YAMAHA

感 動 を ・ と も に ・ 創 る

ヤマハ RTシリーズ
の
ブロードバンド&VPN戦略

2001年12月

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

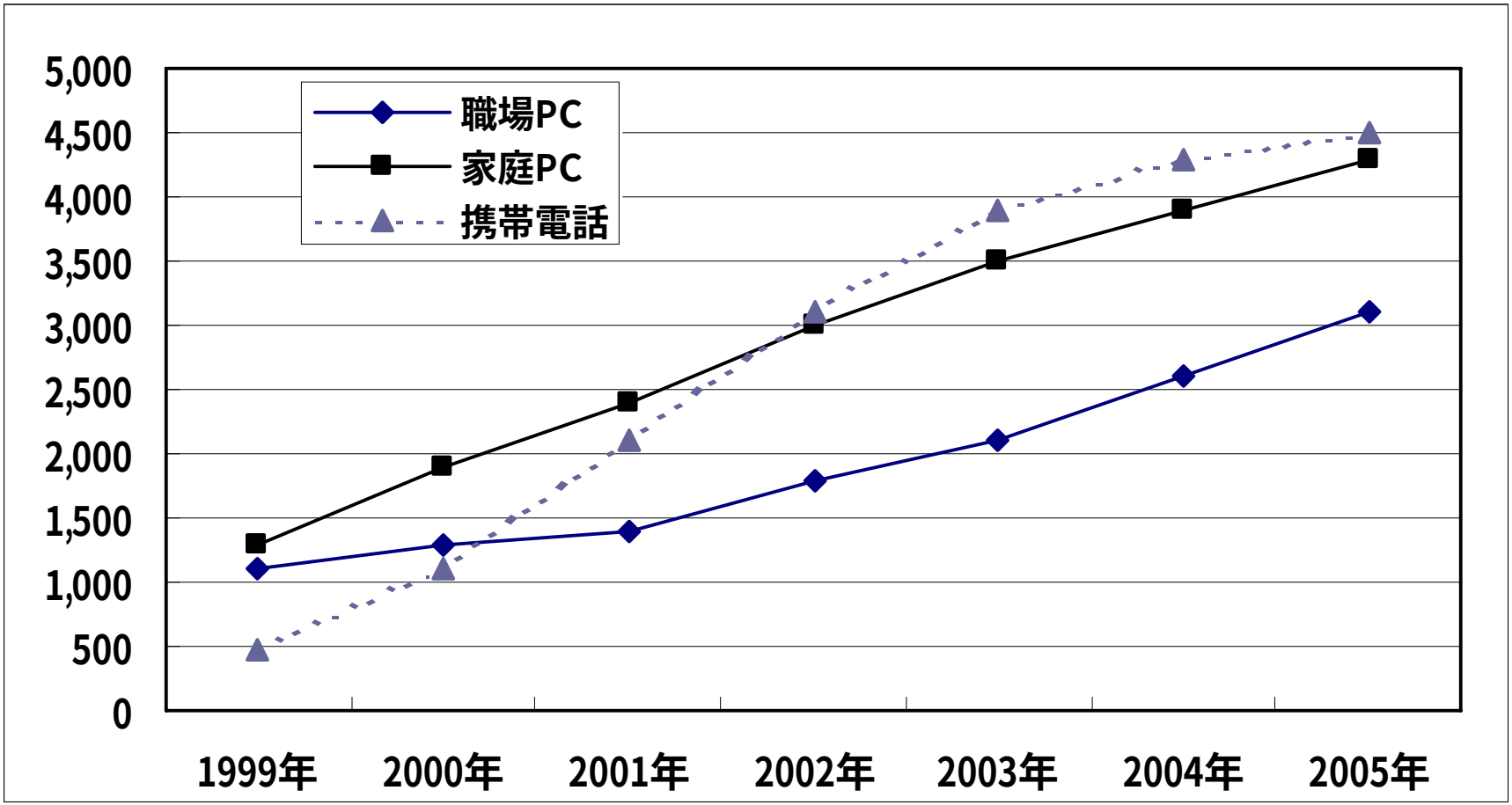
1) 市場動向と要望
2) ヤマハルータについて
3) ブロードバンドとVPNへの取り組み
4) 新製品紹介

[付録資料]
・特徴
・機能解説
　ヤマハルータの構造、NATディスクリプタ機能、
　ファイアウォール機能、
　フィルタ型ルーティングとマルチホーミング
・ネットボランチの使い方
・RTシリーズの使い方

インターネット動向

インターネット人口

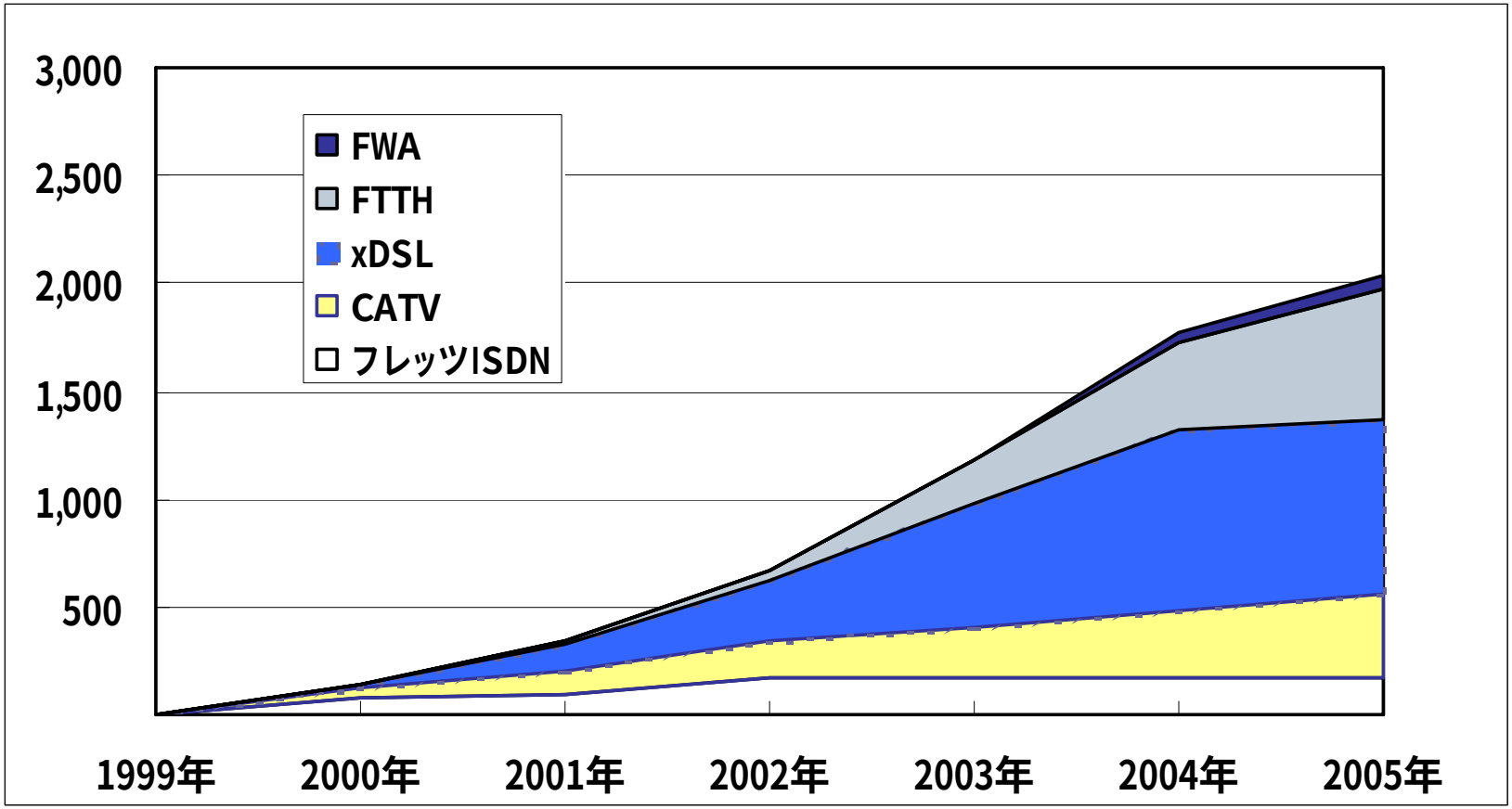
インターネット利用者数は今後も増加基調
PCと携帯電話によるインターネットとは使い分け
日本の総世帯数47百万世帯、新聞（一般紙）の発行総数47百万に迫る見込み



（野村総合研究所資料）

常時接続ネットワーク推移見込

ISDN1000万回線突破（00/12月）
フレッツISDNは2002年170万世帯見込む。ADSL40万人、CATV97万人
2001年度ADSLの普及は150万世帯（DSLAMの供給の制約）



（当社推定値）

個人/SOHOネットワーク動向

個人/SOHO向けインターネット動向

[日常の変化]

・モデム/TA　→ブロードバンド・ルータ
・ダイヤルアップ　→常時接続 & 大容量
・従量課金　→定額制 (使い放題)

「家庭/SOHOにおけるネットワークの日常化」

電気、ガス、水道、電話、と、ネットワーク

個人/SOHO向けルータの需要

[ネットワーク知識の浅いユーザの増加]

- 初期状態での高いセキュリティ性
- ハードウェアの信頼性/耐久性/環境対応性
- ソフトウェアの安定性
- 豊富なドキュメントと手厚いサポート

「使い易さの向上」

マニュアル/WWW設定機能の強化

企業ネットワーク動向

企業内ネットワークの動向

[アクセスラインの多様化/低価格化]

ISDN回線、高速ディジタル専用線、FR網

＋

ブロードバンド回線

(ADSL、CATV、FTTH、など)

↓

Internet VPN(IPsec)、IP-VPN、

フレッツ・シリーズ＋フレッツ・オフィス

企業向けアクセスルータの需要

[要望の多様化]

- ブロードバンド回線(ADSL,CATV,FTTH…)
- 1.5Mbps高速ディジタル専用線
- Internet VPN、IP-VPN
- IPv6、セキュリティ、NAT

「システム提案力の向上」

高速回線対応の低価格製品のラインナップを強化

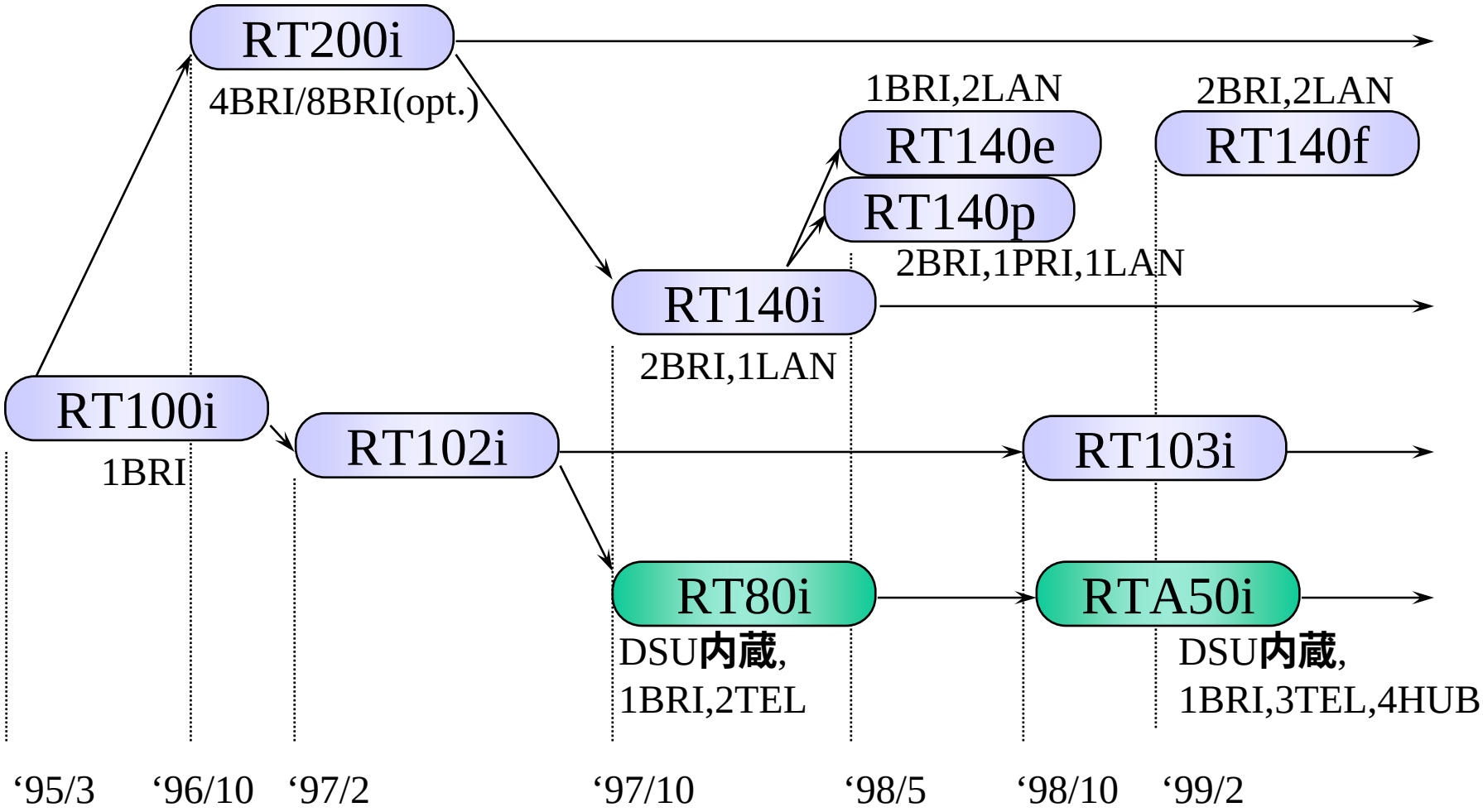
ヤマハルータについて

ヤマハルータの特徴

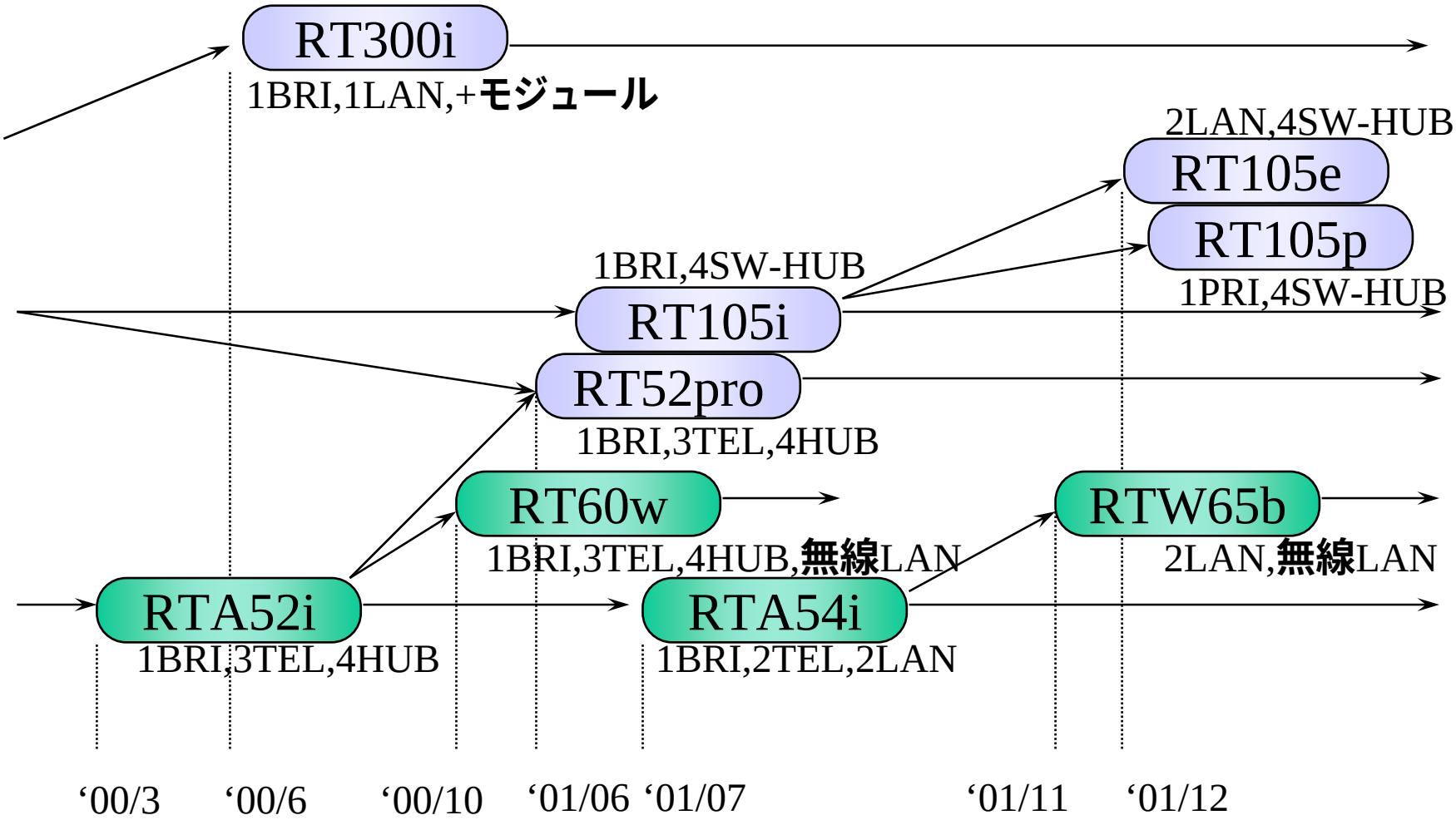
- 高信頼性
  高信頼性部品の採用、部品点数の削減、自社工場で生産
- 自社製LSI (外販用を含む) の多用
  →低レイヤ層から把握
- ファームウェア(ドライバソフトなど)の自社開発
  →迅速対応、ユーザサポートの充実
- 使いやすい設定機能と豊富な設定例

Made in Japan.

