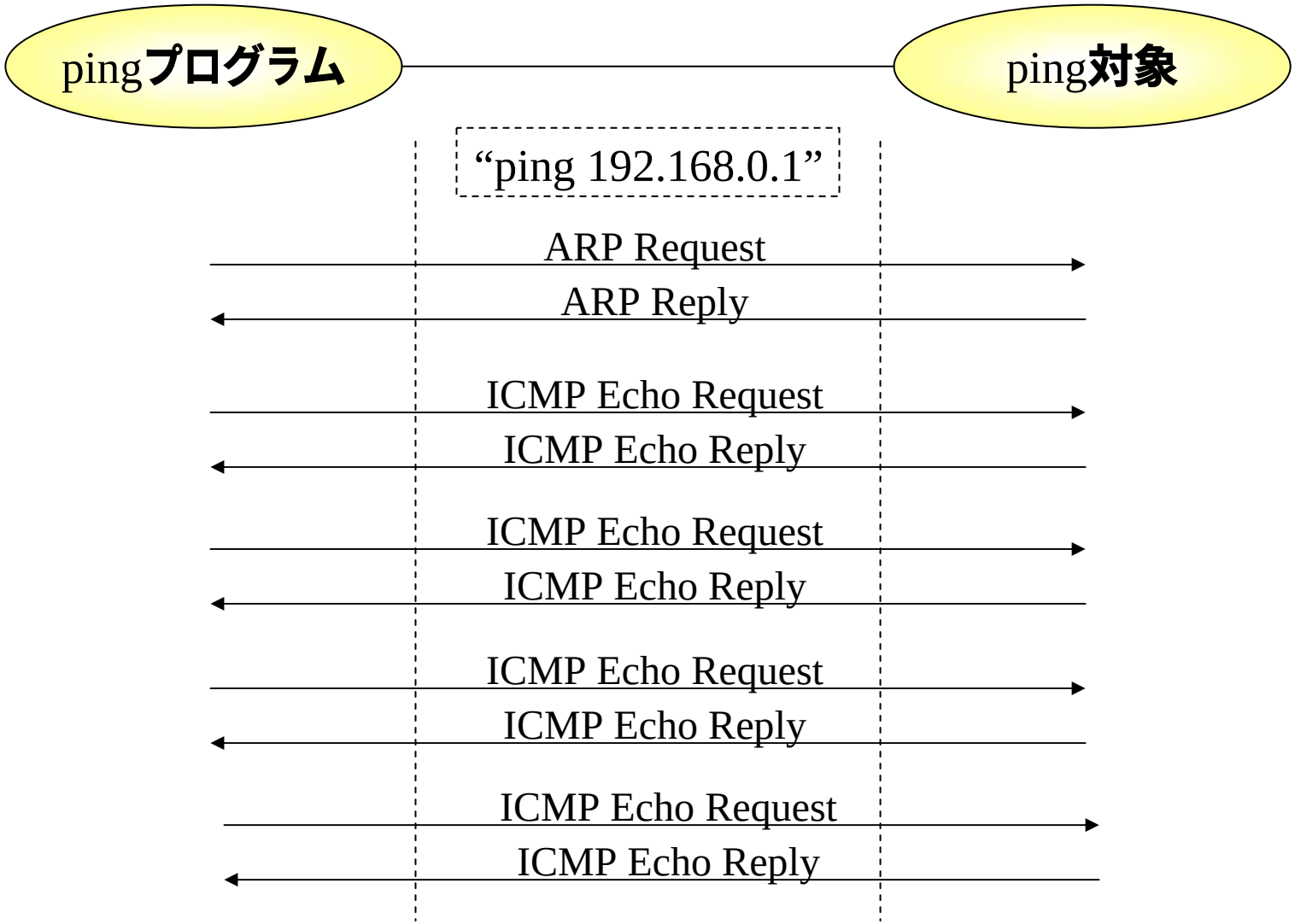
ICMP パケット (問い合わせ)



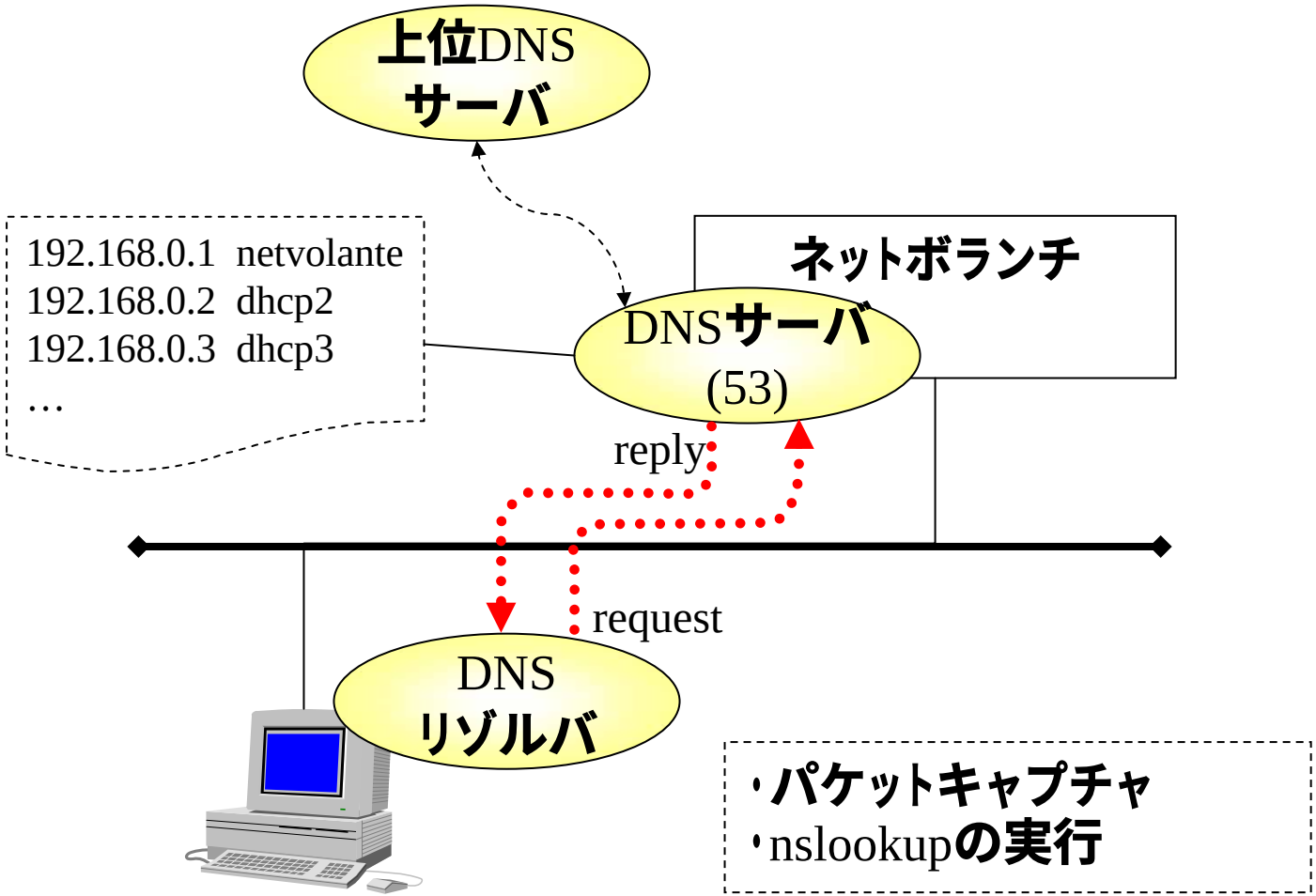
ICMP パケット(応答)