ヤマハルータの歩み#1


RT200i
4BRI/8BRI(opt.)
1BRI,2LAN
RT140e
2BRI,2LAN
RT140f
RT140p
2BRI,1PRI,1LAN
RT140i
2BRI,1LAN
RT100i
1BRI
RT102i
RT103i
RT80i
DSU内蔵,
1BRI,2TEL
RTA50i
DSU内蔵,
1BRI,3TEL,4HUB
‘95/3
‘96/10
‘97/2
‘97/10
‘98/5
‘98/10
‘99/2

ヤマハルータの歩み#2


RT300i
1BRI,1LAN,+モジュール
2LAN,4SW-HUB
RT105e
RT105p
1PRI,4SW-HUB
1BRI,4SW-HUB
RT105i
RT52pro
1BRI,3TEL,4HUB
RT60w
1BRI,3TEL,4HUB,無線LAN
RTW65b
2LAN,無線LAN
RTA52i
1BRI,3TEL,4HUB
RTA54i
1BRI,2TEL,2LAN
‘00/3
‘00/6
‘00/10
‘01/06
‘01/07
‘01/11
‘01/12

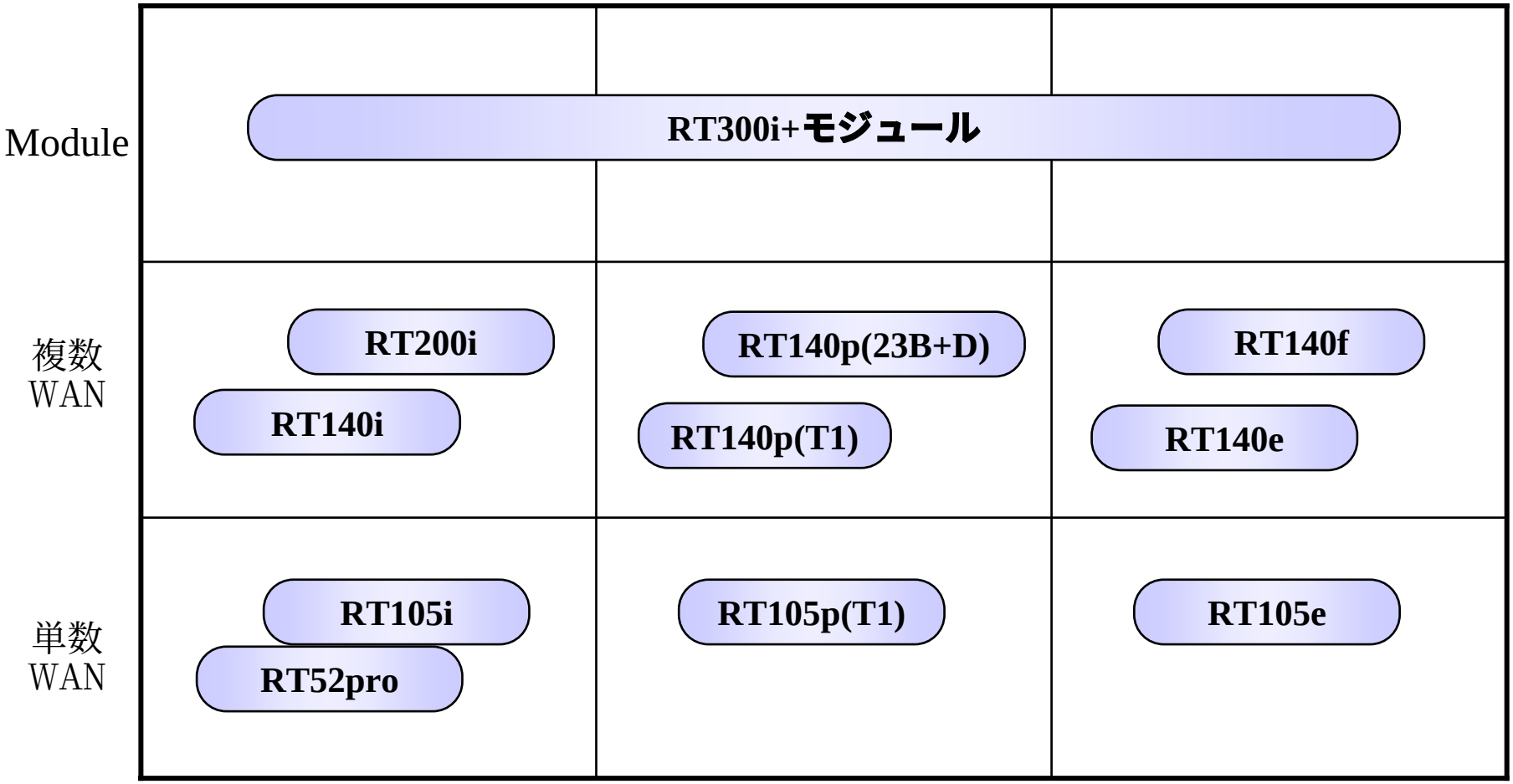
ネットボランチの位置付け

[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)

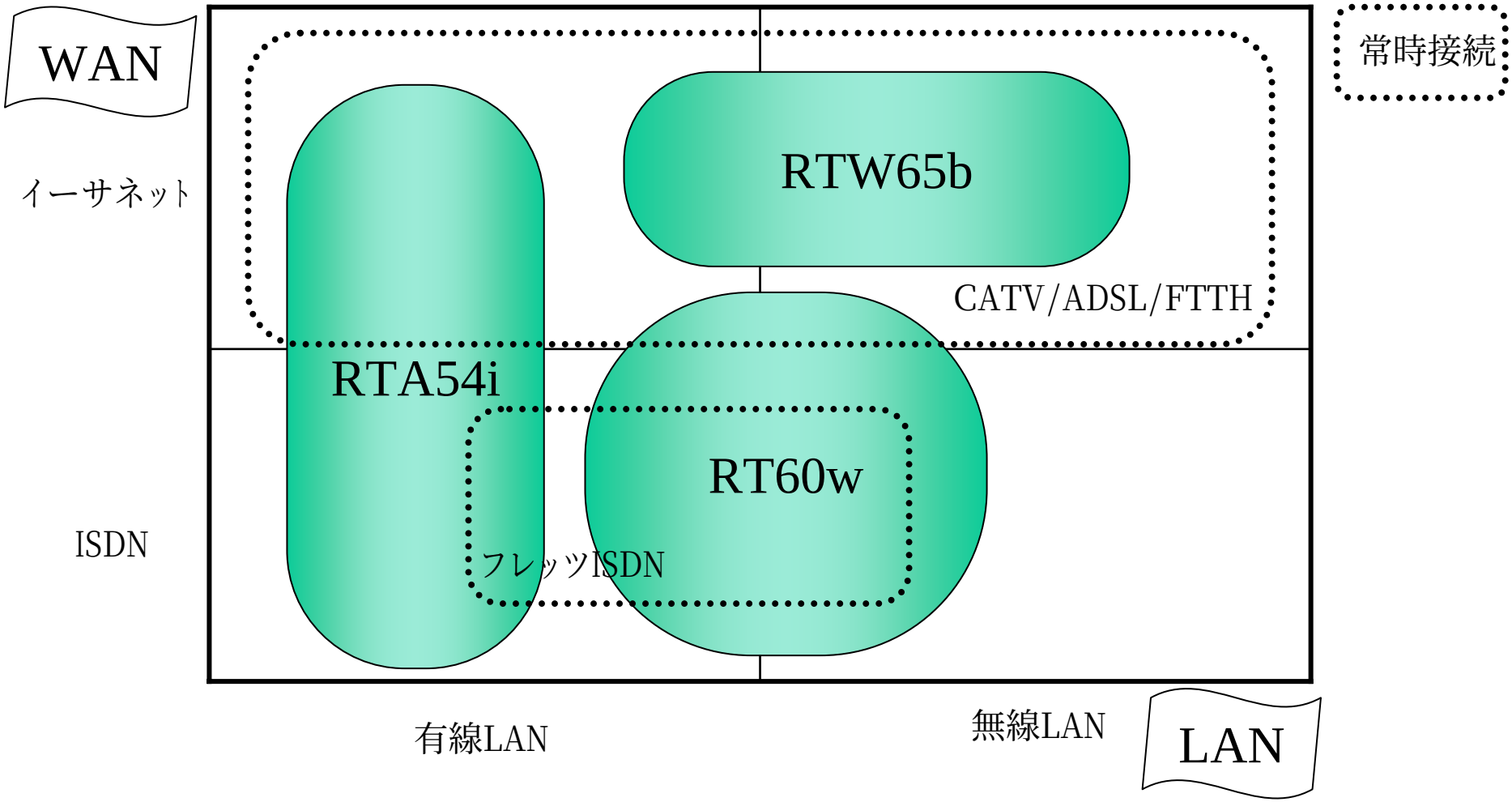
[RT100iの2つの顔]
a) プロバイダ接続用ルータ
b) 拠点側ルータ

主な区分	ネットボランチ	RT105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シリーズの製品構成



ネットボランチの製品構成



ブロードバンドとVPN
への取り組み

ヤマハルータのブロードバンド戦略

「ブロードバンドによる変化」

- 常時接続 & 大容量
- ルータのセキュリティ・ゲートウェイ化

「ヤマハルータらしい付加価値の提供」

- ユーザ・フレンドリー
- セキュリティ・ポリシー
- IPv6による peer to peer な環境

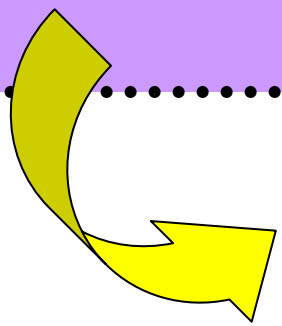
※柔軟性と多機能→トータルバランス

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.xx	・RT105e発売 ・DHCPクライアント機能

ブロードバンドの要素

[必須]
- 2 ethernet
- NAT/IPマスカレード
- PPPoEクライアント機能
- DHCPクライアント機能
- DHCPサーバ機能
- …



[ヤマハルータ]
- ファイアウォール機能
- IPv6
- ISDNによるバックアップ
- フィルタ型ルーティング
- マルチホーミング

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 →動的フィルタと不正アクセス検知
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

IPsec Version 2 RFC:RFC2401～RFC2409、RFC2451

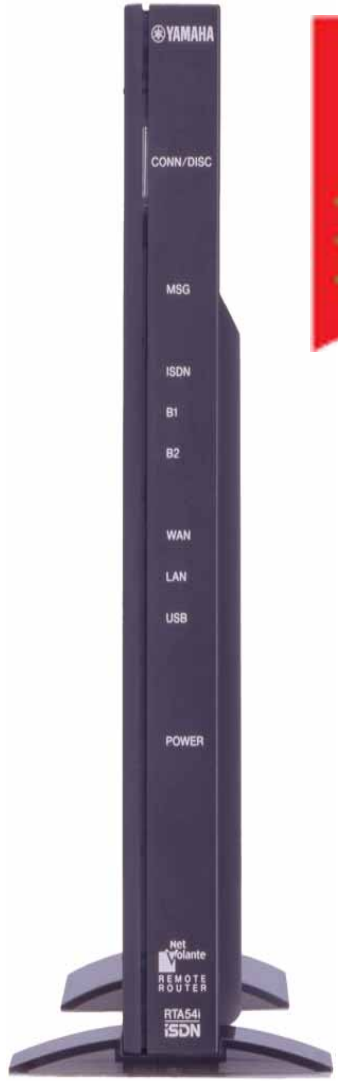
Internet VPNの要素

[必須]
- IPsec Version 2 RFC対応
- 相互接続性
- …

[ヤマハルータ]
- ファイアウォール機能
- NATディスクリプタ
- IPv6
- ダイヤルアップVPN
- VPNパススルー
- 圧縮
- ISDNによるVPNバックアップ

RTA54i
製品概要

(オープンプライス)



RTA54iに求められるもの

- ***3つのインタフェースを使いこなす。(無駄にしない)***
  1) ISDNポート、WANポート、LANポートを統一的に管理。
  2) CATVやADSLを利用する環境でも、ISDN回線を活用できる機能を提供する。
  3) ISDN回線のみで利用している環境で、WANポートも生かせる機能を提供する。
- ***初心者がWWW設定画面の迷子にならないこと***
  1) 設定状況で、変化する画面を無くす。減らす。
  2) 階層構造と表示画面の位置関係が常に確認できること。
- ***ブロードバンド対応だけど、ISDNダイヤルアップルータ***
  1) RTA52iと同等の機能が利用できること。(RTA52iの後継機種)
  2) ブロードバンドを利用している場合でも、RTA52iを使っているのと
     同様の機能が利用できること。
- ***ファイアウォール機能によるセキュリティを簡単に利用可能***
  1) ビギナーが安心できるセキュリティ機能 (セキュリティレベル)
  2) エキスパートが遊べるセキュリティ機能 (設定、編集機能)
- ***平易な文章、トラブルシューティングしやすい情報提供、…***

RTA54iのコンセプト

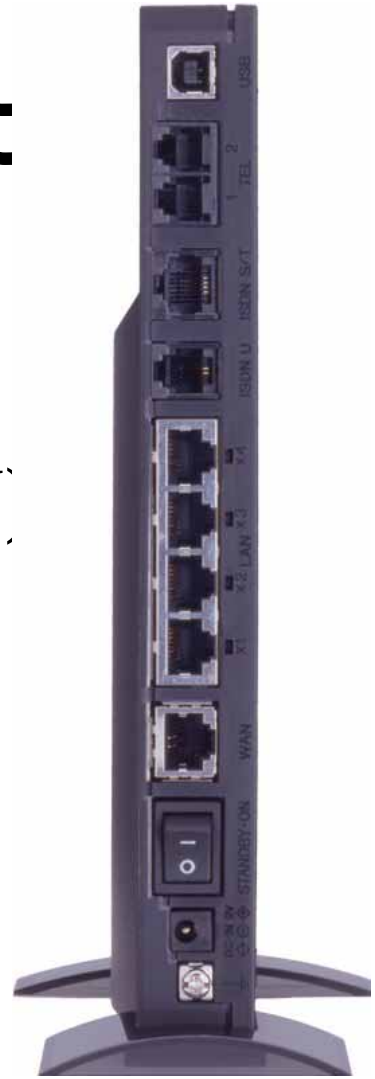
「ISDN/CATV/ADSLなどの常時接続環境を
誰でも 安全に 確実に 簡単に 利用できる製品」

- 安全性(初期設定、ファイアウォール、VCCIなど)
- 信頼性/耐久性(部品点数の削減、雷対策など)
- 安定性(ファームウェアの継承)
- 使い易さ(WWW設定機能、ユーティリティ)
- RTA50i/RTA52iのイメージを継承しながら、
モノリスをモチーフにしたミニマルなデザイン

※ミニマルなデザイン＝要素を徹底的に研ぎ澄ませた無駄のない洗練されたデザイン

RTA54iの特徴

- 本格的なファイアウォール機能を手軽に
- LAN/WAN/ISDN:3つのインタフェース
- USBポート
  (ISDN-TA,ブロードバンドTA,擬似LAN
- RTシリーズと共通のコンソールコマンド
- かんたん設定(WWW設定機能)
  多機能/多用途を簡単に利用可能



RTW65b
製品概要

RTW65b

(オープンプライス)

RTW65bに求められるもの

- ***ネットボランチらしくないブロードバンド・ルータ***
  1) ヤマハルータ初のISDNを搭載しないモデル
  2) ユーザや設置場所を選ばない親和性の高いデザイン
- ***ネットボランチらしいブロードバンド・ルータ***
  1) 初期設定の高いセキュリティ性
  2) 親切で使い易いマニュアルとWWW設定機能
- ***無線LANインタフェースを使いこなす。***
  1) 無線LANの使い易さの提供
  2) セキュリティ機能の提供(128 bit WEP)
  3) 相互接続性 (WiFi取得, RT60wとの無線ブリッジ機能)
- ***ファイアウォール機能によるセキュリティを簡単に利用可能***
  1) ビギナーが安心できるセキュリティ機能 (セキュリティレベル)
  2) エキスパートが遊べるセキュリティ機能 (設定、編集機能)
- ***平易な文章、トラブルシューティングしやすい情報提供、…***

RTW65bのコンセプト

「ブロードバンド対応機能と無線LANの利便性を
誰でも 安全に 確実に 簡単に 利用できる製品」
→より多くのユーザに親しまれる新ネットボランチ

- 安全性(初期設定、ファイアウォール、VCCIなど)
- 信頼性/耐久性(部品点数の削減、外部アンテナなど)
- 安定性(ファームウェアの継承)
- 使い易さ(WWW設定機能、無線LAN)
- あらゆる環境に適応力のあるミニマルなデザイン

※ミニマルなデザイン＝要素を徹底的に研ぎ澄ませた無駄のない洗練されたデザイン

RTW65bの特徴

- LAN/WAN(10BASE-T/100BASE-TX 各1ポート)
- 本格的なファイアウォール機能を手軽に
- かんたん設定
  多機能を簡単に利用可能、RTA54iの機能を継承
- 無線LANインタフェース
  IEEE 802.11b,ESS-ID,WEP(64bit/128bit),14チャネル
- USBポート(ブロードバンドTA,擬似LAN)
- RTシリーズと共通のコンソールコマンド

RT105e/RT105p
製品概要

RT105e

(希望小売価格 110,000**円)**

RT105p

(希望小売価格 180,000**円)**

RT105シリーズに求められるもの

- ***信頼性、安定動作、耐久性***
- ***センタールータ(RT300i)との相互接続性***
- ***企業向け最新ファームウェア(Rev.6系)機能***
  1) 各種機能
  2) 設定機能

- ***低価格なアクセスラインへの対応したラインナップ***
  1) CATV/ADSLなどのブロードバンド回線
  2) 高速ディジタル専用線(192kbps～1.5Mbps)

RT105シリーズの共通特徴

- **企業向けルータ用最新ファームウェアの継承**

  信頼性、ファイアウォール、IPsec、OSPF、IPv6、NAT

  ディスクリプタ、…

- **ハードウェアの信頼性**

  少ない部品点数、ネットボランチと共通部品など

- LAN**側インタフェース**

  10BASE-T/100BASE-TX**スイッチングハブ**(4**ポート**)

- **電源内蔵のコンパクト筐体**

  220(W)×141.5(D)×42.6(42.6)、**体積**:1.326**リットル**

RT105eの特徴

- 高速CPUの採用 (高スループット対応)
  RT105i比：1.66倍→スループット：16Mbps
- LAN側インタフェース
  10BASE-T/100BASE-TXスイッチングハブ(4ポート)
  セカンダリ・セグメント機能
  MDI/MDI-X自動判別機能
- WAN側インタフェース
  10BASE-T/100BASE-TX(1ポート)

RT105pの特徴

・LAN側インタフェース

10BASE-T/100BASE-TXスイッチングハブ(4ポート)

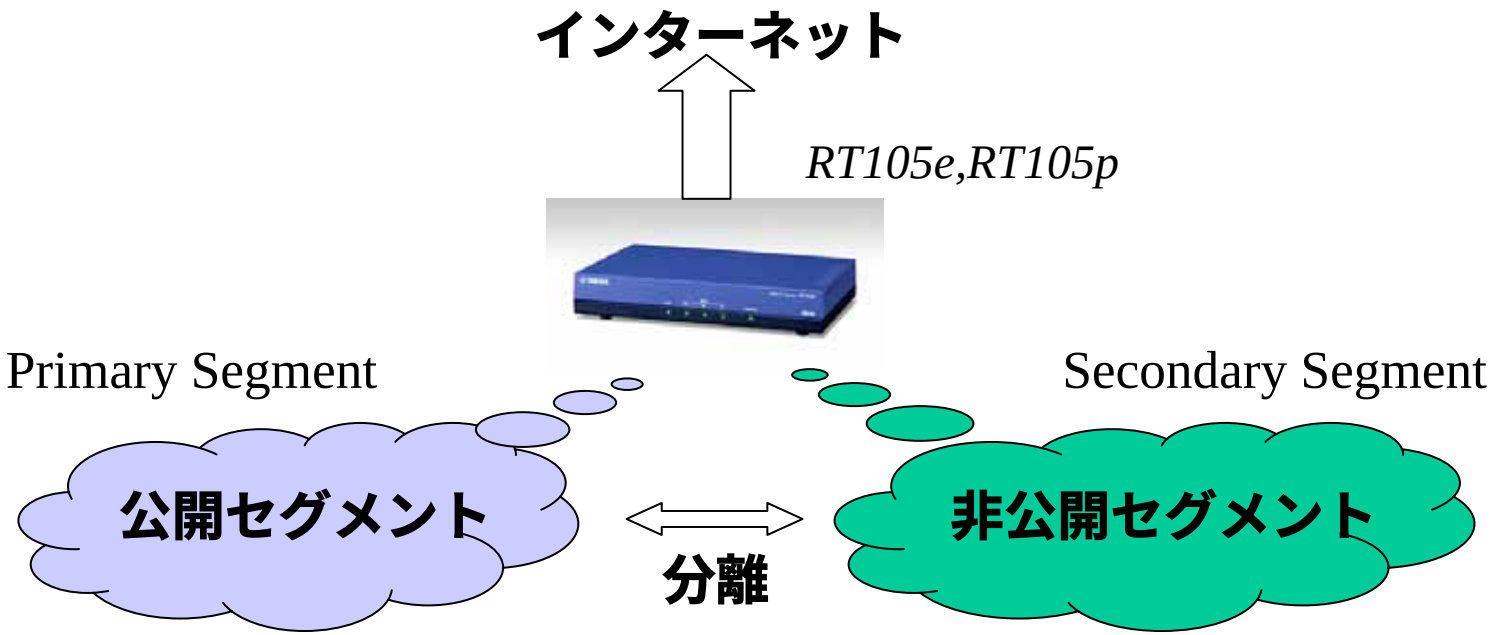
セカンダリ・セグメント機能

MDI/MDI-X自動判別機能

・WAN側インタフェース

高速ディジタル専用線(192Kbps～1.5Mbps)

セカンダリ･セグメント機能



LAN側のネットワークを2つに分割する機能

→公開用サーバを設置する際のセキュリティ向上

(RT105e/RT105pのみ)

MDI/MDI-X自動判別機能

・LANポートに接続された機器のMDIとMDI-Xを
自動判別する機能

MDI　：端末に接続するポート(=)
MDI-X：ハブに接続するポート(X,Uplink)

→配線ミスの軽減
NOR/REV切り替えスイッチやUplinkポートの削減

(RT105e/RT105pのみ)

付録資料

常時接続時代のセキュリティ

- 静的&動的パケットフィルタリング
  メモリの許す限り無制限
- 不正アクセス検知機能(IDS)
- サービス停止機能、ステルス機能
- 豊富な情報と設定例

[RTA54i/RTW65bのWWW設定機能...かんたん設定]

- 自動設定セキュリティ・フィルタ・ポリシー
  ネットボランチは「可能な限り積極的にLANを守る」
- セキュリティレベルによって高度なセキュリティを
  かんたんに利用可能
- ユーザフレンドリーなファイアウォール編集機能

IPv6 Ready

- 1998年より共同研究を開始
  - →研究者向けWS-ONE(β版)
  - →一般向けWS-ONE(β版)
  - →2001年6月より正式版の提供開始
- IPアドレスが128ビット(IPv4の4倍)
  - 深刻なIPアドレスの枯渇問題に対応し、無償搭載
- アドレス変換を挟まない peer to peer 通信の確保
  - →ネットワークアプリケーション
- ネットボランチの対応
  - RTA54i/RT60w/RTW65bは、同クラスで唯一
  - IPsecは、未実装

Kindness(誰でも安心)

利用者一義の製品開発

[ネットボランチシリーズ...RTA54i/RTW65b]

- 使い易いWWW設定機能&ヘルプ画面
- 初心者でも安心のマニュアル(丁寧で豊富な説明)
- PCを設定するユーティリティ(パソコンセットアップ)
- 接続/切断ユーティリティ(RTAssist)