<capture> - Ethereal
File Edit Capture Display Tools Help
No. Time Source Destination Protocol Info
3 0.000625 MKT-hirano-vaio 192.168.0.1 ICMP Echo (ping) request
4 0.001895 192.168.0.1 MKT-hirano-vaio ICMP Echo (ping) reply
Frame 4 (74 on wire, 74 captured)
Ethernet II
Internet Protocol, Src Addr: 192.168.0.1 (192.168.0.1), Dst Addr: MKT-hirano-vaio (192.16
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
Total Length: 60
Identification: 0x4caa
Flags: 0x00
Fragment offset: 0
Time to live: 64
Protocol: ICMP (0x01)
Header checksum: 0xacc2 (correct)
Source: 192.168.0.1 (192.168.0.1)
Destination: MKT-hirano-vaio (192.168.0.3)
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0xcd5b (correct)
Identifier: 0x0200
Sequence number: 86:00
Data (32 bytes)
0020 00 03 00 00 cd 5b 02 00 86 00 61 62 63 64 65 66 .....[.. ..abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi
Filter:
Reset
Internet Control Message Protocol (icmp)

ping動作

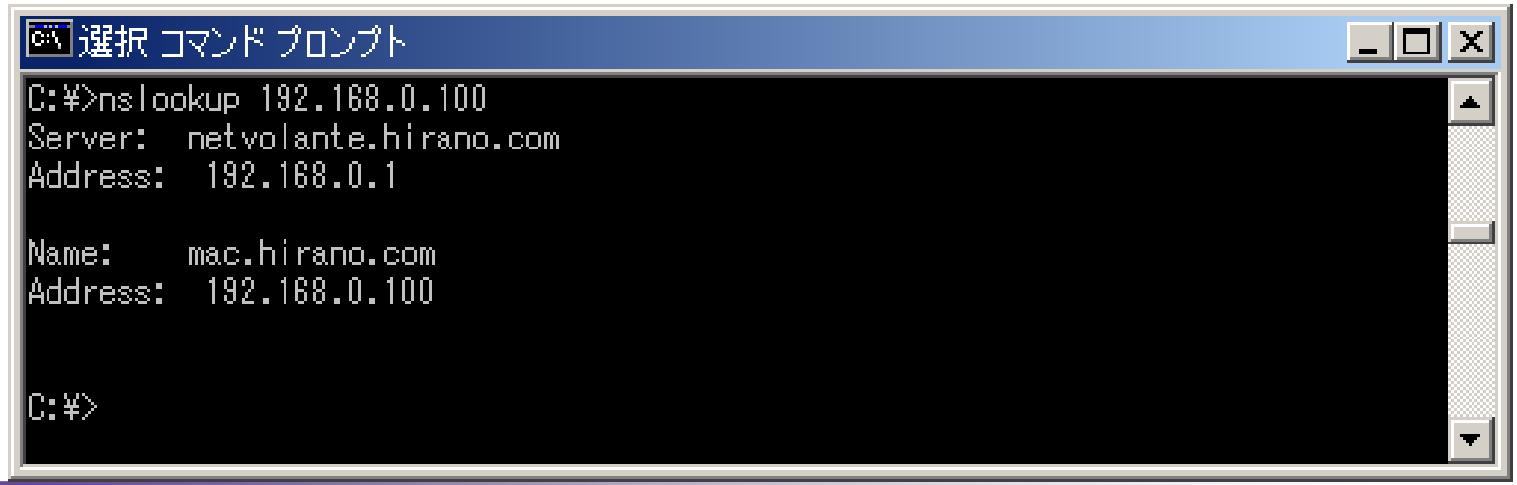


UDPパケットの観測環境

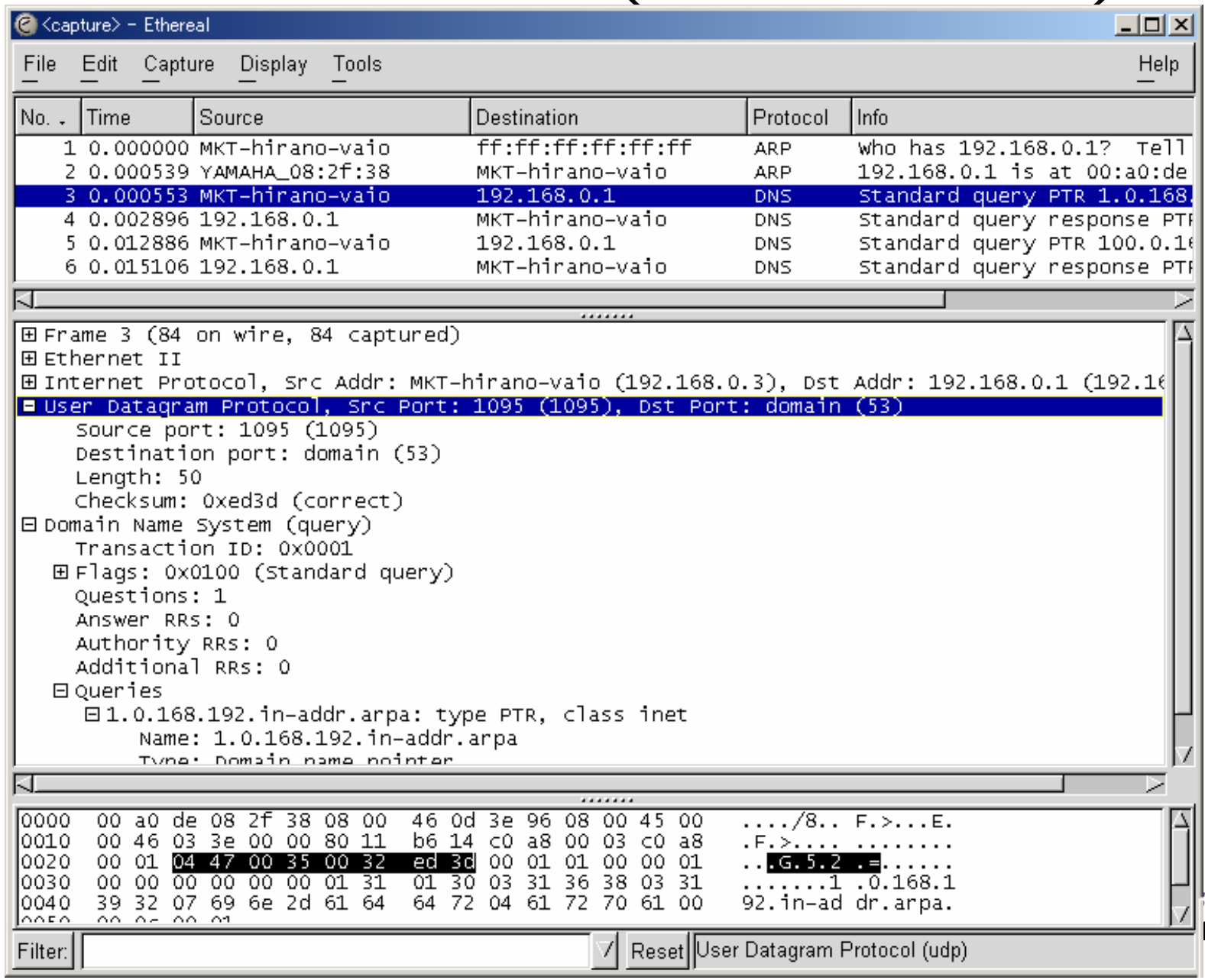


UDPパケット(DNSの問い合わせ)

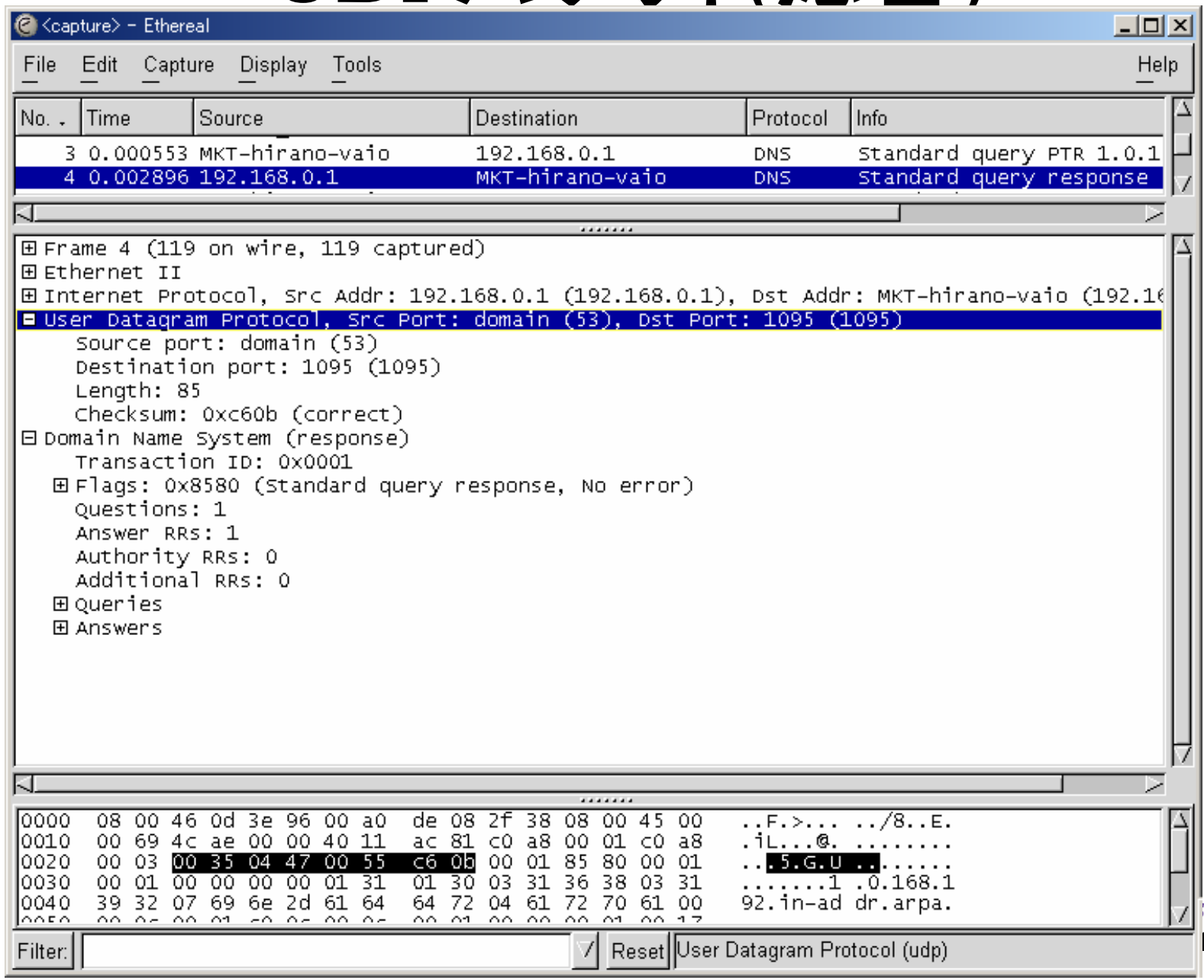
[**設定**]
dhcp service server
dhcp scope 1 192.168.0.2-192.168.0.254/24
dns server **プロバイダの**DNS**名**
dns private address spoof on
ip host mac.hirano.com 192.168.0.100
ip host netvolante.hirano.com 192.168.0.1
ip host dhcp2.hirano.com 192.168.0.2
ip host dhcp3.hirano.com 192.168.0.3



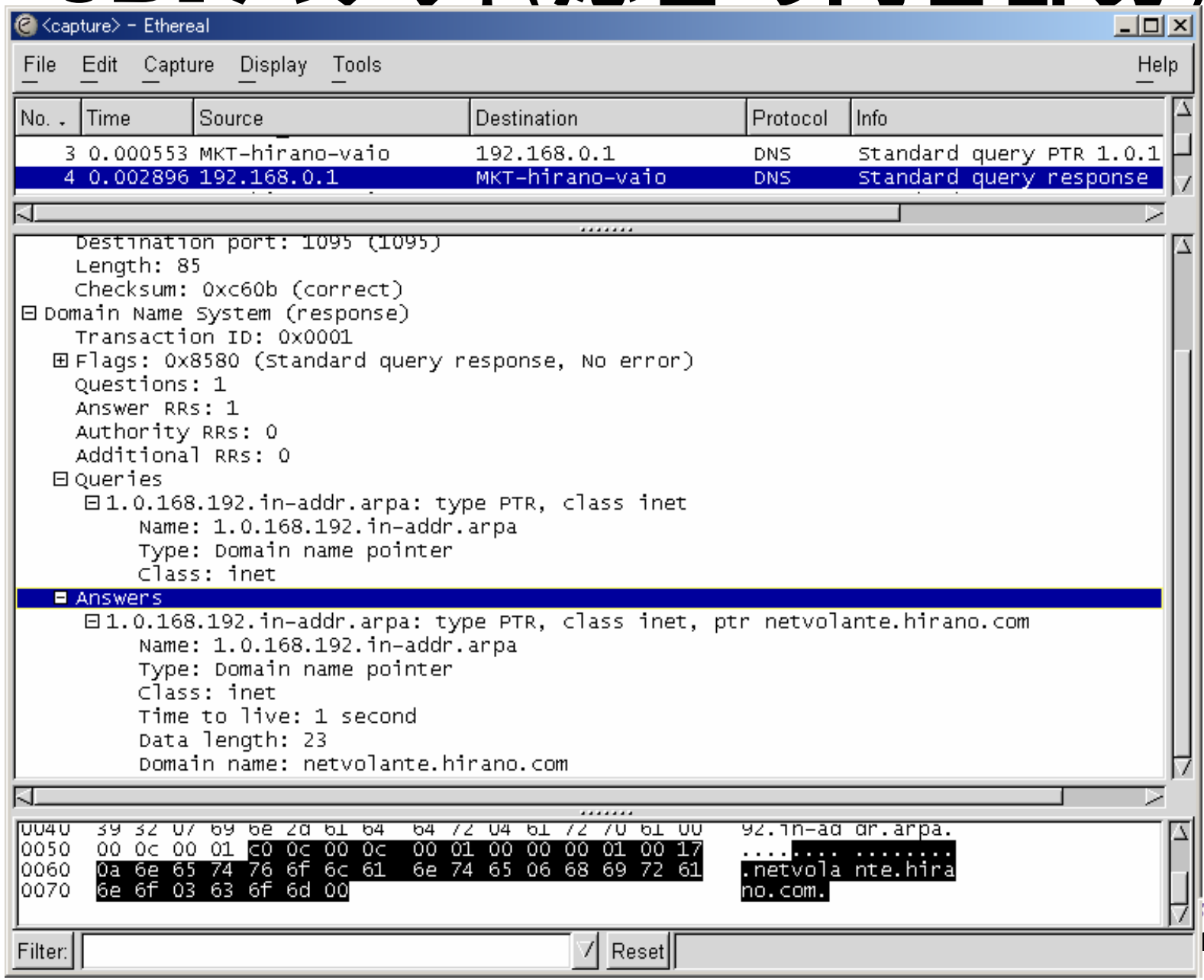
UDPパケット(問い合わせ)