[RTシリーズ]

- きめ細かい設定機能(困った時でも安心)
- 機能を連想しやすいコマンド書式
- ユーザフレンドリーなCLI編集機能
- ホームページとマニュアルでの豊富な設定例

高品質

利用者一義の製品開発

- 静電気対策、雷対策 (強化)
- 電波障害
- 信頼性/耐久性(部品点数の削減)
- 安定性(ファームウェアの継承)
- 故障率の改善

ヤマハルータの構造

柔軟性と多機能のために

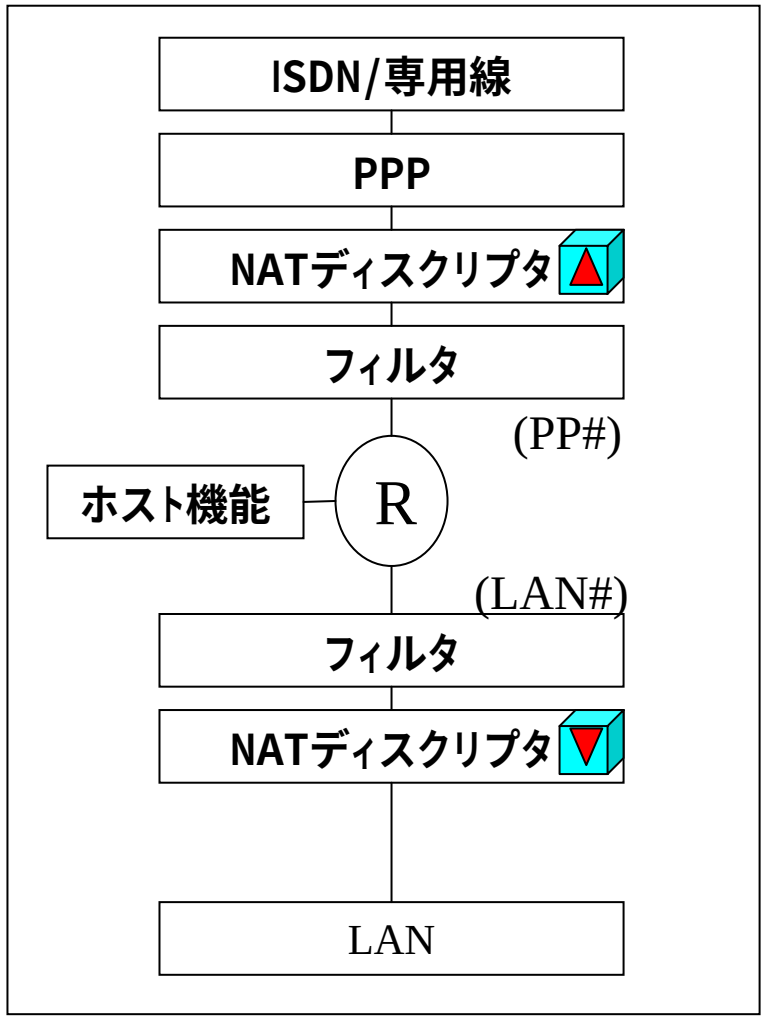
多機能で信頼性のある
モジュール構成

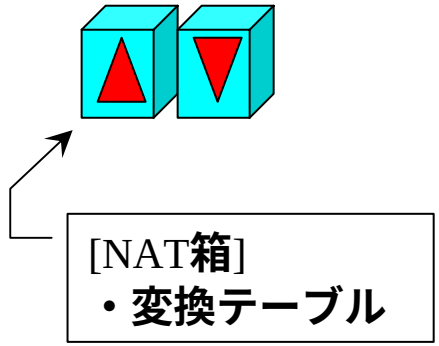
構造#1(PPP)

RT140i

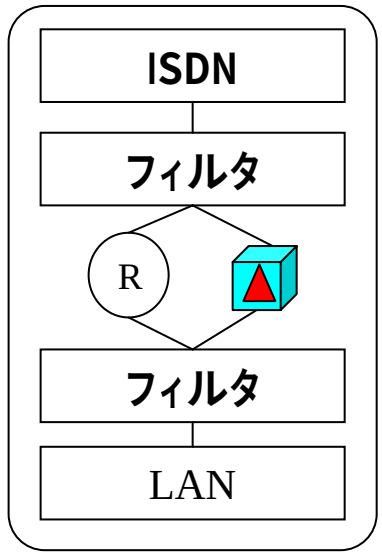
RT105i

RTA52i





比較構成例

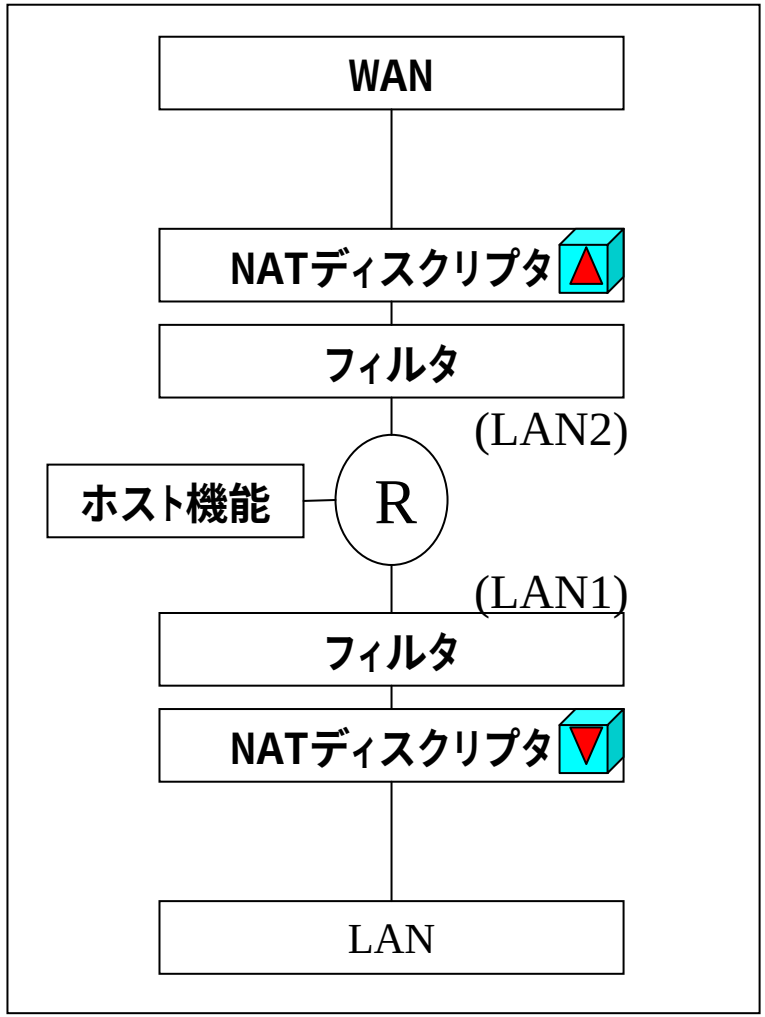


構造#2(ローカルルータ)

RT300i

RT140e

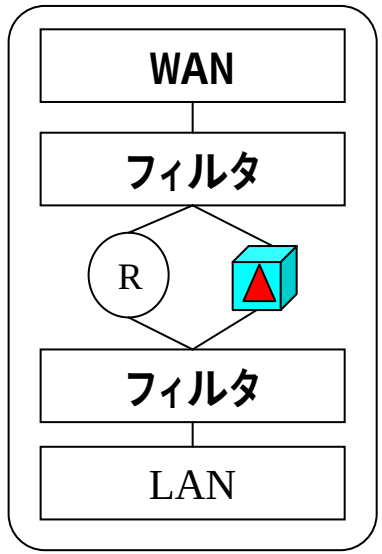
RT105e



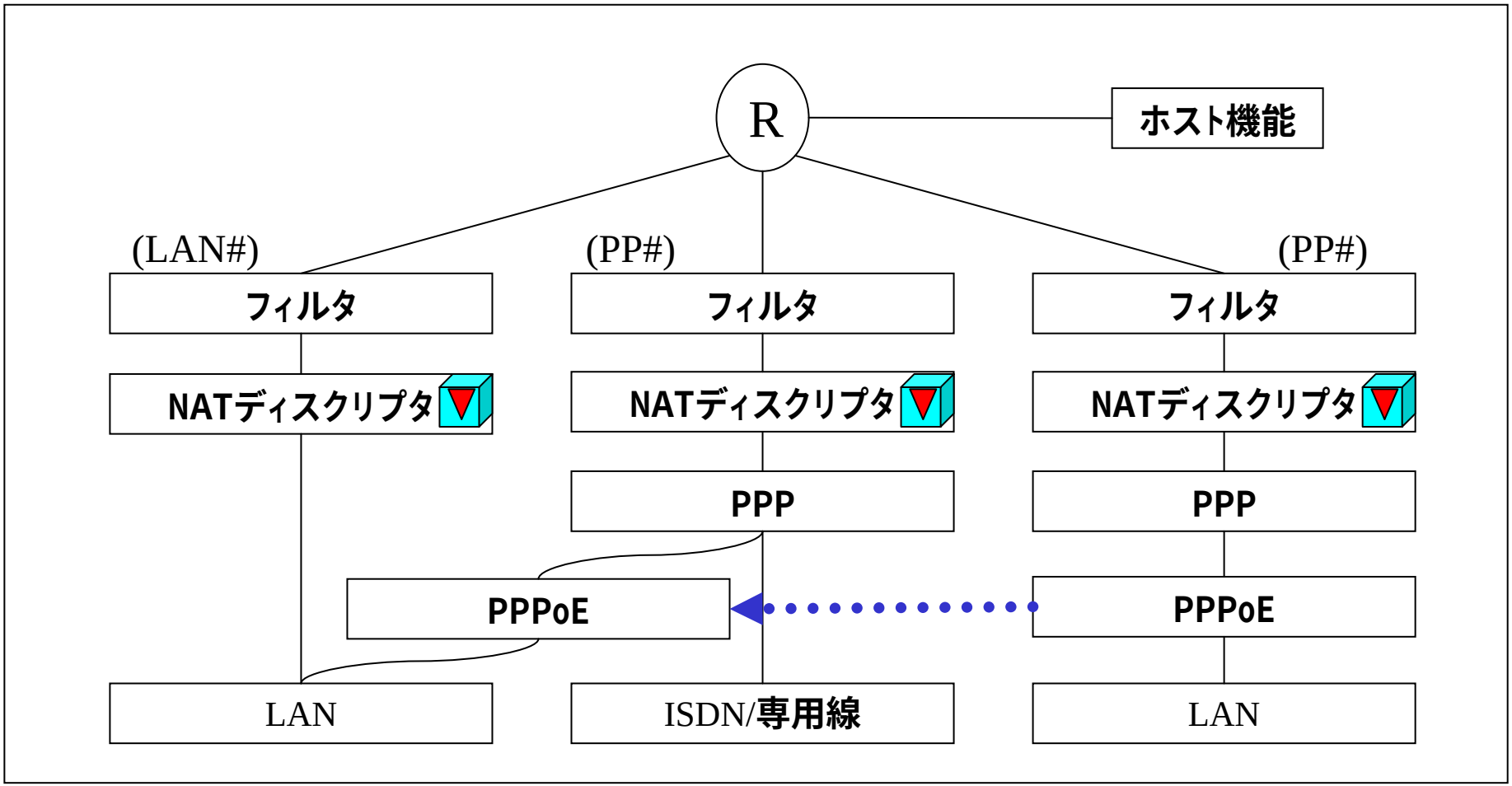
RTW65b

RTA54i

比較構成例



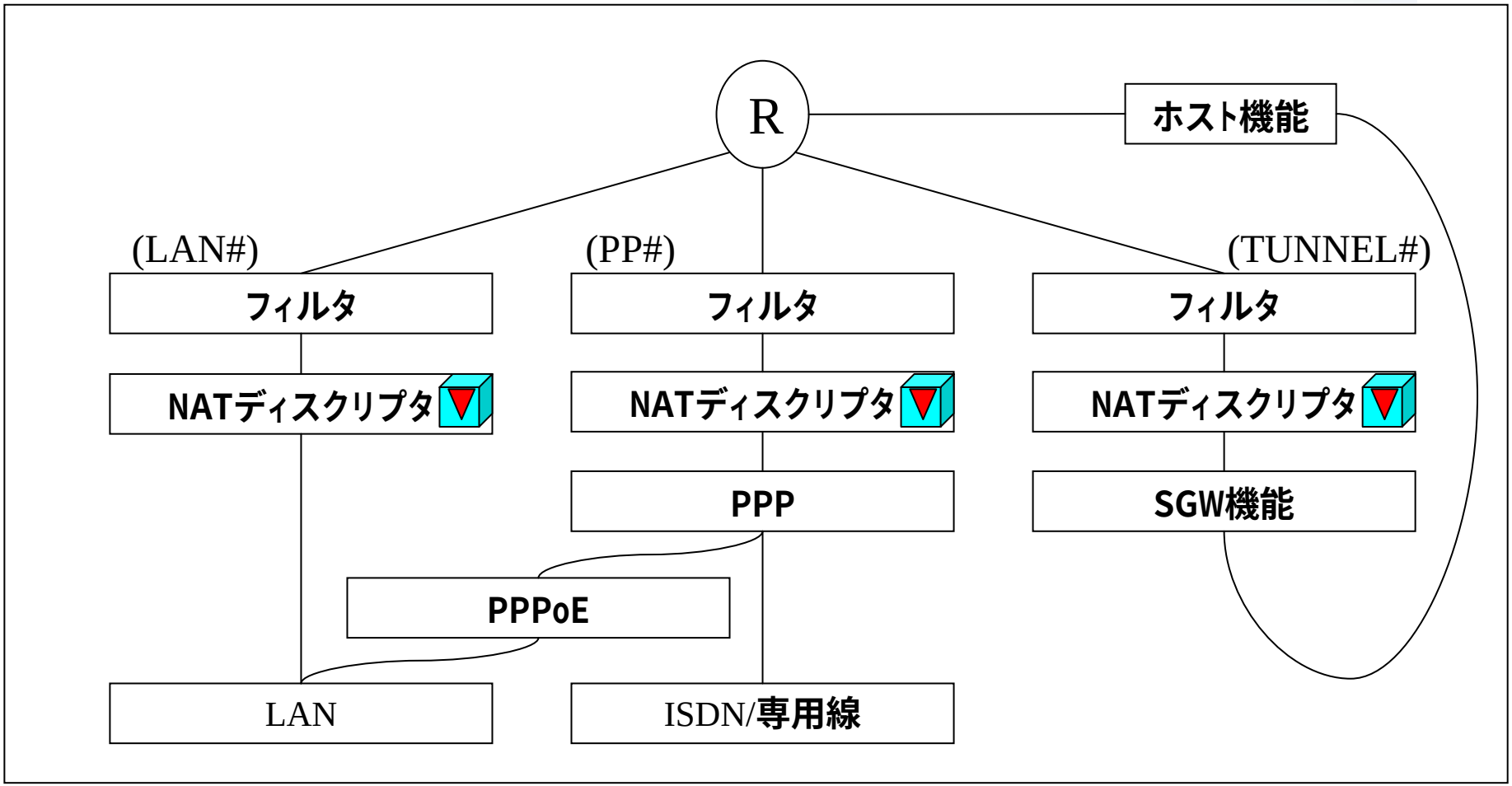
構造#3(PPPoE)


R
ホスト機能
(LAN#)
(PP#)
(PP#)
フィルタ
フィルタ
フィルタ
NATディスクリプタ
NATディスクリプタ
NATディスクリプタ
PPP
PPP
PPPoE
PPPoE
LAN
ISDN/専用線
LAN

RT300i

構造#4(VPN)

RT105シリーズ



NATディスクリプタ

- NATディスクリプタの特徴
  - a) IPマスカレード形式
  - b) NAT形式
  - c) NAT+IPマスカレード形式
- NATディスクリプタの構造
- 応用例#1,#2
- IPマスカレードの処理選択
- IPマスカレードの例外処理

NATディスクリプタの特徴

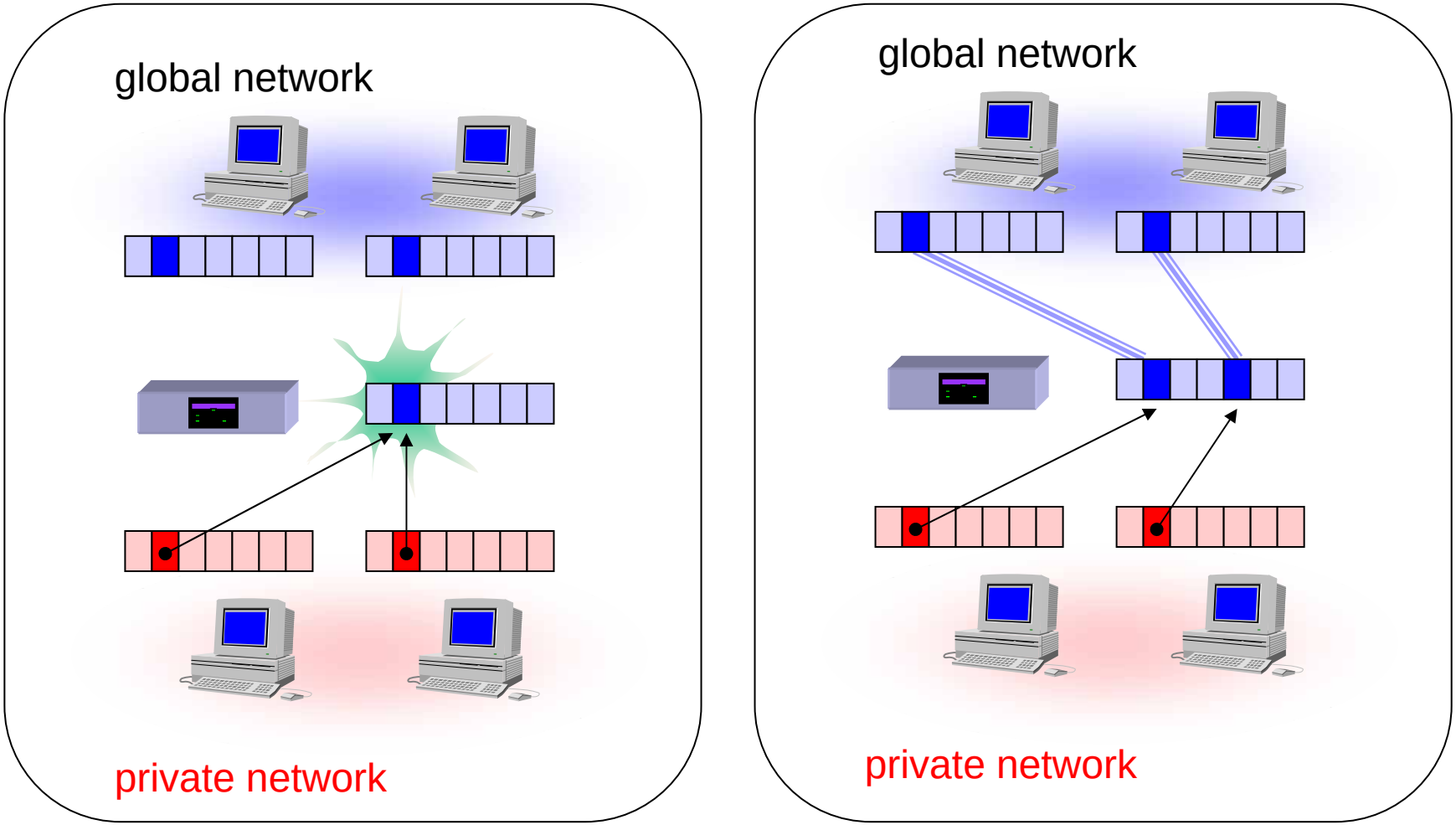
- LANインタフェースに対応
  - LANのprimary⇔secondaryの変換が可能
- TUNNELインタフェースに対応
  - VPNで変換が可能
- 3つの変換タイプ
  - NAT形式
  - IPマスカレード形式
  - NAT + IPマスカレード形式
- 制限の緩和
  - 複数の変換規則を並列的に適用可能
    (ひとつのインタフェースに16組)

アドレス変換機能の優位点

- LAN,PP(PPP&PPPoE),TUNNEL(IPsec)に自在に適用可能
- IPマスカレード:ひとつのインタフェースに16個
- NAT:メモリの許す限り無制限
- VPNパススルー(出来て当然)
- DMZホスト機能(IPマスカレードのincoming処理選択)
- 本格的なFTP,CU-SeeMe,NetMeeting Version 3.0対応
  通信データ内のアドレス情報などを書き換えることで
  アドレス変換越しでも安定した通信が可能となる。