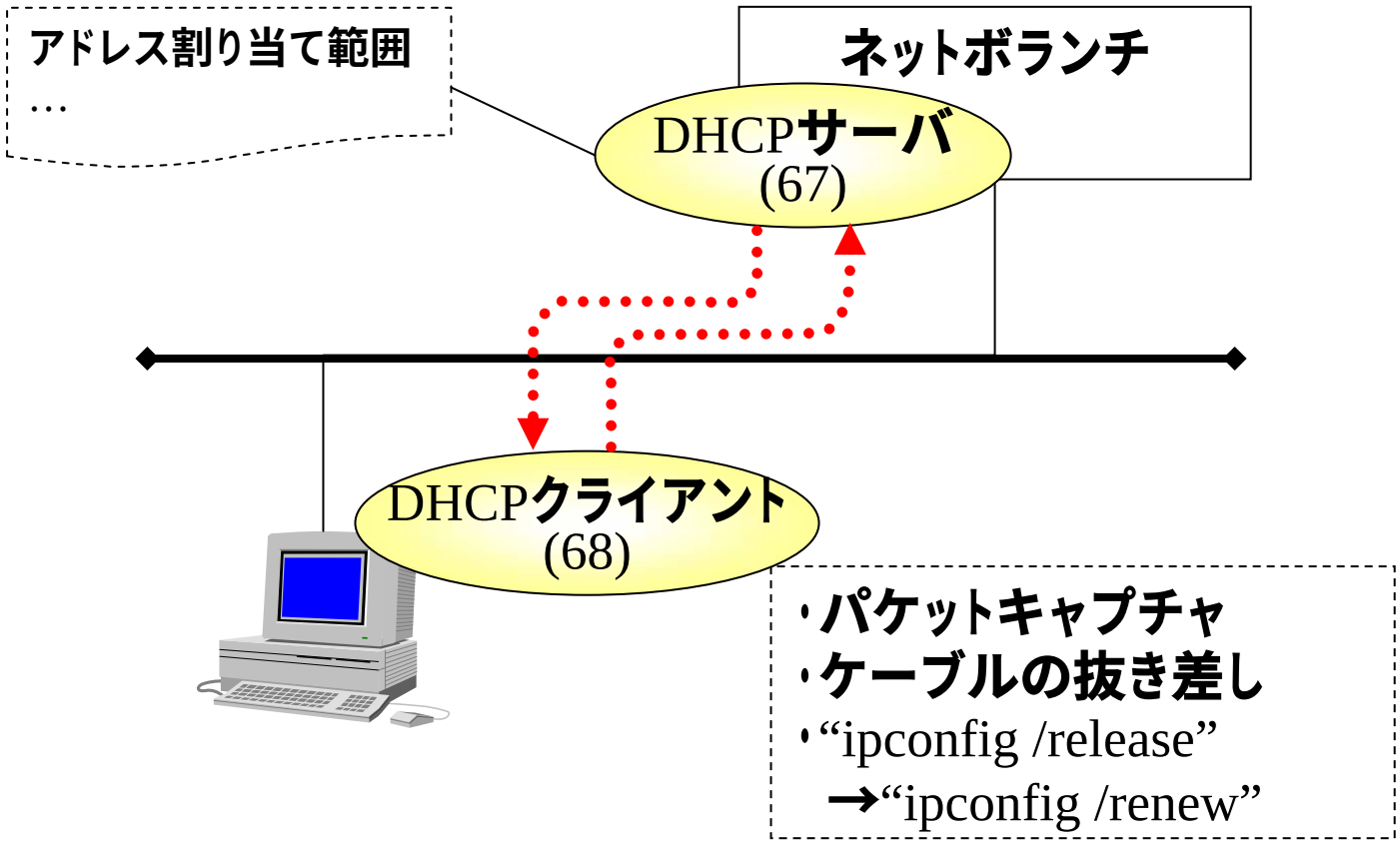
UDPパケット(応答)


<capture> - Ethereal
File Edit Capture Display Tools Help
No. Time Source Destination Protocol Info
3 0.000553 MKT-hirano-vaio 192.168.0.1 DNS Standard query PTR 1.0.1
4 0.002896 192.168.0.1 MKT-hirano-vaio DNS Standard query response
Frame 4 (119 on wire, 119 captured)
Ethernet II
Internet Protocol, Src Addr: 192.168.0.1 (192.168.0.1), Dst Addr: MKT-hirano-vaio (192.16
User Datagram Protocol, Src Port: domain (53), Dst Port: 1095 (1095)
Source port: domain (53)
Destination port: 1095 (1095)
Length: 85
Checksum: 0xc60b (correct)
Domain Name System (response)
Transaction ID: 0x0001
Flags: 0x8580 (Standard query response, No error)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
Answers
0000 08 00 46 0d 3e 96 00 a0 de 08 2f 38 08 00 45 00 ..F.>... ../8..E.
0010 00 69 4c ae 00 00 40 11 ac 81 c0 a8 00 01 c0 a8 .iL...@. ....
0020 00 03 00 35 04 47 00 55 c6 0b 00 01 85 80 00 01 ...5.G.U ....
0030 00 01 00 00 00 00 01 31 01 30 03 31 36 38 03 31 ....1 .0.168.1
0040 39 32 07 69 6e 2d 61 64 64 72 04 61 72 70 61 00 92.in-ad dr.arpa.
Filter:
Reset
User Datagram Protocol (udp)

UDPパケット(応答の内容部分)