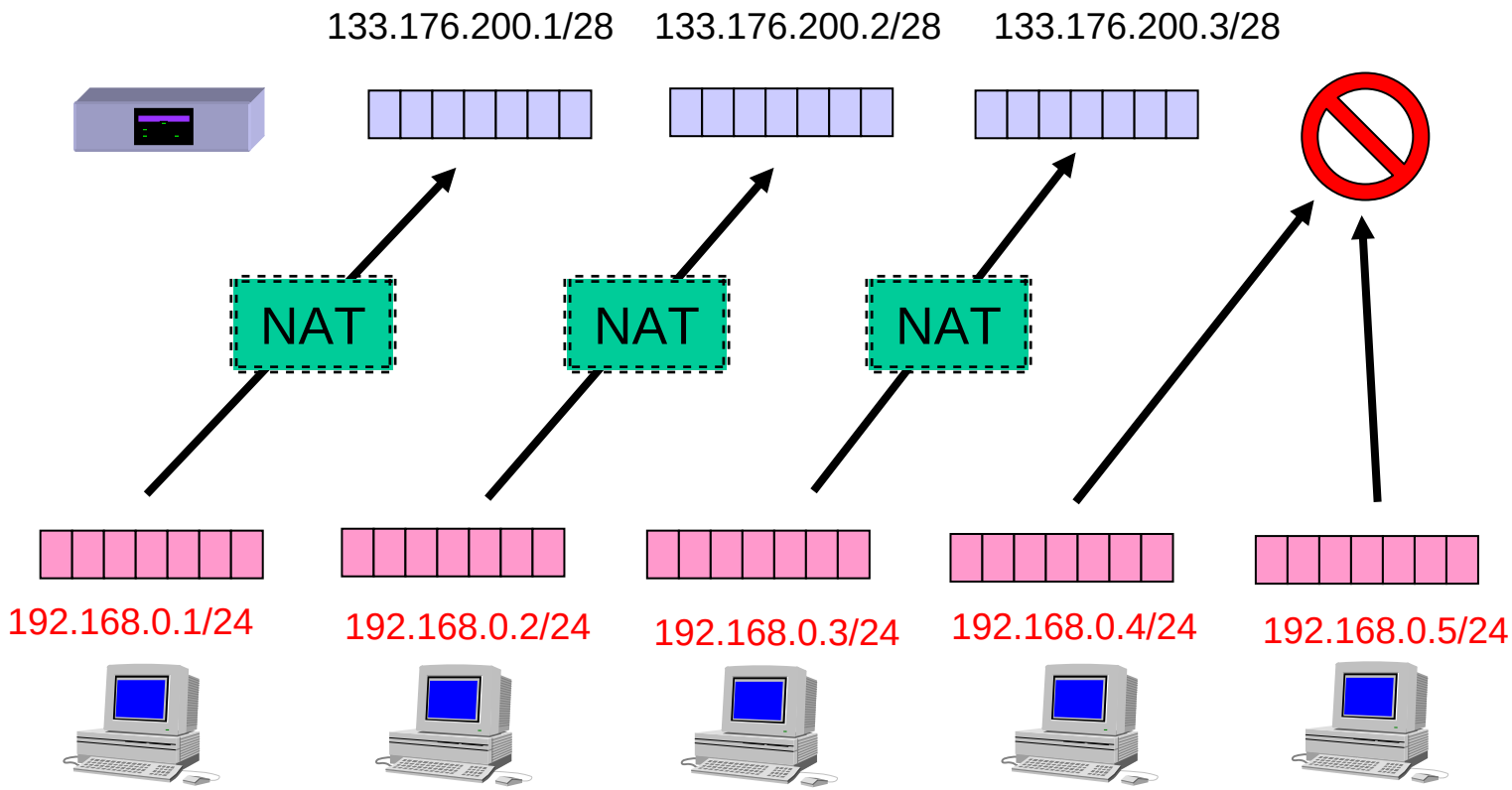
IPマスカレード(IP Masquerade)

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



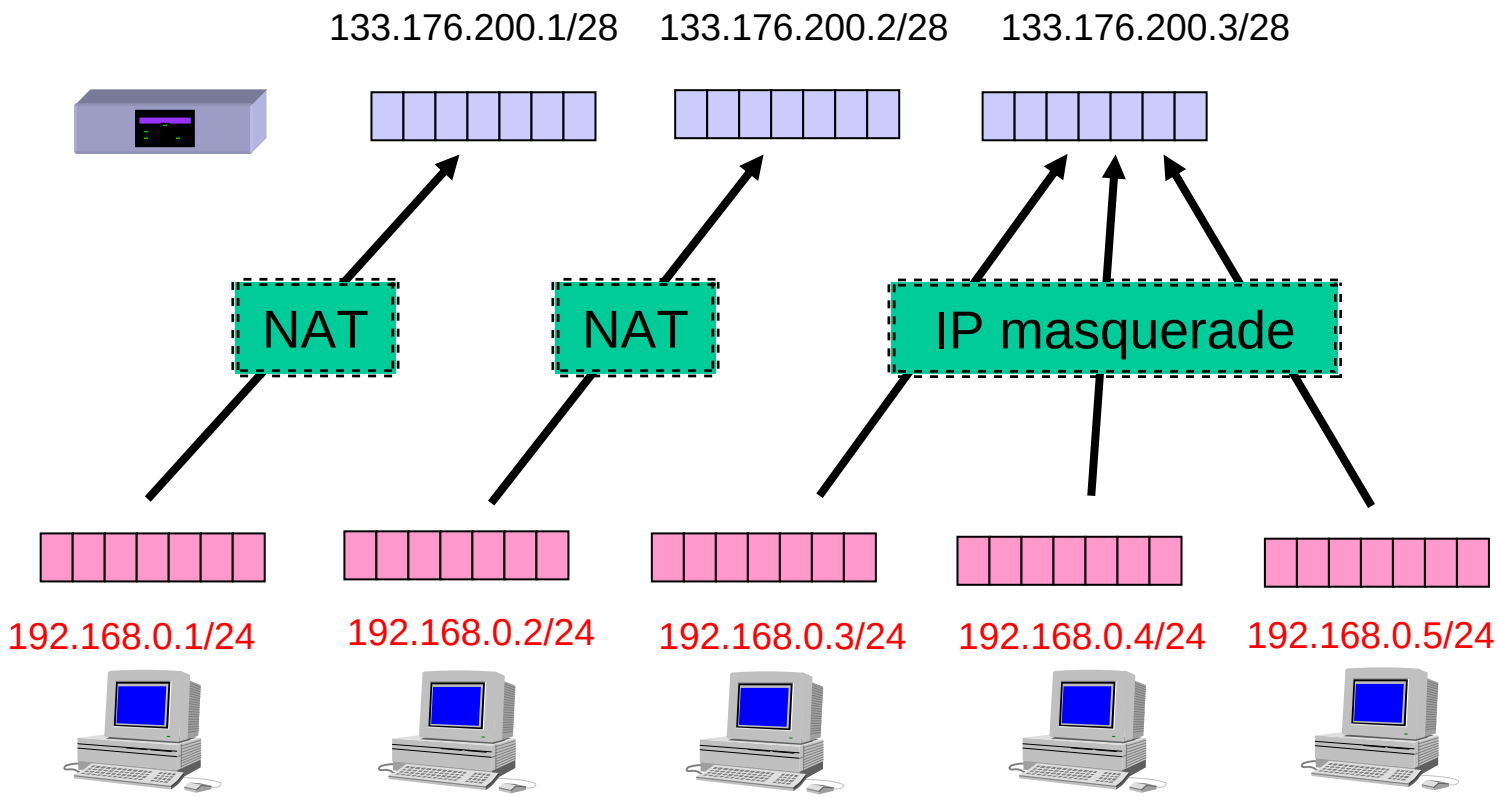
NAT (Network Address Translation)

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

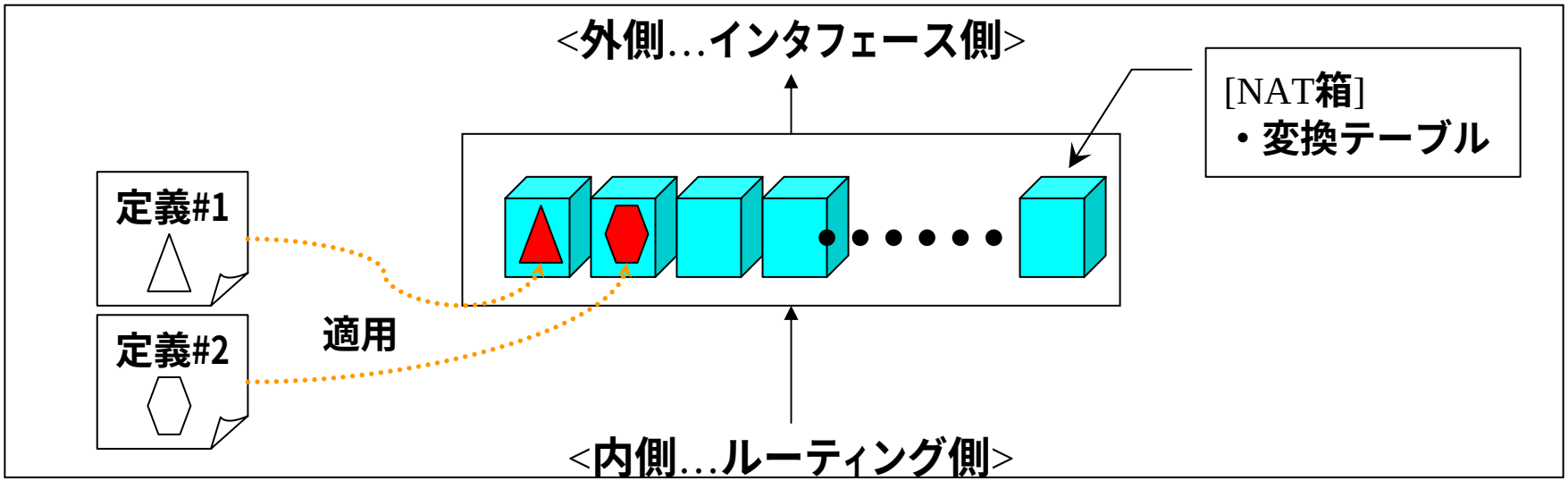


NAT + IPマスカレード形式

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

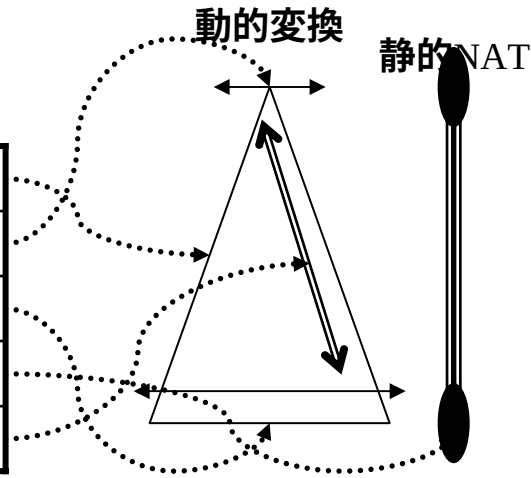


NATディスクリプタの構造

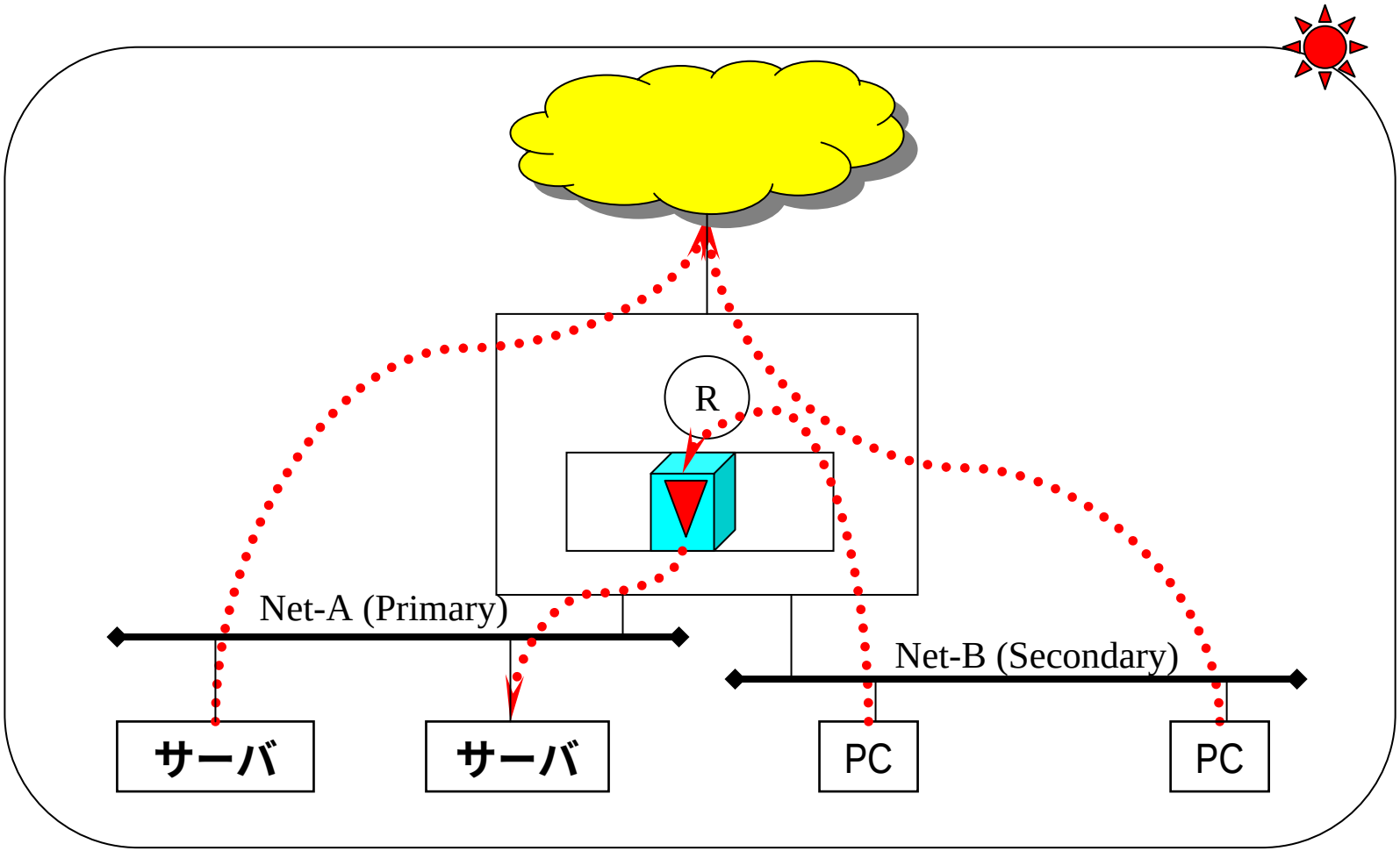


[定義→アドレス変換の設計図]

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

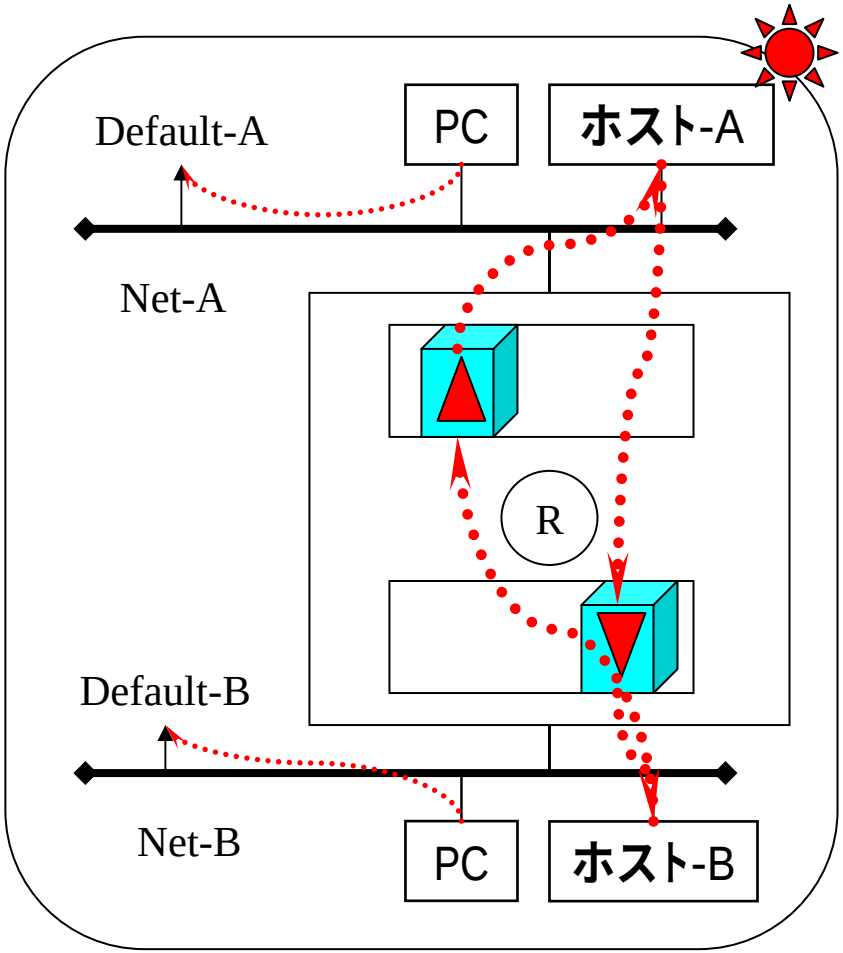


NATディスクリプタの応用例#1

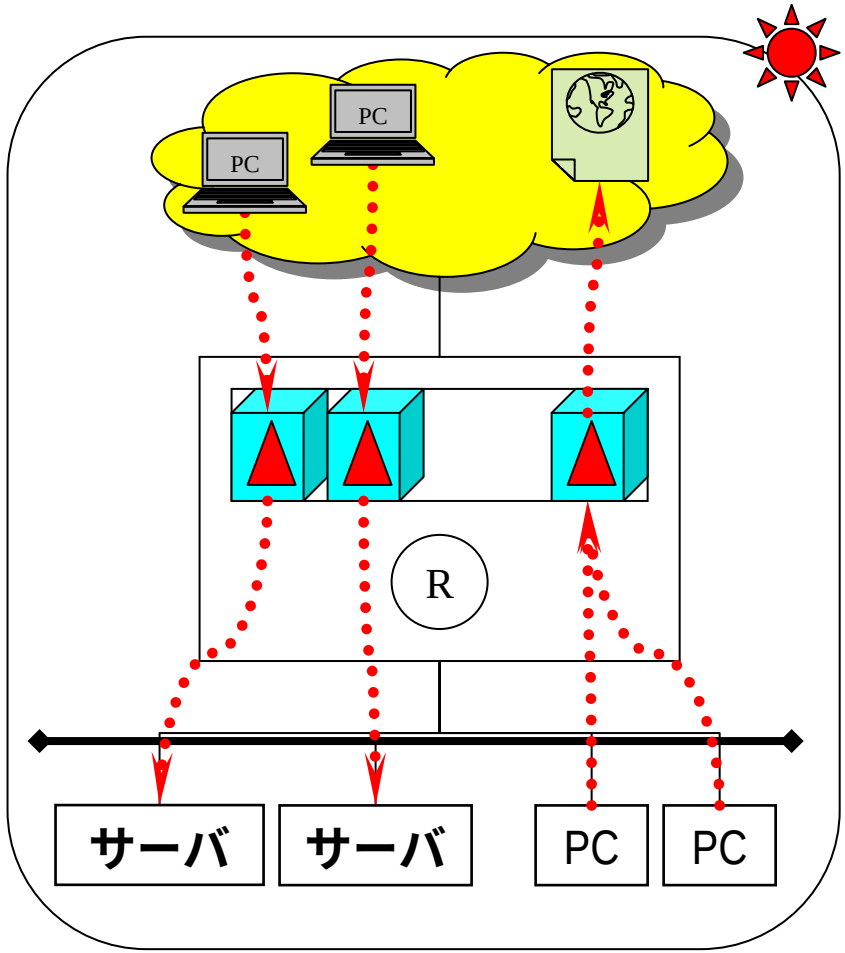


primary⇔secondary間のIPマスカレード (逆マスカレード)

NATディスクリプタの応用例#2

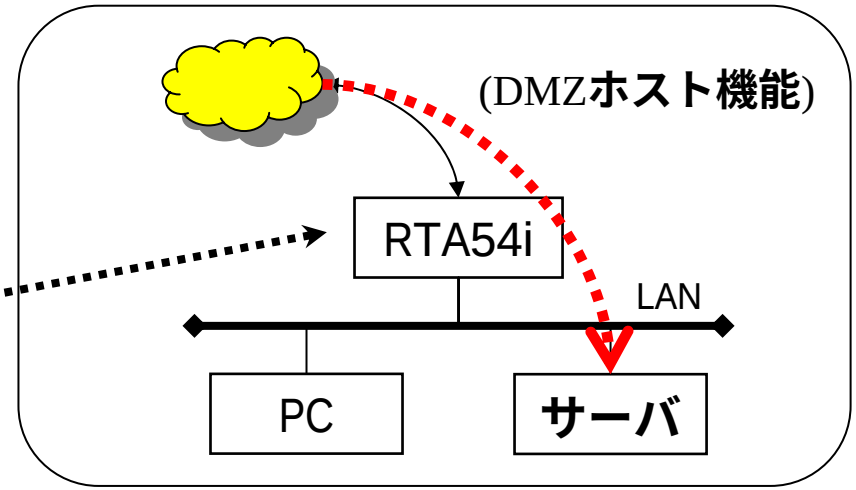


2つの隔離されたネット間での通信(hot line)



公開サーバにIPマスカレード適用

IPマスカレードの処理選択

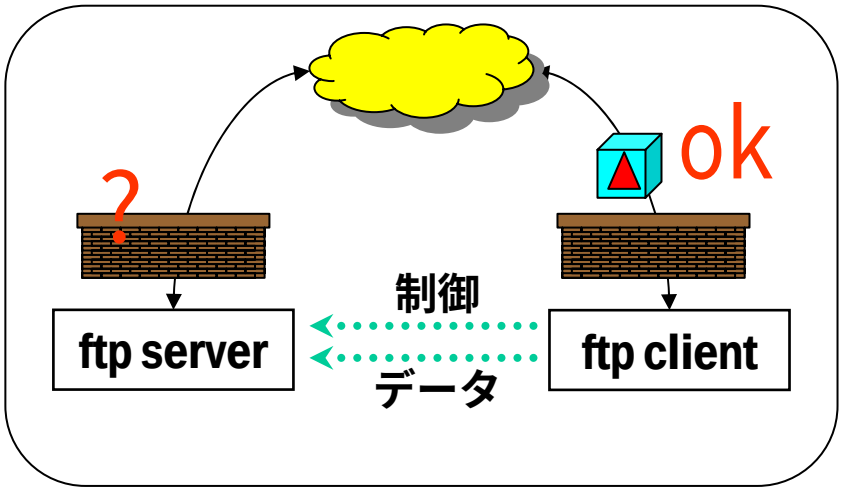


ISDN/ADSL/CATVプロバイダ接続(LAN)

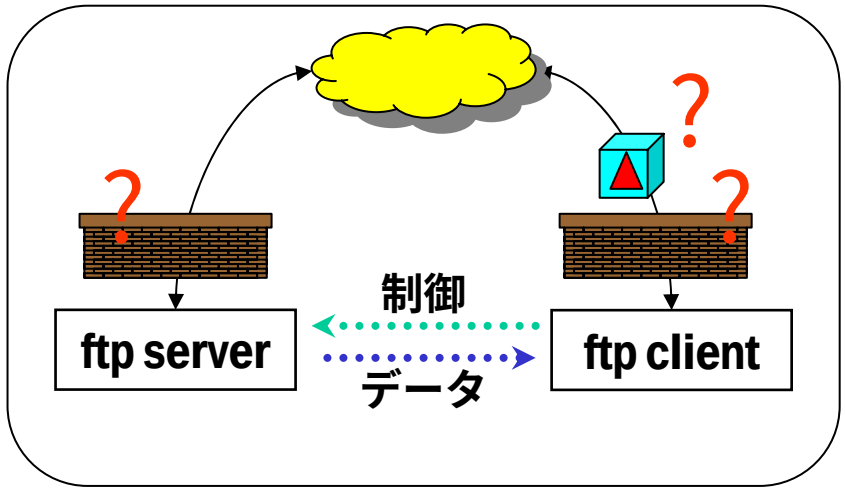
[IPマスカレードのincoming packetに関する処理選択]

- through … 変換せずに通す (疎通性→外からping OK)
- reject … 破棄して、TCPの場合はRSTを返す (セキュリティ性)
- discard … 破棄して、何も返さない (ステルス性)
- forward … 指定されたホストに転送する
  (DMZホスト機能、ネットアプリの対応性)

IPマスカレードの例外処理



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

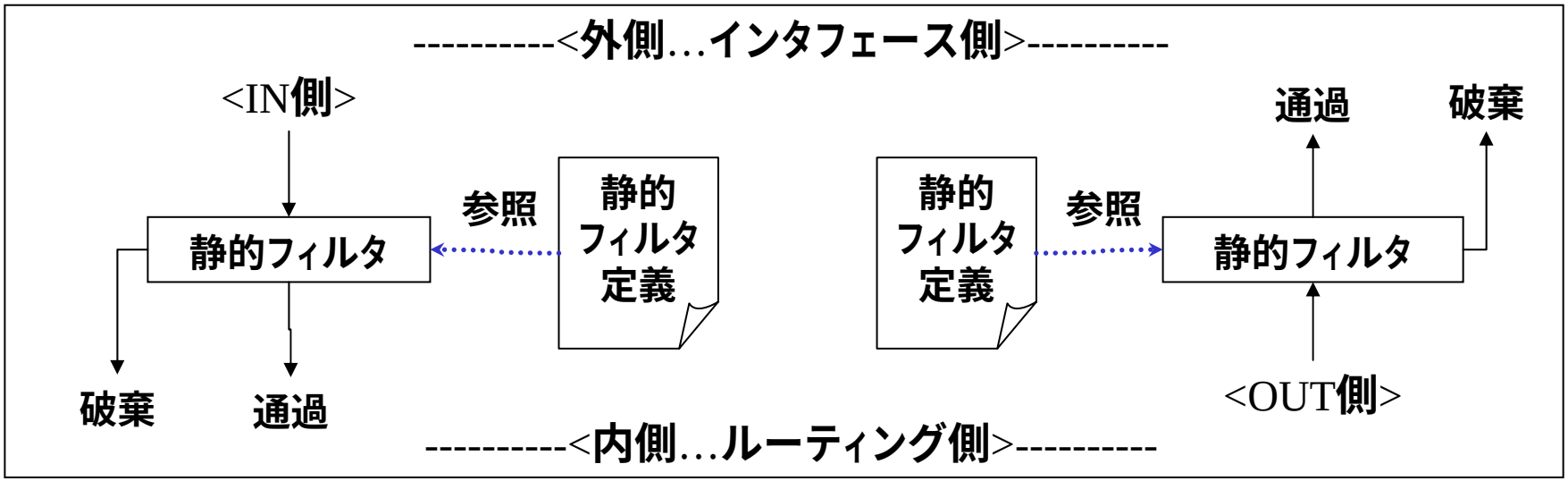
[例外処理を必要とする通信]

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

ファイアウォール機能
(パケット･フィルタリング)

- 従来のパケット・フィルタリング
- 従来のセキュリティ・フィルタ
- 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
- 一部の通信路を塞ぐ
- 静的セキュリティ・フィルタ
- 動的セキュリティ・フィルタ

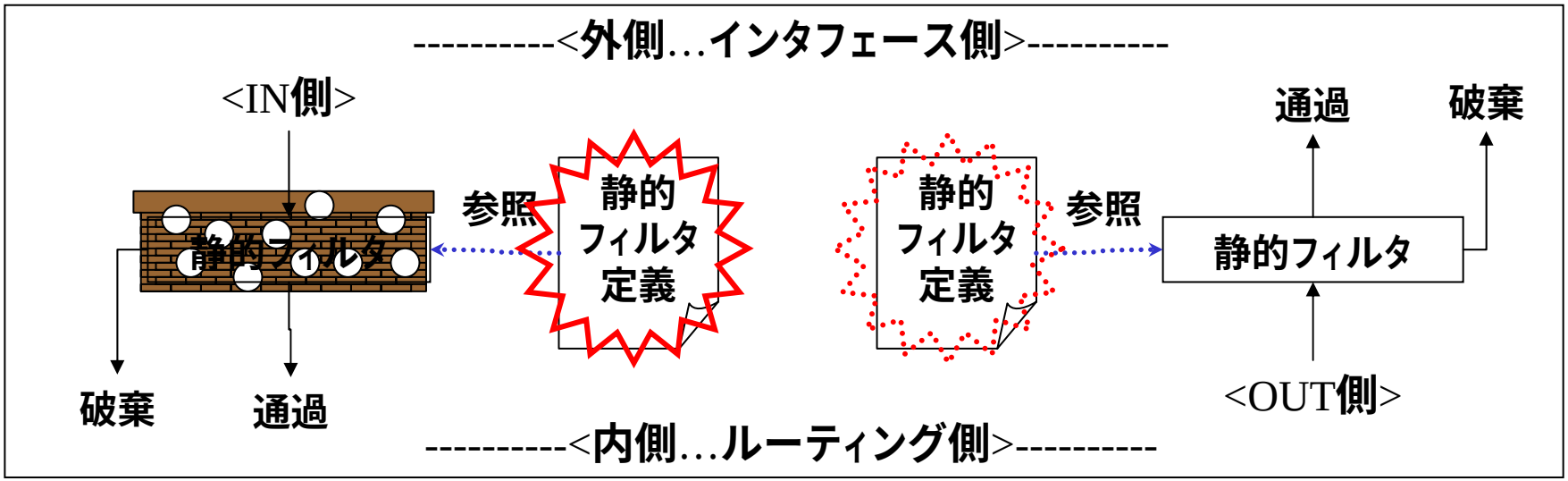
従来のパケットフィルタリング



[静的フィルタの問題点]

- TCP：一方向性のestablishedフィルタの限界
  判断条件)TCPフラグのうちACKとRSTのいずれかがセット
- UDP：必要なポートは常に開けておく。
  例）DNS、NTP

従来のセキュリティ・フィルタ



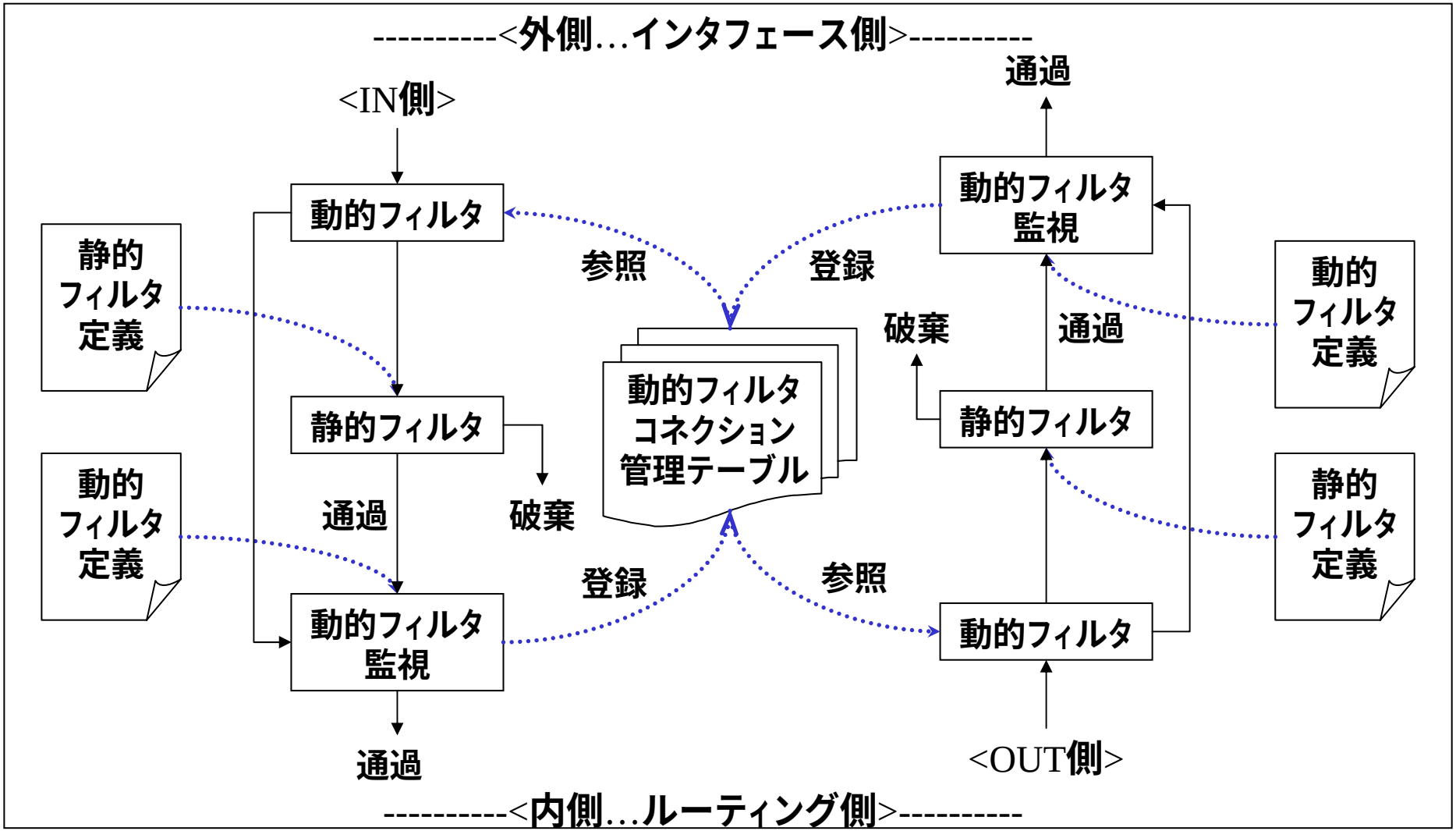

```
# フィルタ定義例（LAN側ネットワークが192.168.0.0/24の場合）
ip filter 10 reject 192.168.0.0/24 * * * *
ip filter 11 pass * 192.168.0.0/24 icmp * *
ip filter 12 pass * 192.168.0.0/24 established * *      # tcpの片方向性を実現する仕組み
ip filter 13 pass * 192.168.0.0/24 tcp * ident          # メール転送などの時の認証(ident)
ip filter 14 pass * 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
```

セキュリティ・レベル

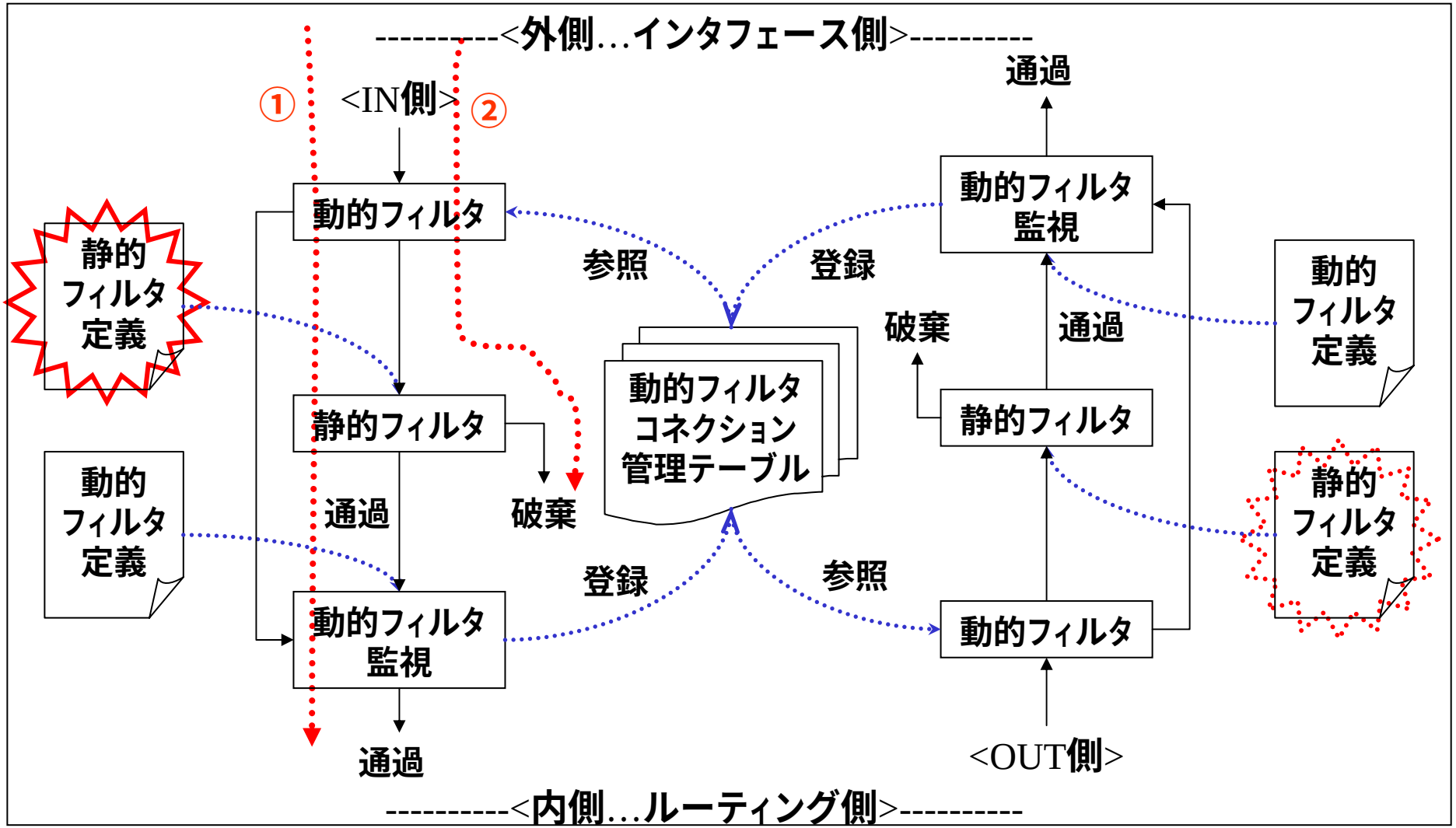
(ネットボランチのセキュリティ強度の選択機能)

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)						☆	☆

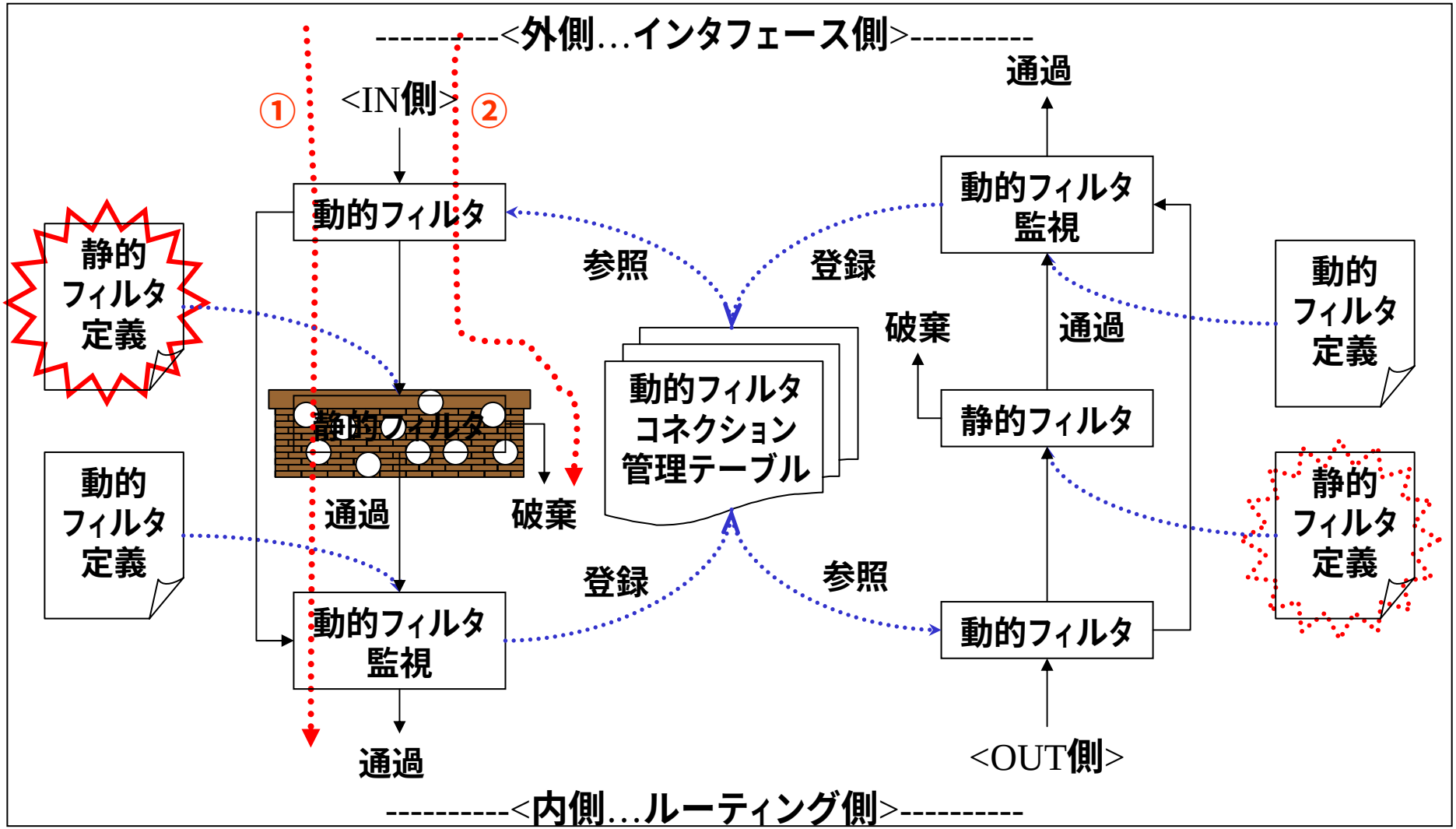
ファイアウォールの構造



一部の通信路を塞ぐ


----------<外側…インタフェース側>----------
①
<IN側>
②
通過
動的フィルタ
監視
静的
フィルタ
定義
動的フィルタ
参照
登録
動的フィルタ
コネクション
管理テーブル
破棄
通過
静的フィルタ
動的
フィルタ
定義
静的フィルタ
破棄
通過
動的
フィルタ
定義
登録
参照
動的フィルタ
監視
動的フィルタ
静的
フィルタ
定義
通過
<OUT側>
----------<内側…ルーティング側>----------