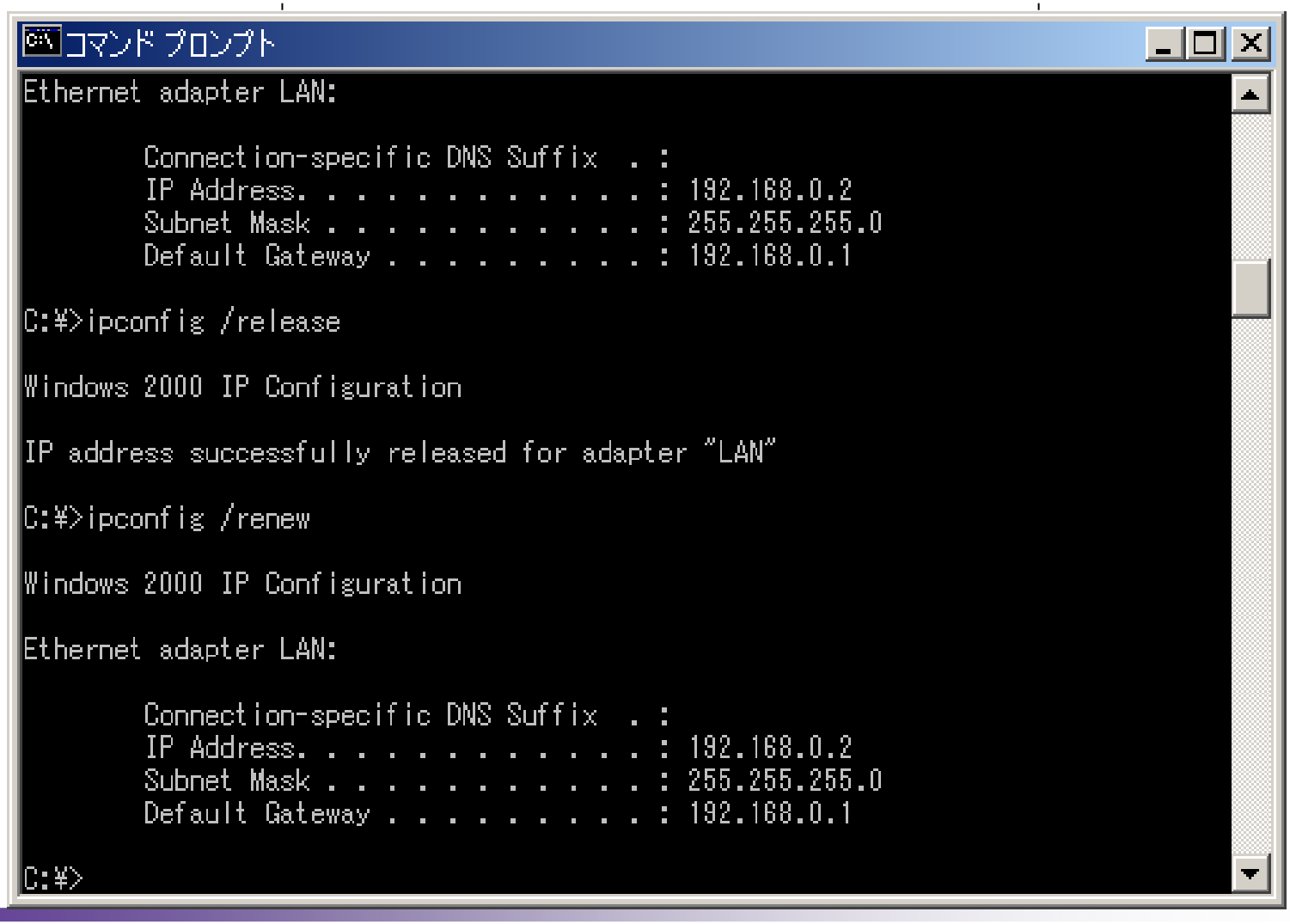


DHCPパケットの観測環境

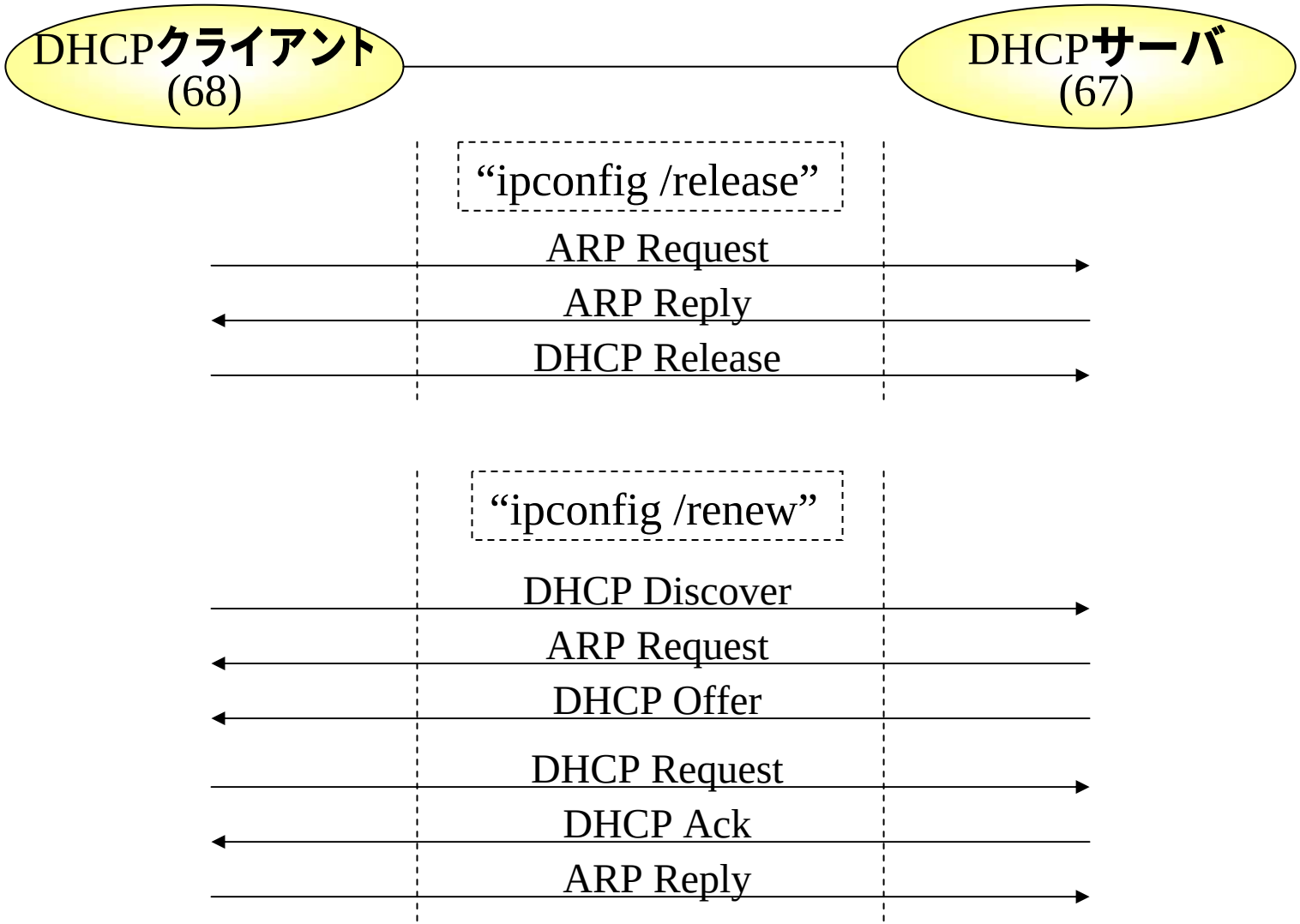


DHCPによるアドレスの開放と割り当て

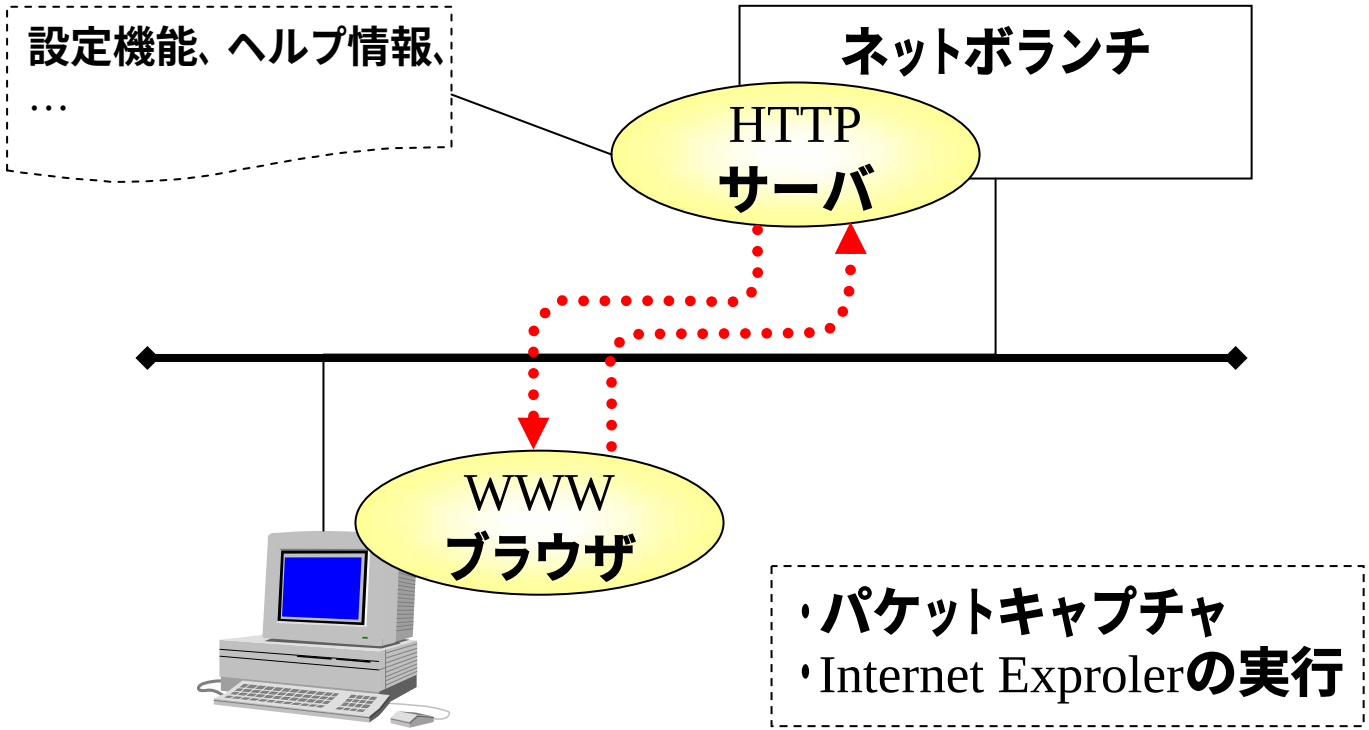
“ipconfig /release”→“ipconfig /renew”