静的セキュリティ・フィルタ



```
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 * * * * *
```

設定例#1

(静的セキュリティフィルタ)

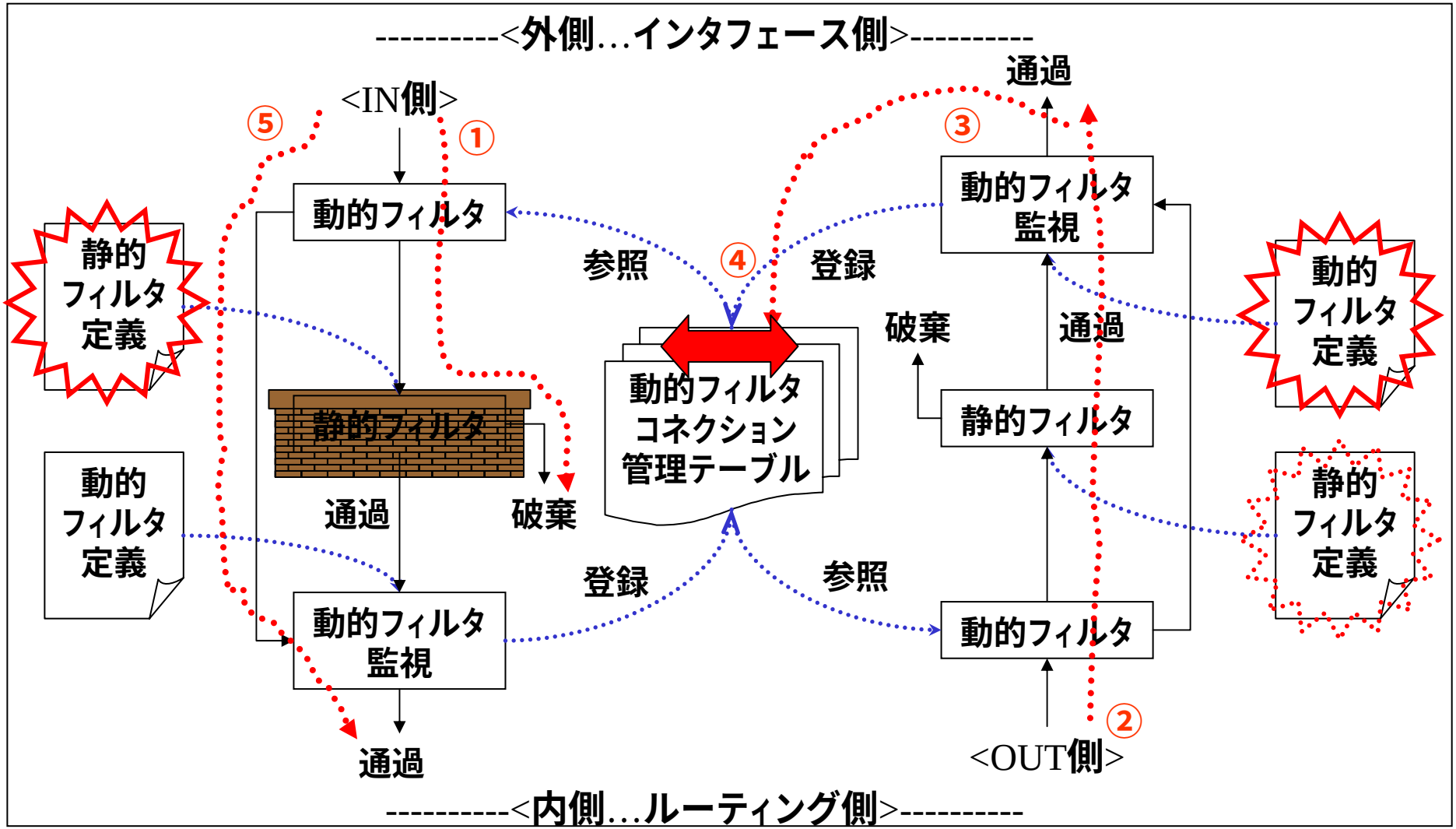
[条件]

- 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| # 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
```

動的セキュリティ・フィルタ



```
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 * * * * *
```

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| # 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
```

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)

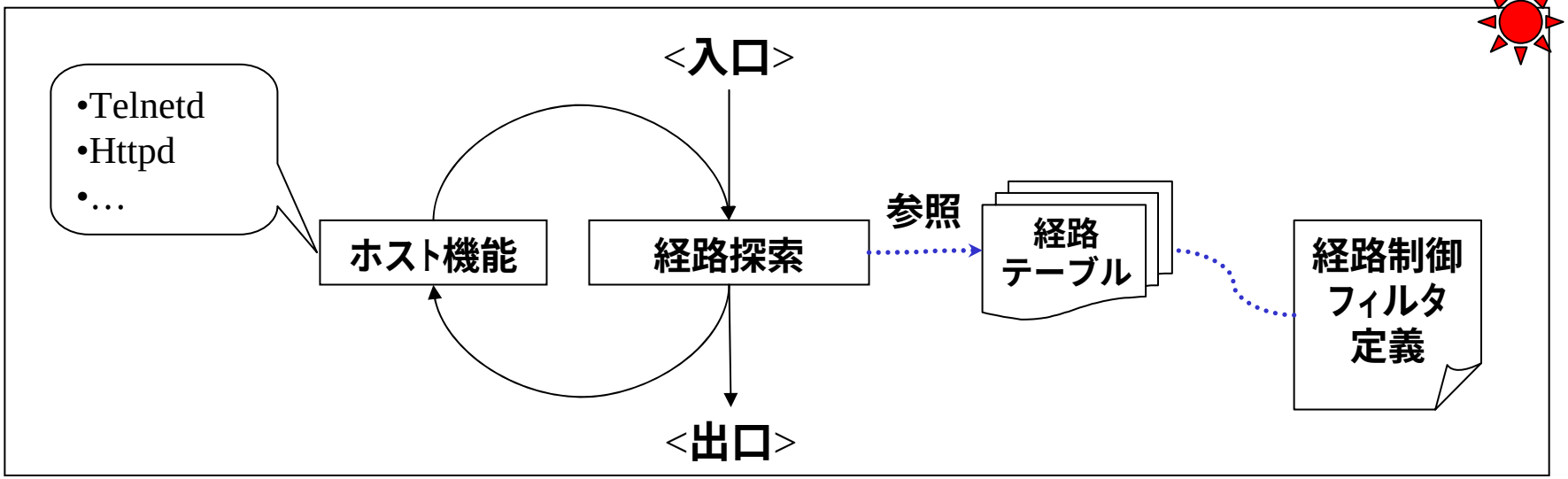
RTA50i

RTA52i *RTA54i*

拡張

RT300i

フィルタ型ルーティングの構造



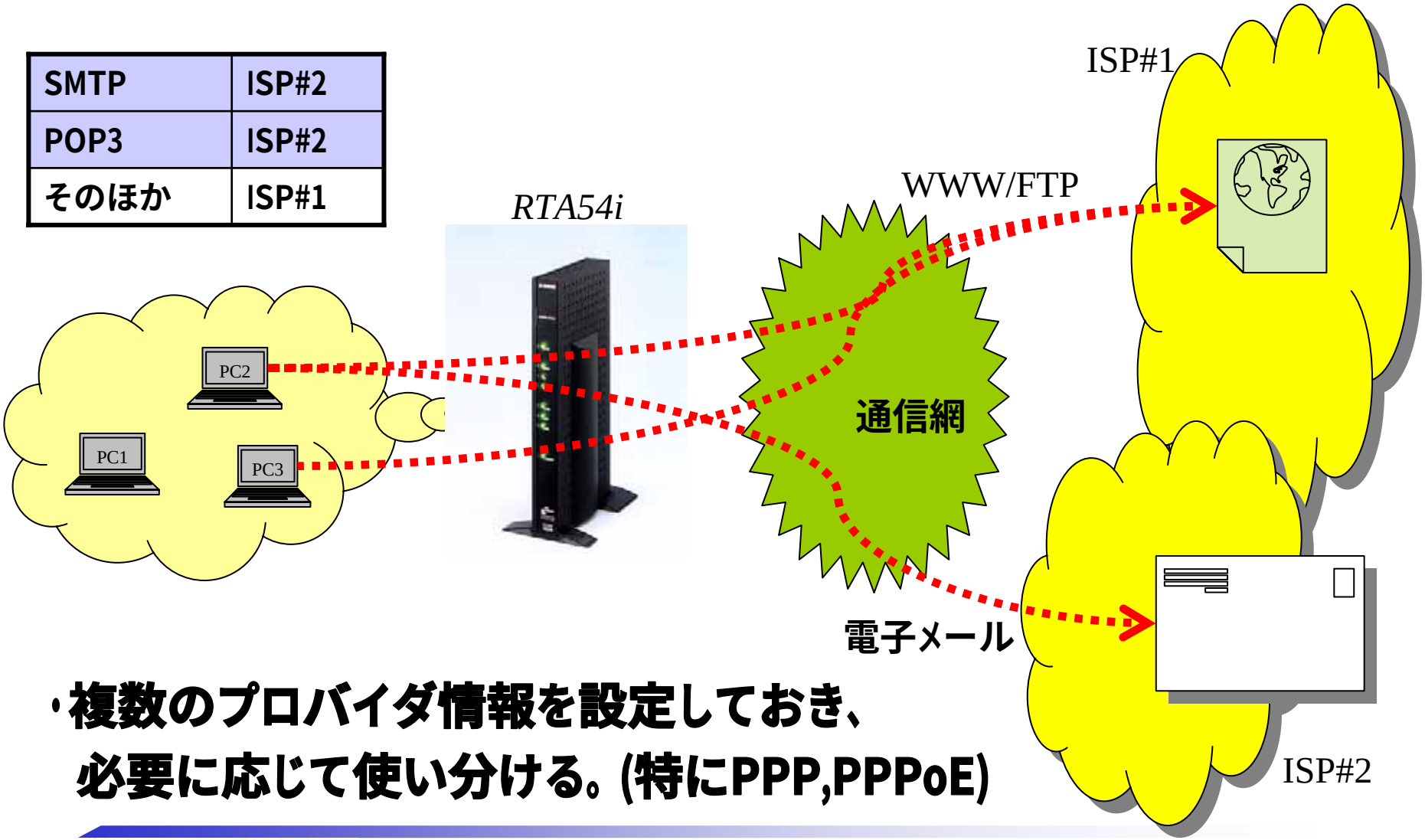
[経路を判別する内容]

☆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**

プロトコル毎プロバイダ選択

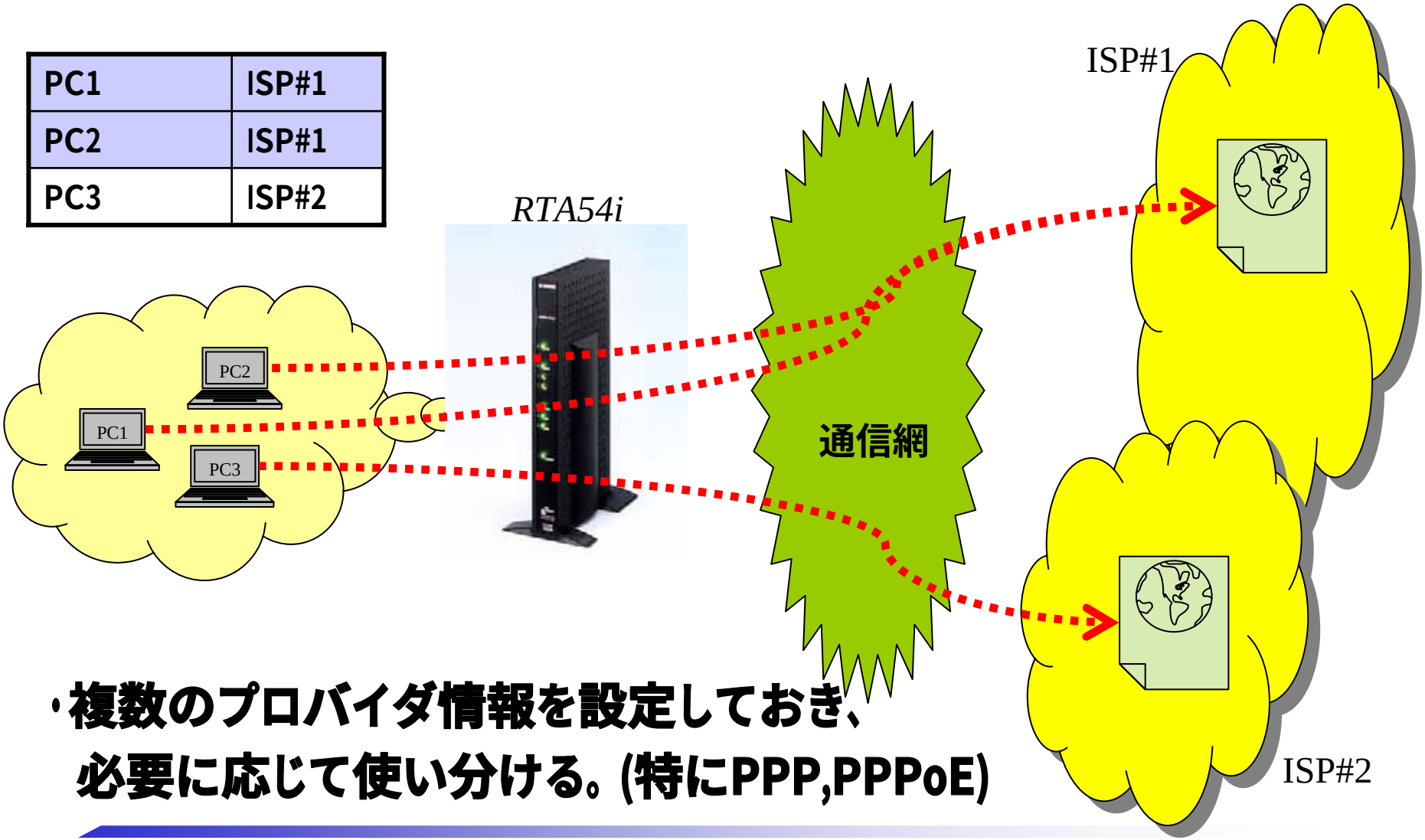
SMTP	ISP#2
POP3	ISP#2
そのほか	ISP#1



・複数のプロバイダ情報を設定しておき、
必要に応じて使い分ける。(特にPPP,PPPoE)

ホスト毎プロバイダ選択

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

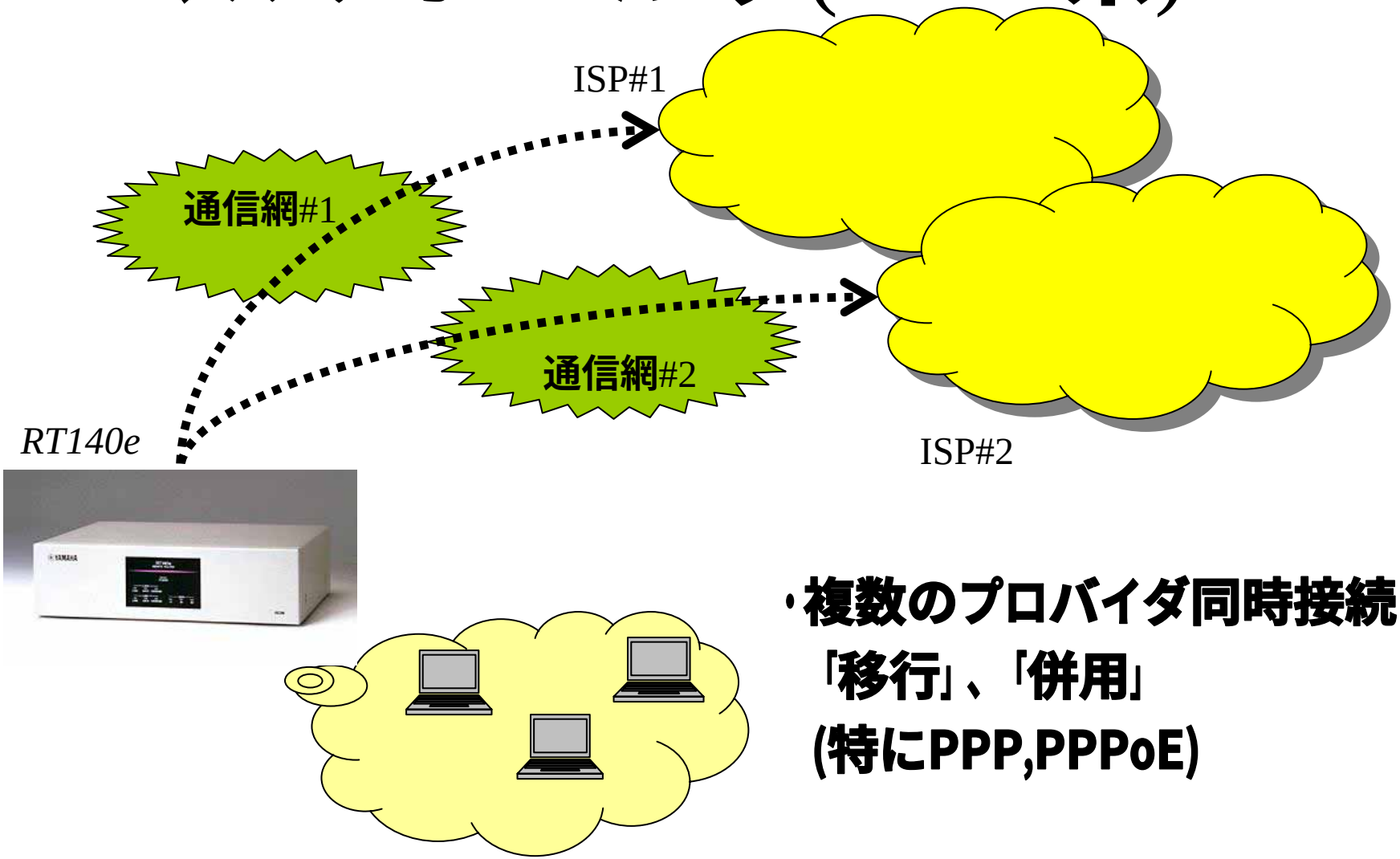


・複数のプロバイダ情報を設定しておき、
必要に応じて使い分ける。(特にPPP,PPPoE)

接続状態に応じたプロバイダ選択

・複数のプロバイダ情報を設定しておき、
必要に応じて使い分ける。(特にPPP,PPPoE)

マルチホーミング(Rev.6系)



・複数のプロバイダ同時接続
「移行」、「併用」
(特にPPP,PPPoE)

ヤマハルータ
の
いろいろな使い方
「NetVolante」

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

	RTA54i	RT60w	RTW65b
ISDN U	1	1	–
ISDN S/T	1	1	–
TELポート	2	3	–
WANポート	1	–	1
LANポート	4(HUB)	4(HUB)	1
無線LAN(IEEE 802.11b)	–	–	1
USBポート	1	–	1
液晶ディスプレイ	–	1	–
LED	8(前)+4(後)	7	7

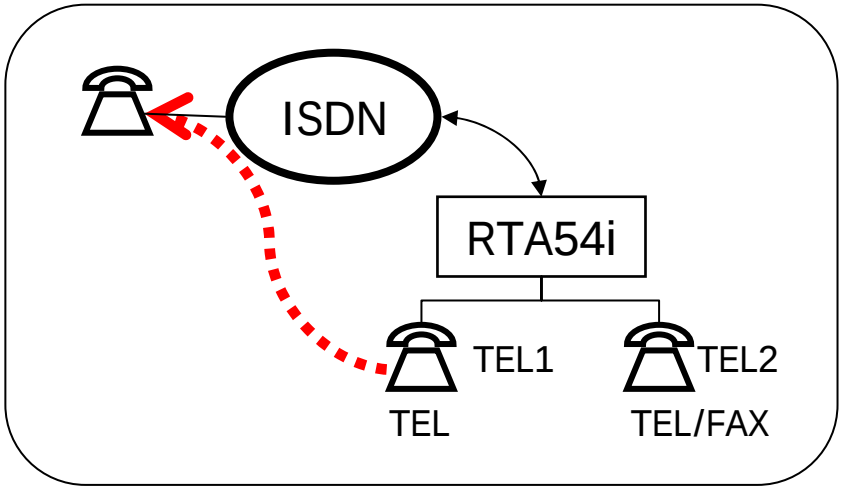
NetVolanteにおけるUSBポート

～～RS-232C(シリアル)ポートからUSBポートへ～～

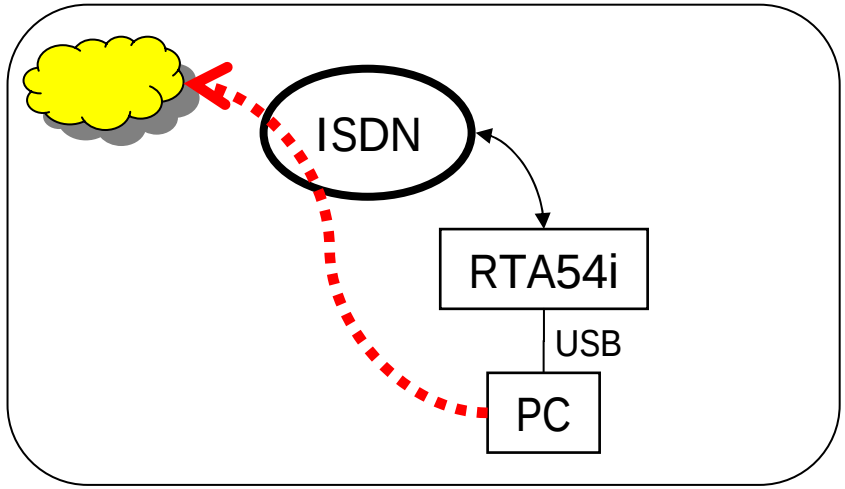
RS-232Cに比べて、高速化が可能

a) 擬似LAN機能で、スループット向上
b) ブロードバンドTAで、スループット向上
c) ISDN-TA(MP,128Kbps)で、スループット向上
d) コンソール操作も可能、しかも、快適

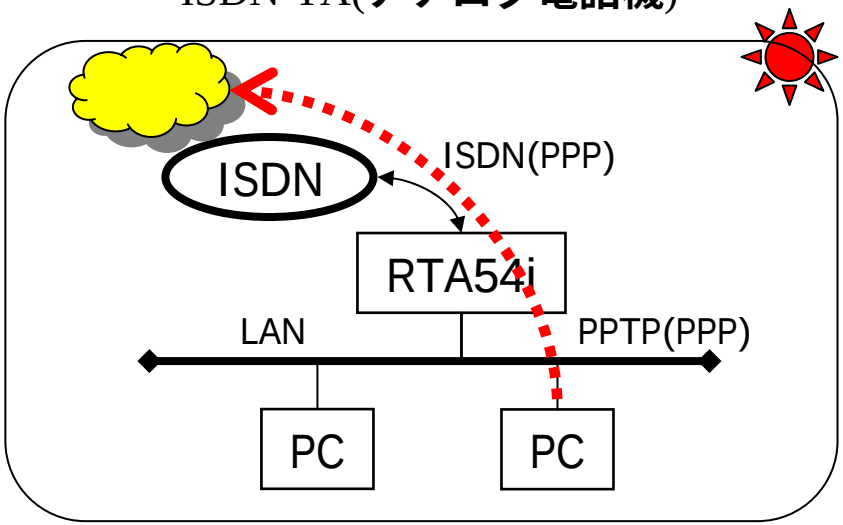
ISDN回線の基本



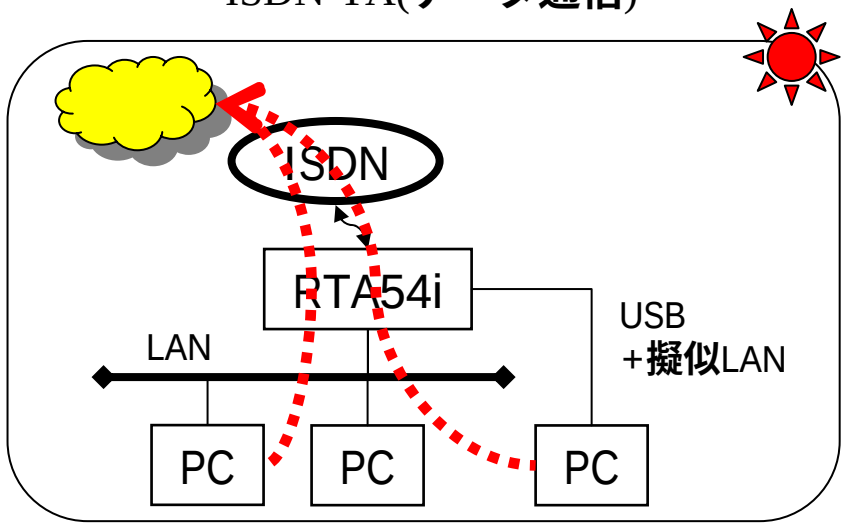
ISDN-TA(**アナログ電話機**)



ISDN-TA(**データ通信**)

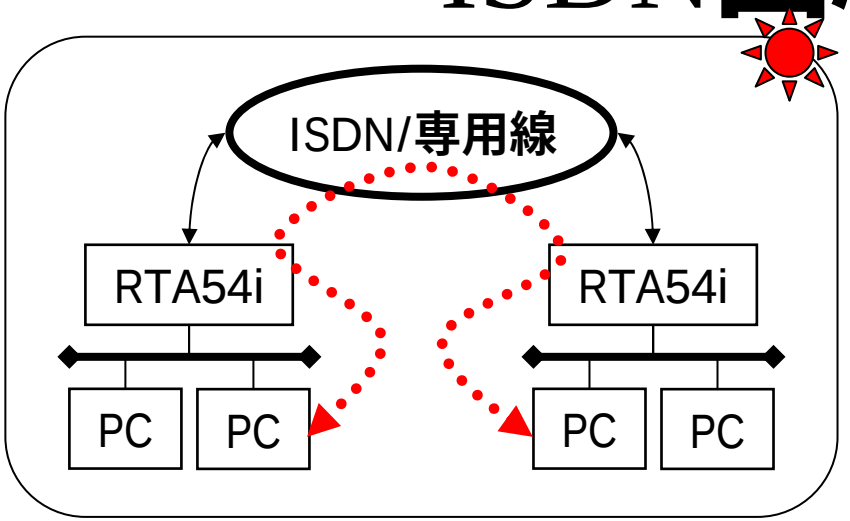


LAN-TA (PPTP client,MS VPN Adapter)

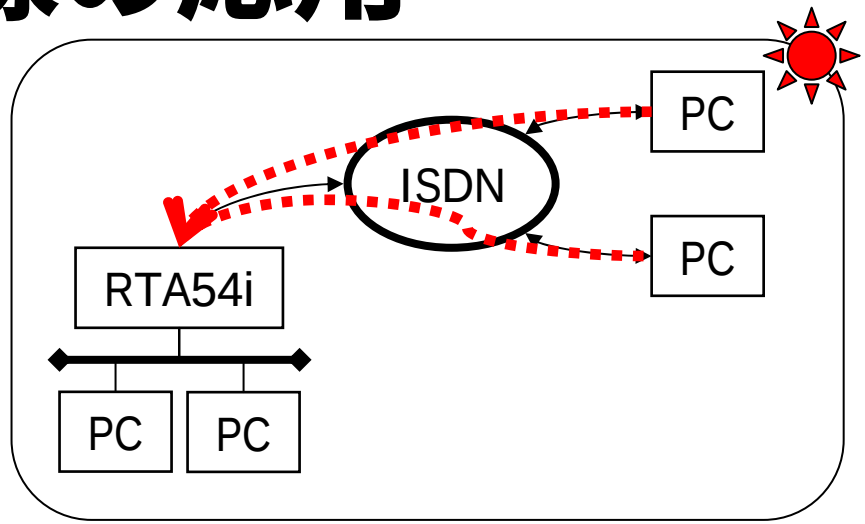


ダイヤルアップ・プロバイダ接続(LAN/USB)

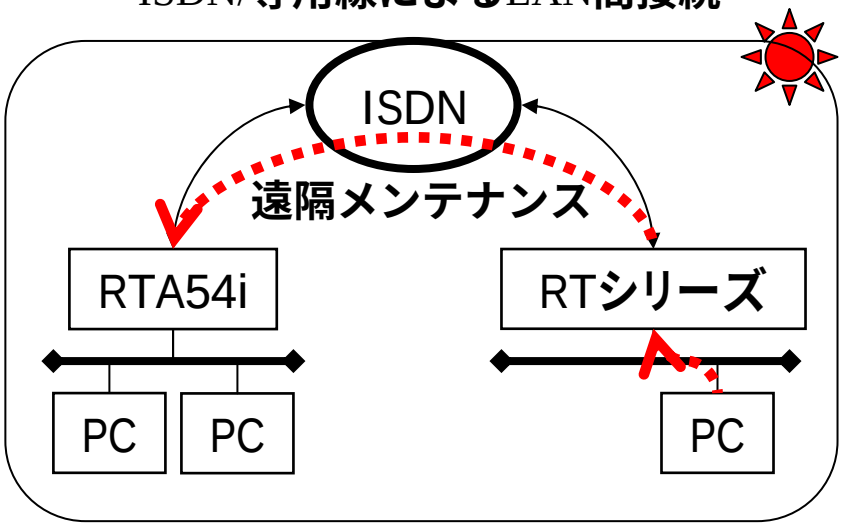
ISDN回線の応用



ISDN/専用線によるLAN間接続

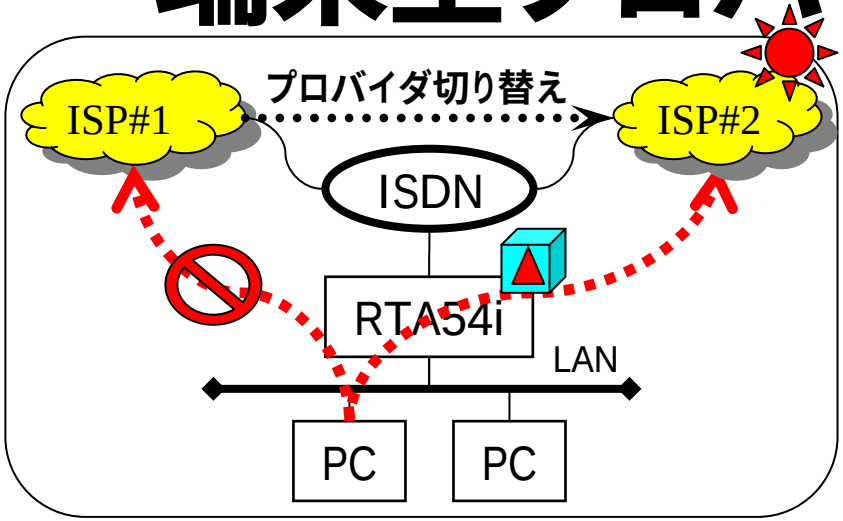


ダイヤルアップサーバ

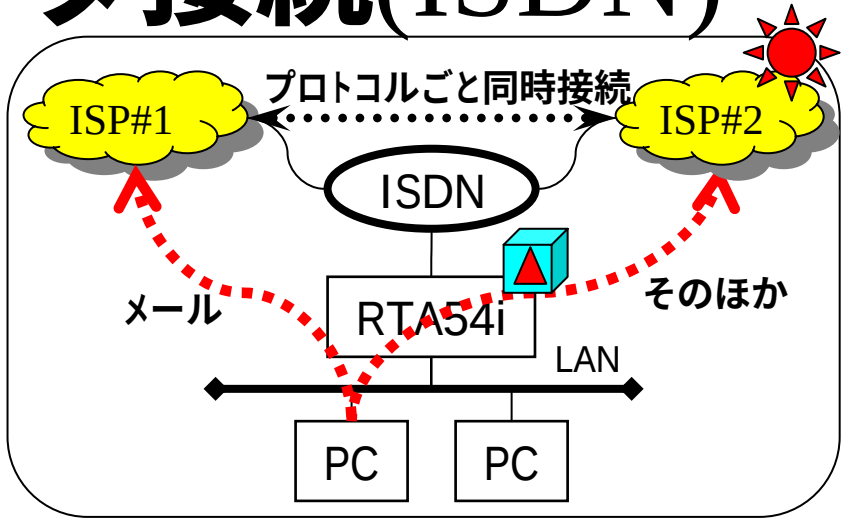


リモートセットアップ

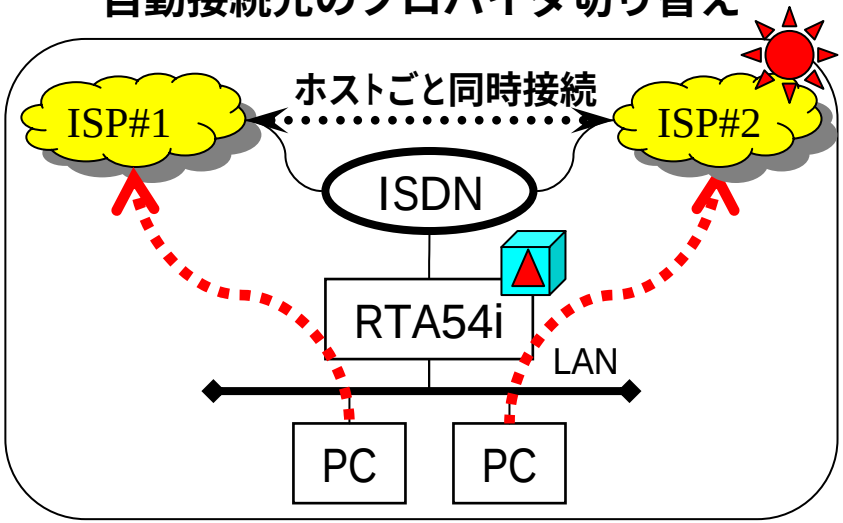
端末型プロバイダ接続(ISDN)



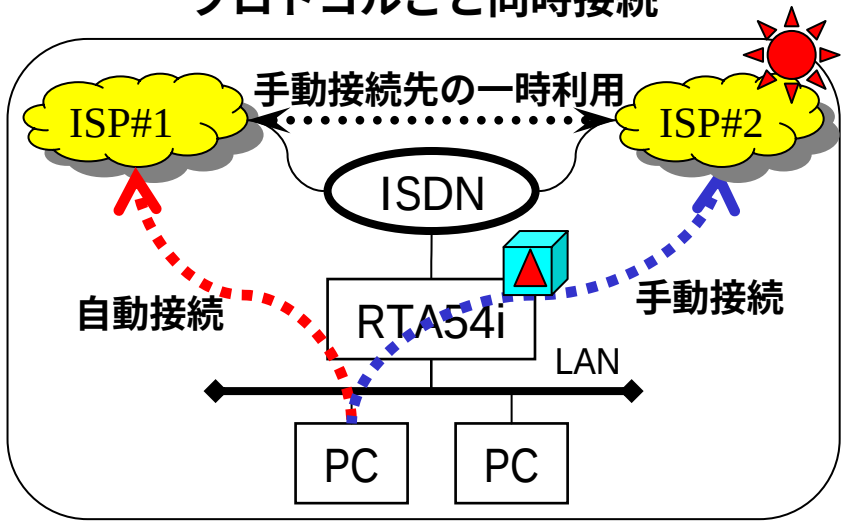
自動接続先のプロバイダ切り替え



プロトコルごと同時接続

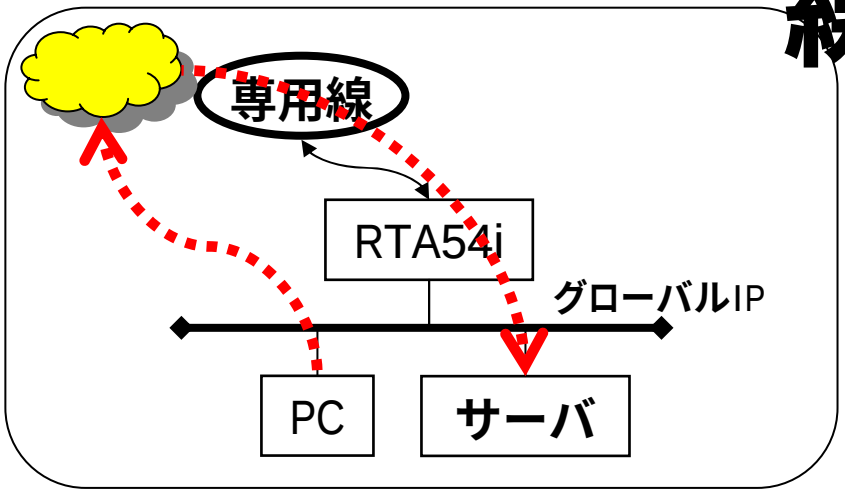


ホストごと同時接続

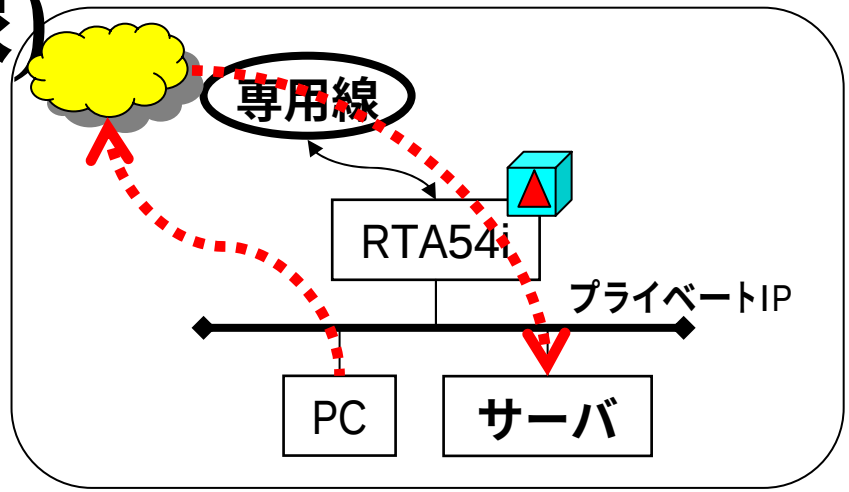


手動接続先の一時切り替え

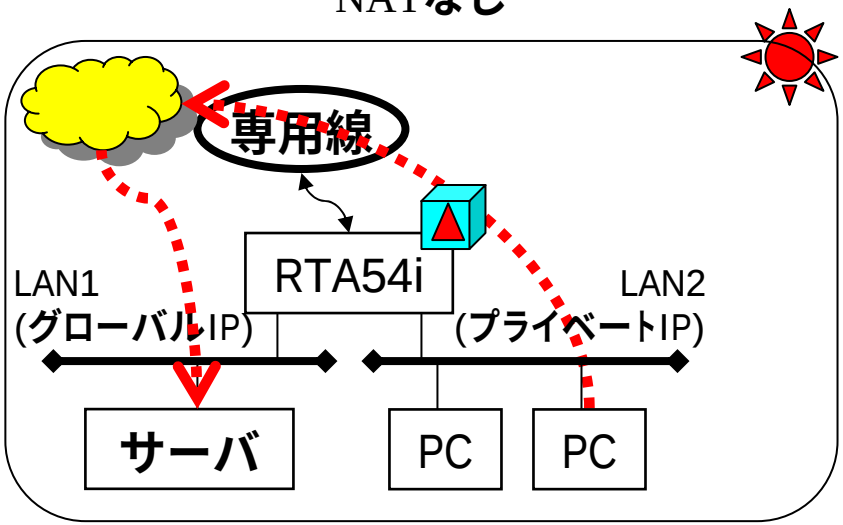
ネットワーク型プロバイダ接続(専用線)