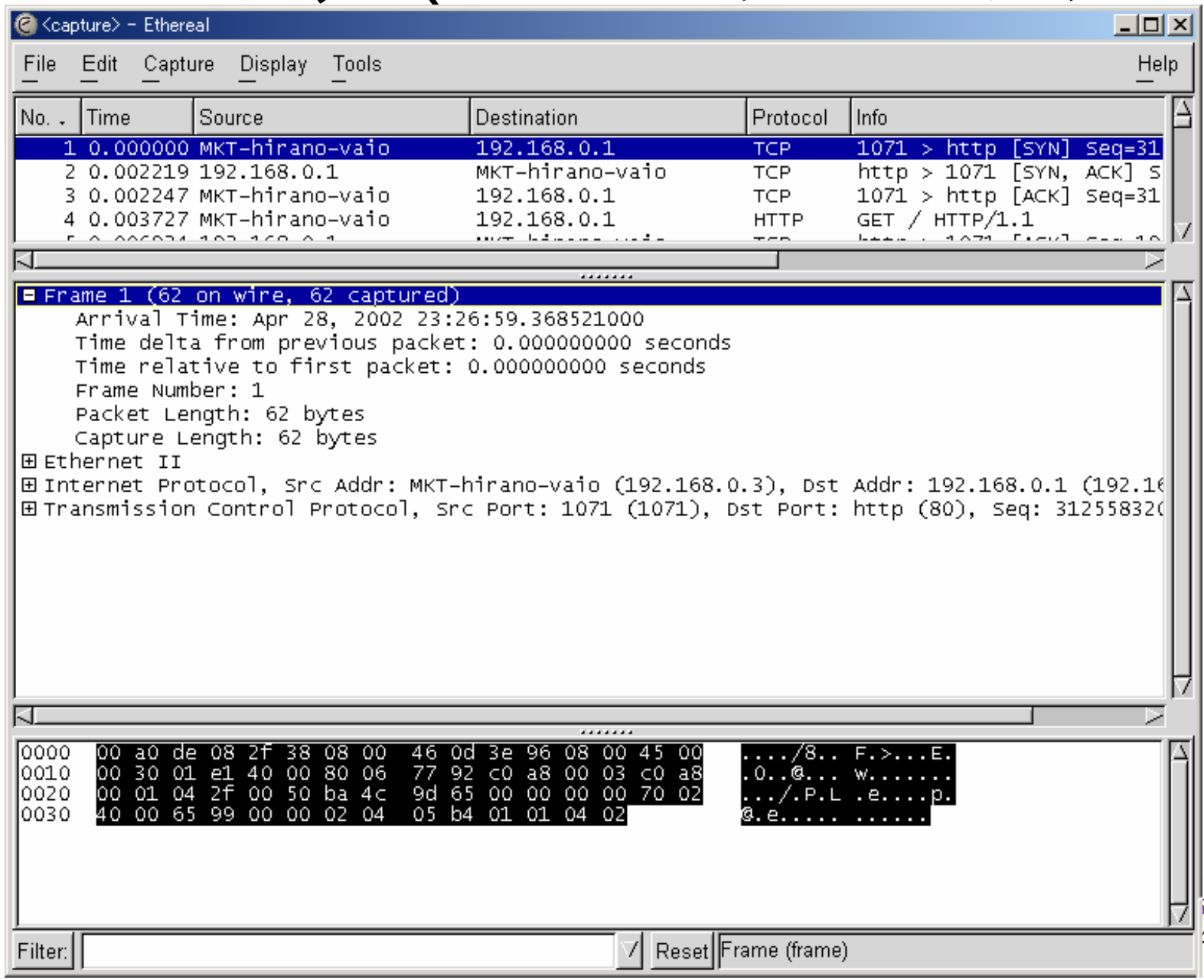
DHCPパケットの開放と割り当て



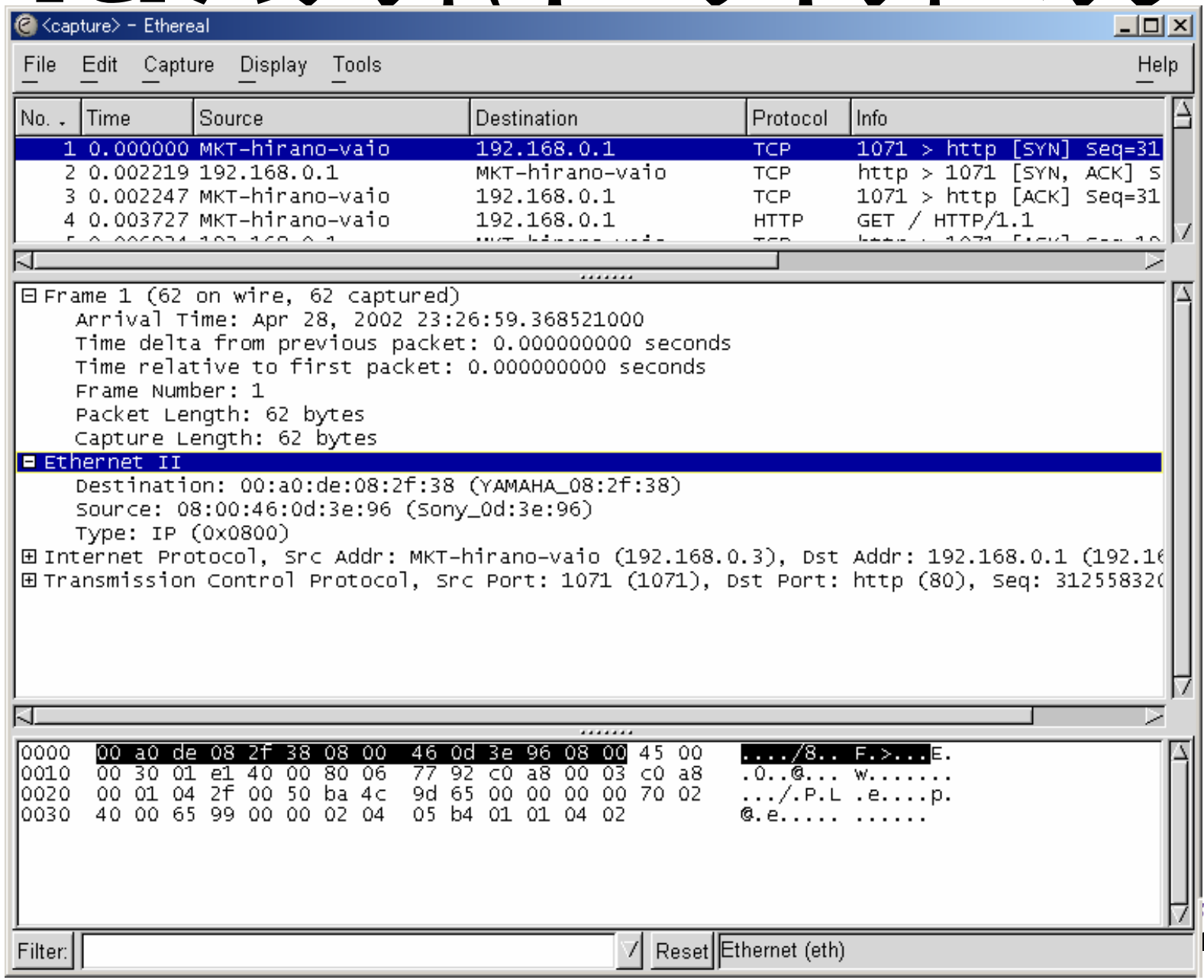
TCPパケットの観測環境



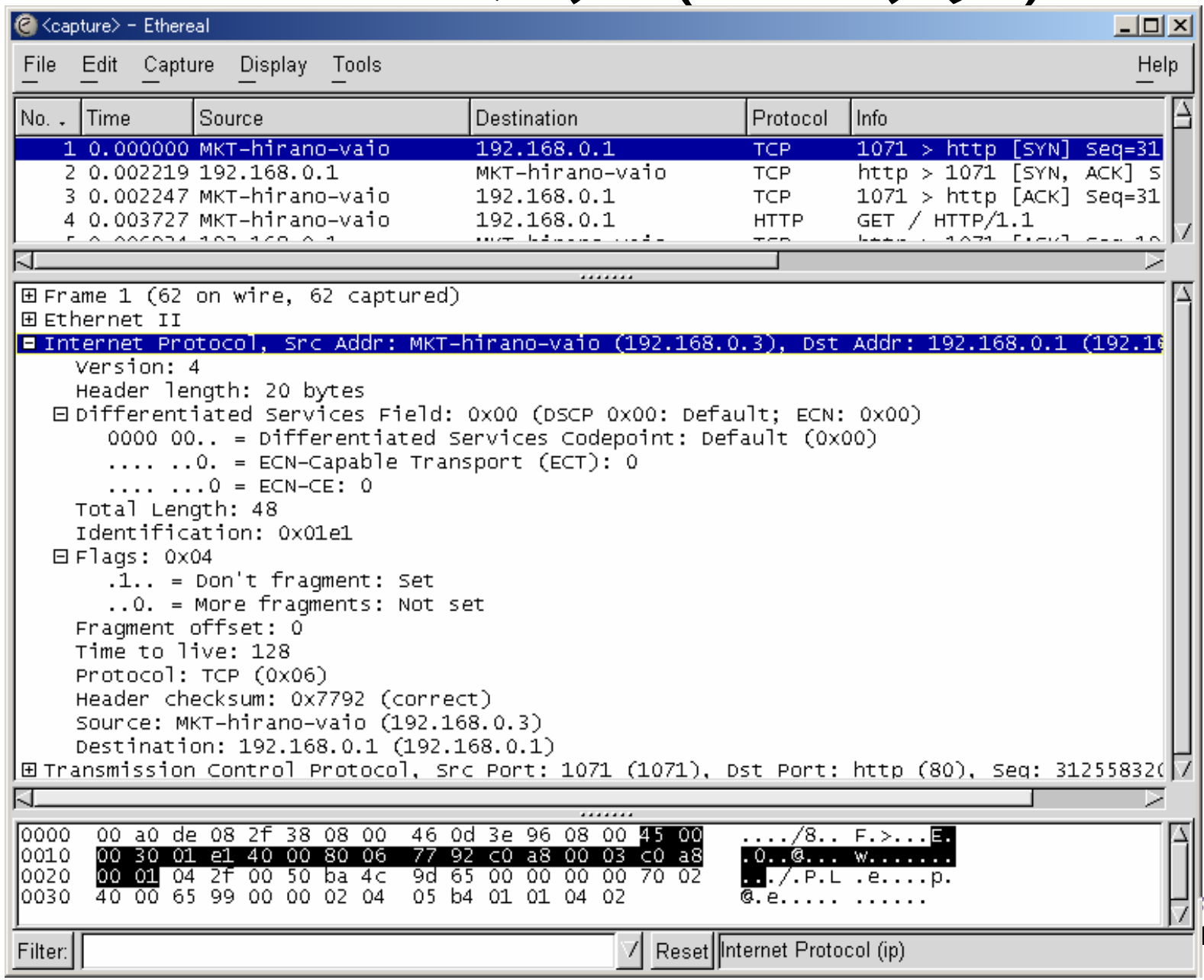
TCPパケット(WWWサーバアクセス)



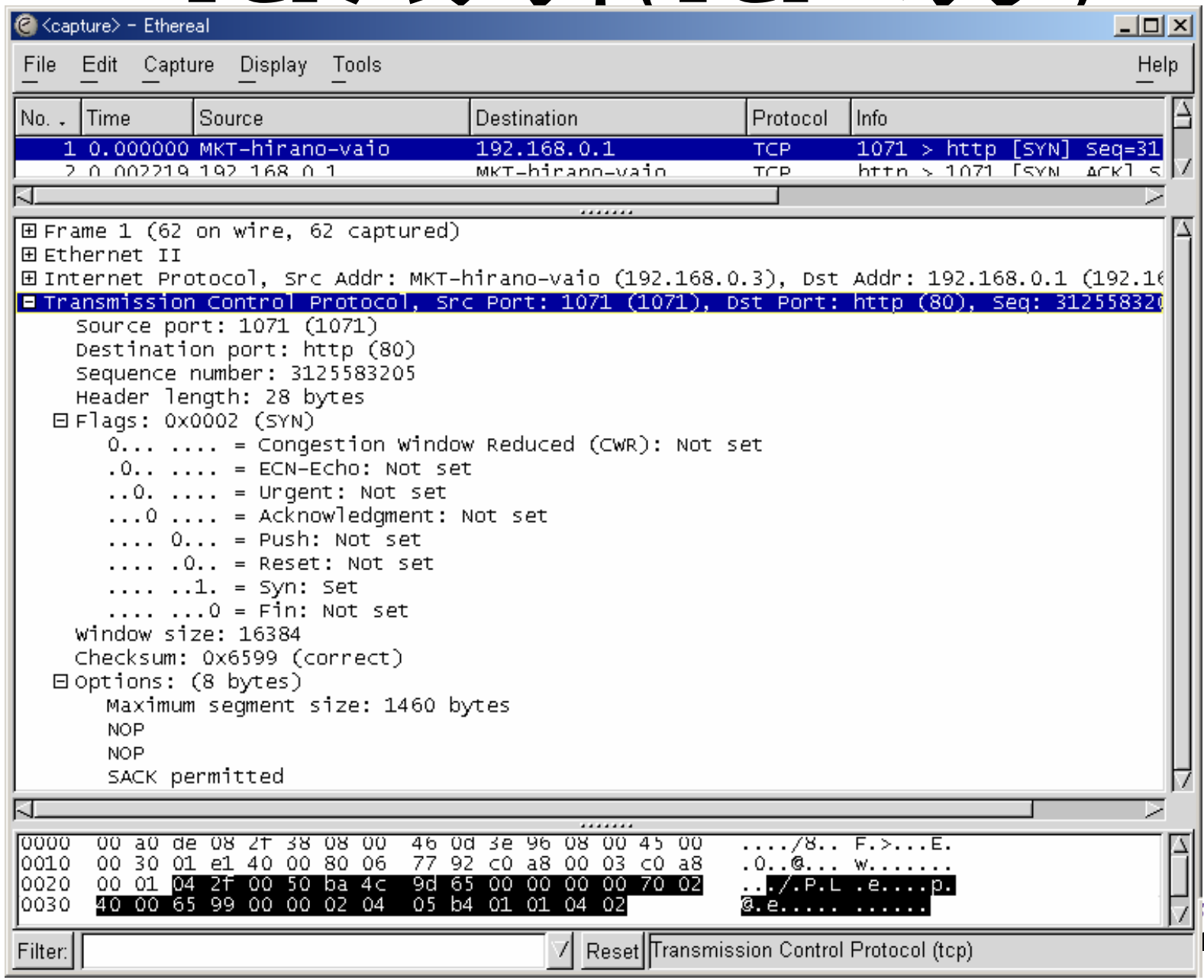
TCPパケット(イーサネットヘッダ)



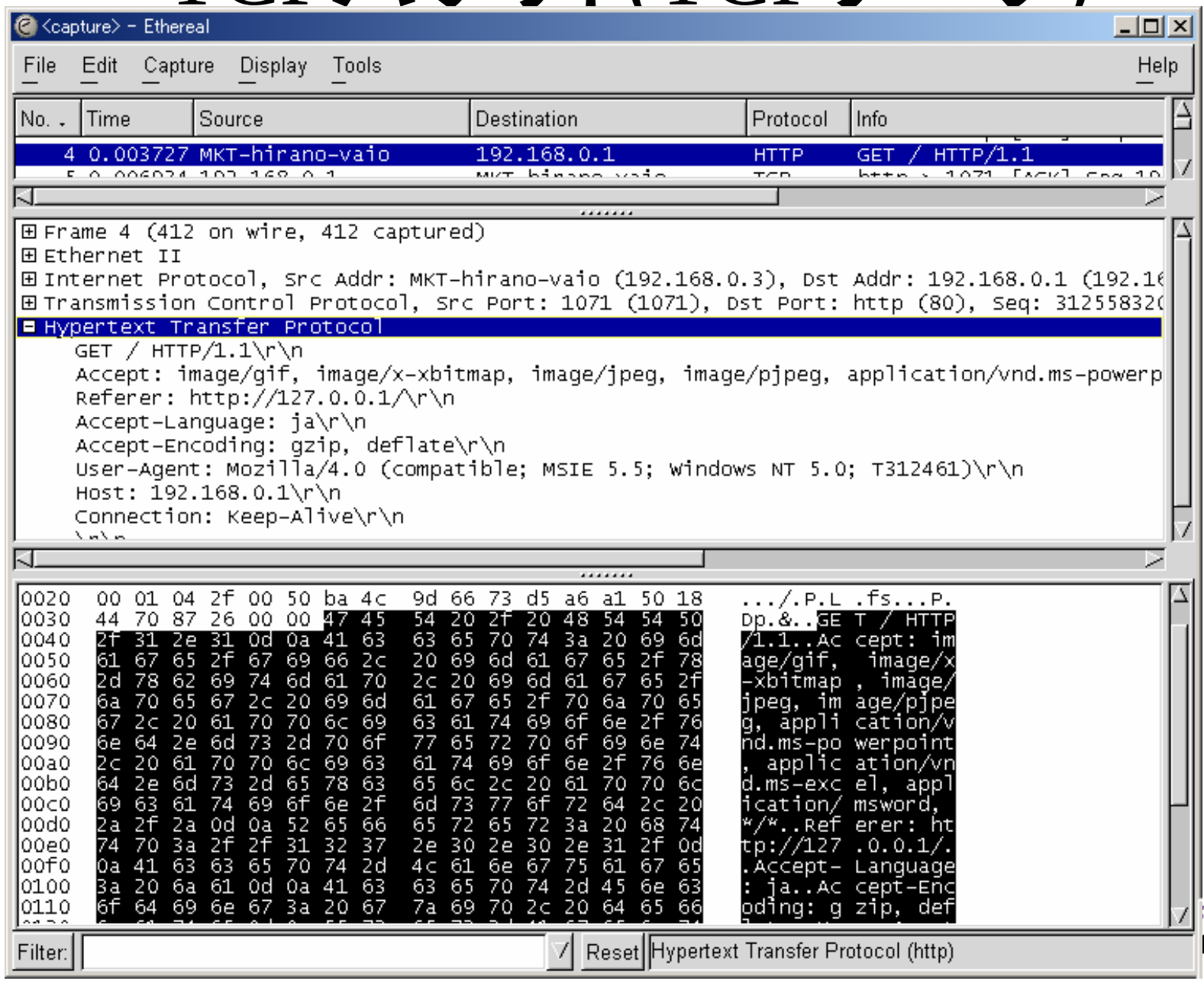
TCPパケット(IPヘッダ)



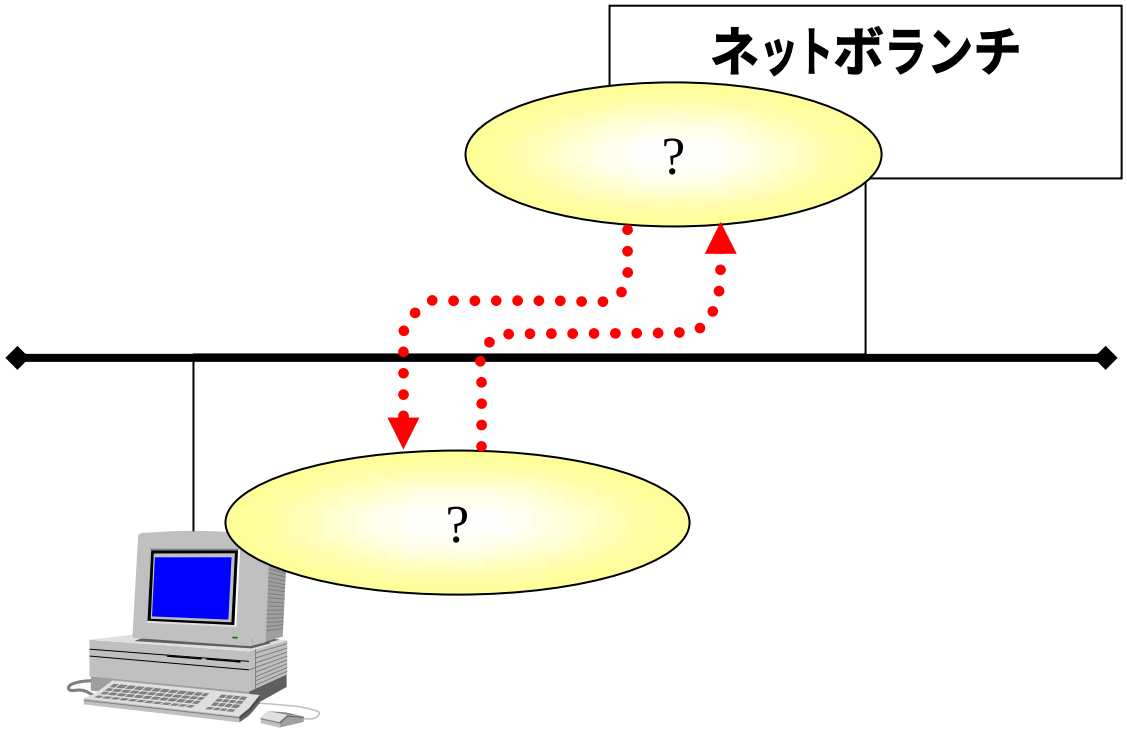
TCPパケット(TCPヘッダ)



TCPパケット(TCPデータ)



ルーターで観測できるプロトコル例



[TCP]
・telnet

[UDP]
・tftp
・RIP (**起動時など**)

[**マルチキャスト**]
・RIP2 (**起動時など**)