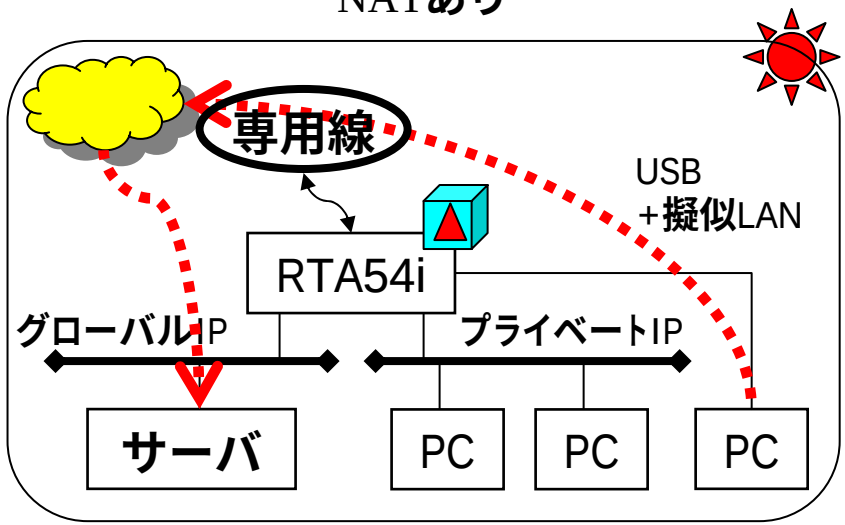
NATなし



NATあり

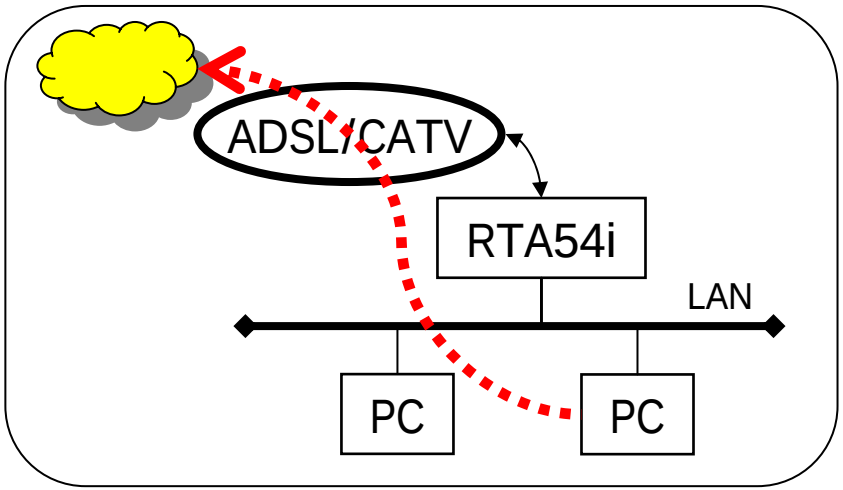


NATなし&あり(LAN1/LAN2)

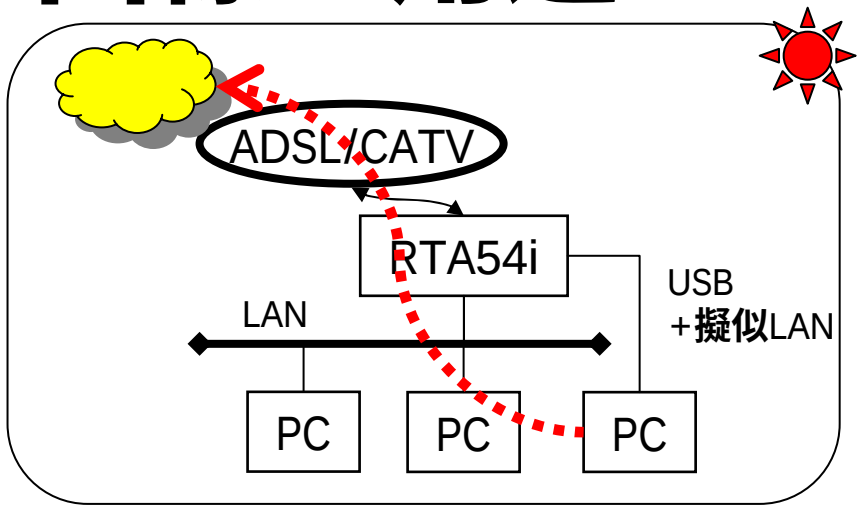


NATなし&あり(USB+擬似LAN)

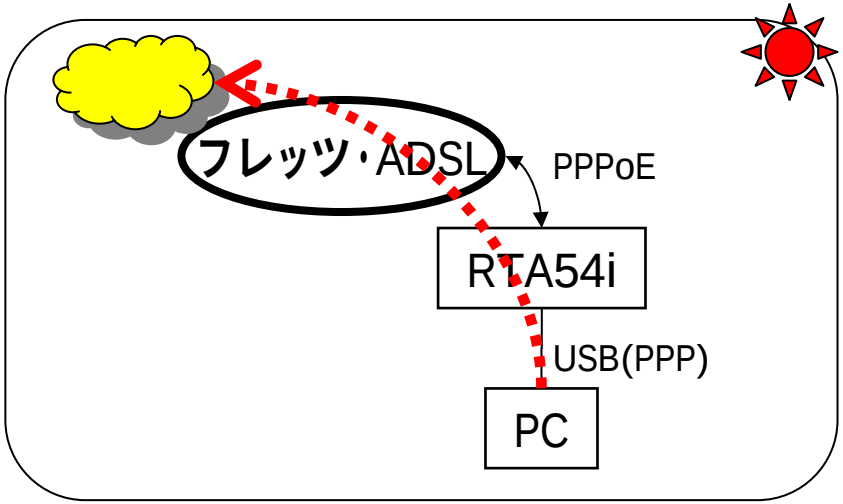
ブロードバンド回線の用途



ADSL/CATV**プロバイダ接続**(LAN)

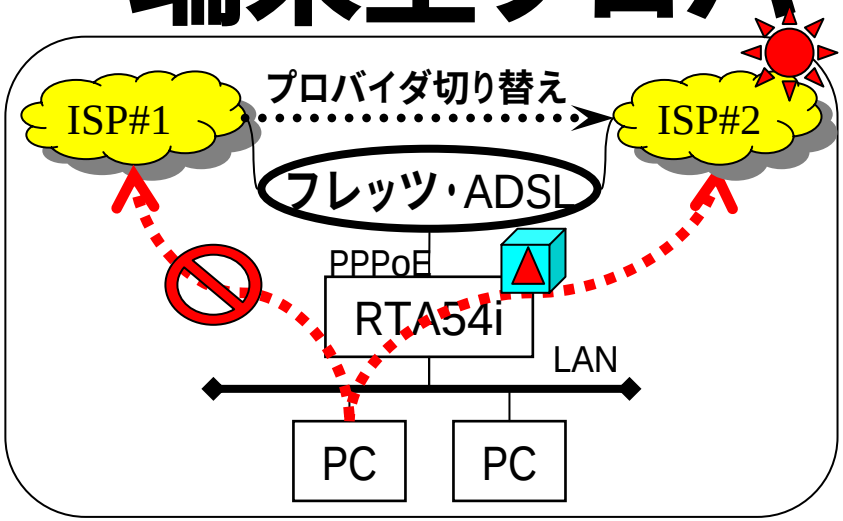


ADSL/CATV**プロバイダ接続**(USB**の擬似**LAN)

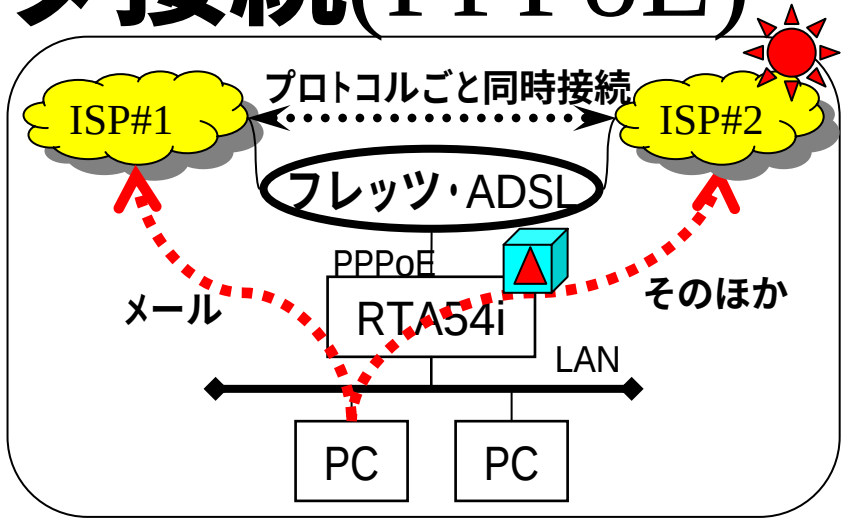


ブロードバンドTA(**フレッツ**・ADSL,USB)

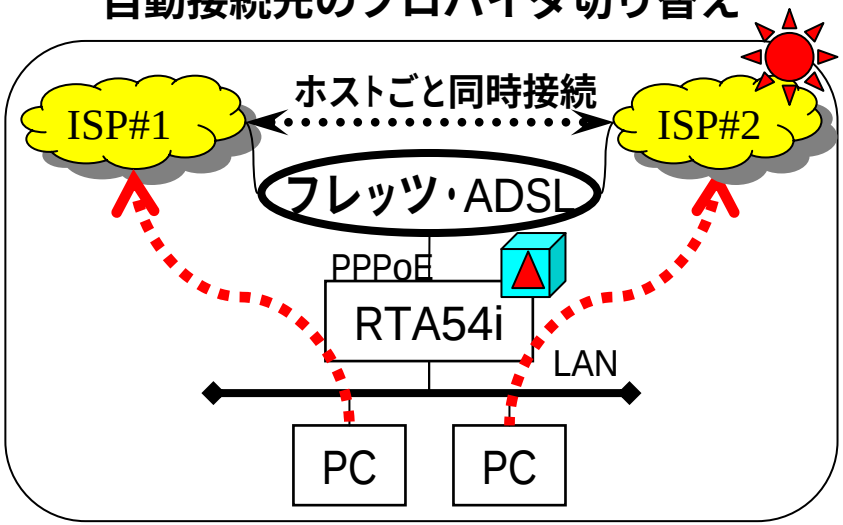
端末型プロバイダ接続(PPPoE)



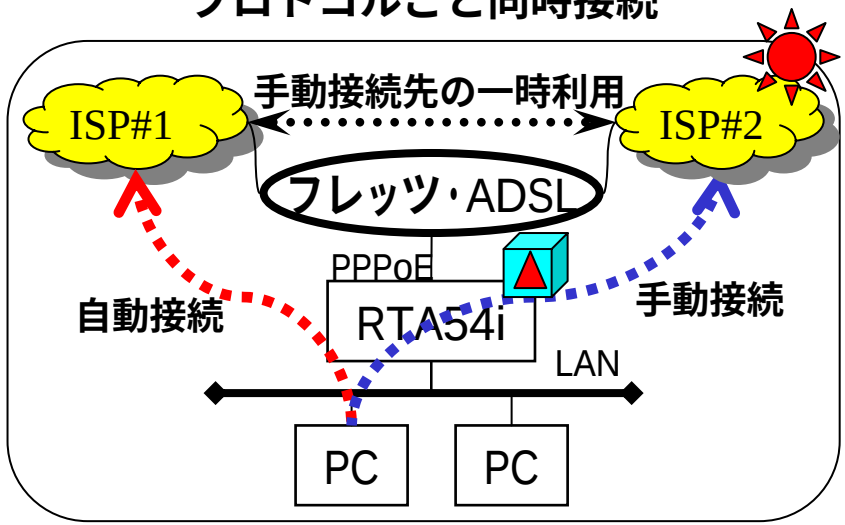
自動接続先のプロバイダ切り替え



プロトコルごと同時接続

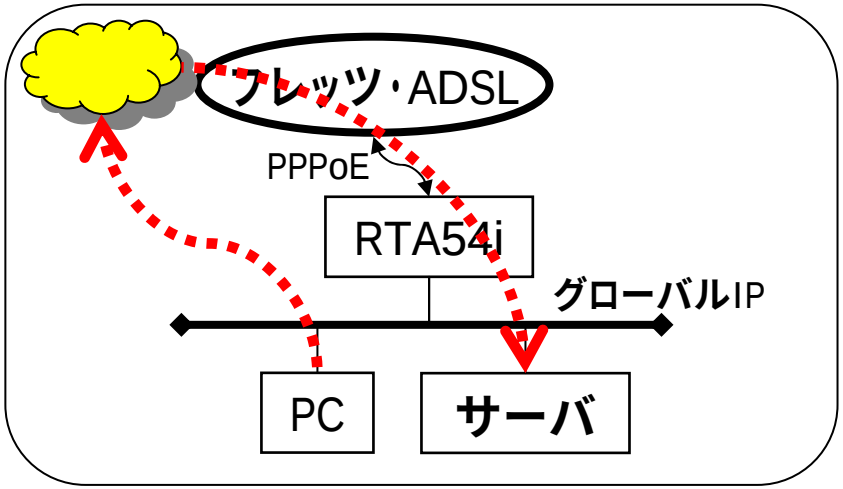


ホストごと同時接続

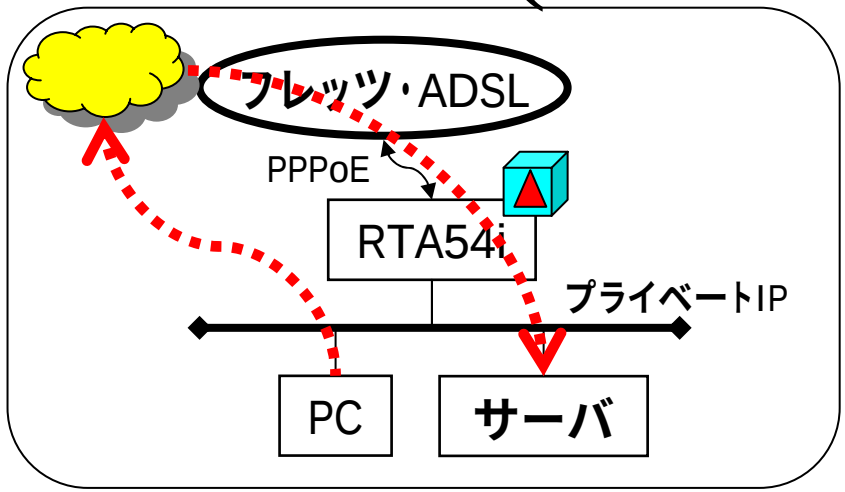


手動接続先の一時切り替え

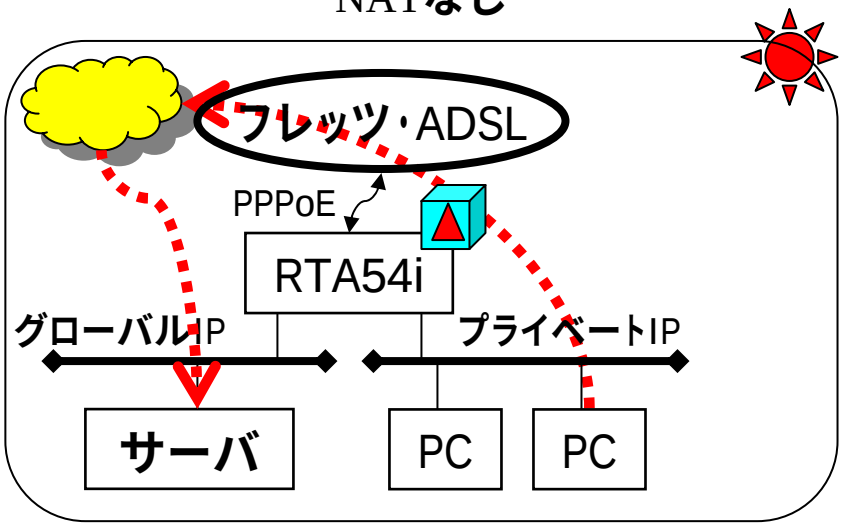
ネットワーク型プロバイダ接続(PPPoE)



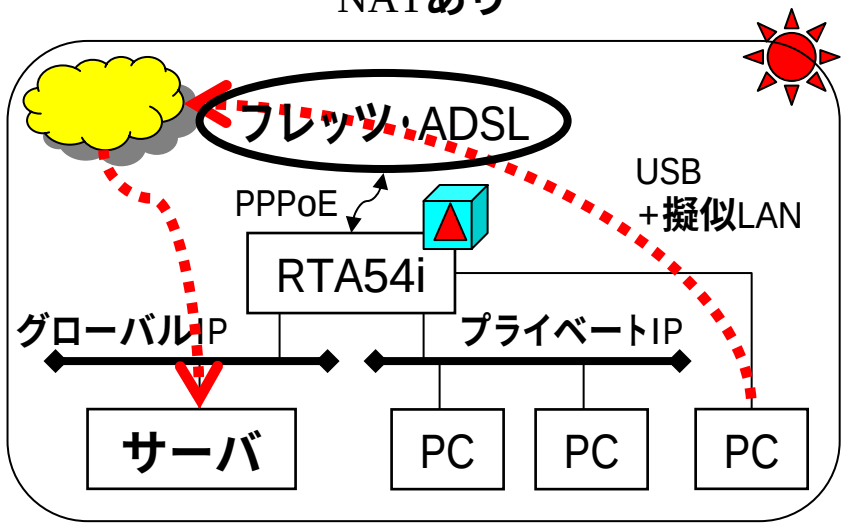
NATなし



NATあり

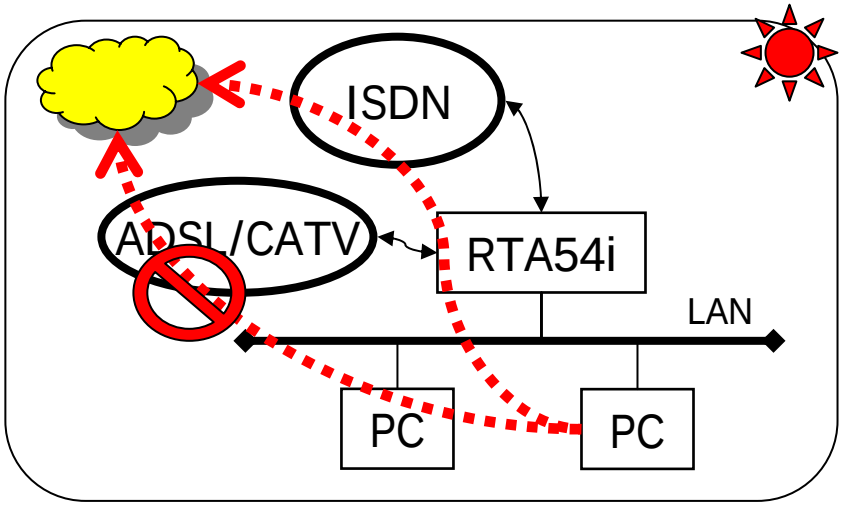


NATなし&あり(primary/secondary)

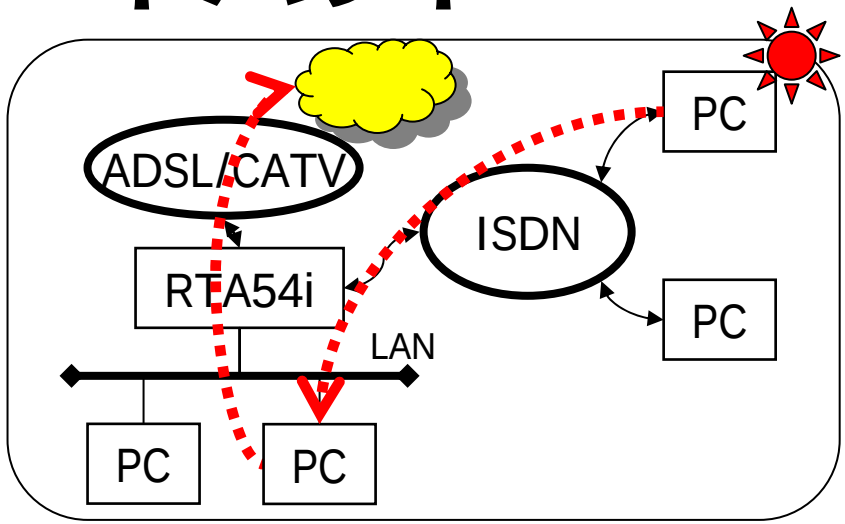


NATなし&あり(USB+擬似LAN)

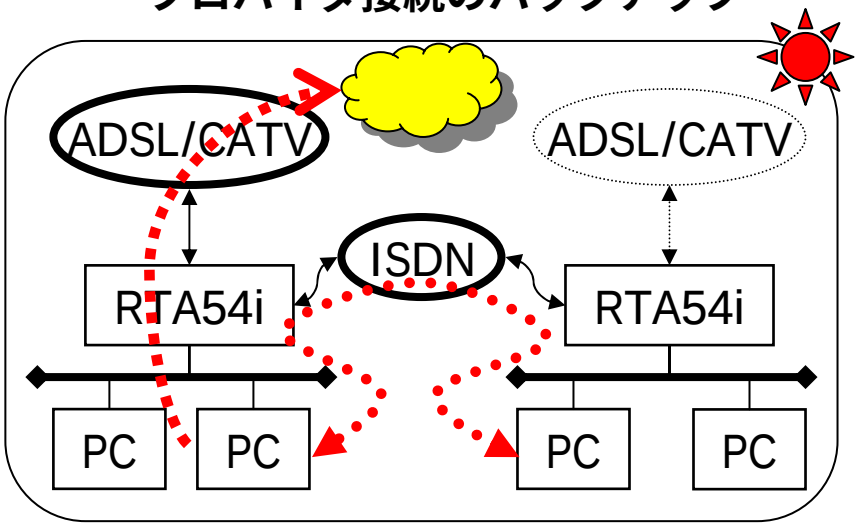
ISDN+ブロードバンド



プロバイダ接続のバックアップ

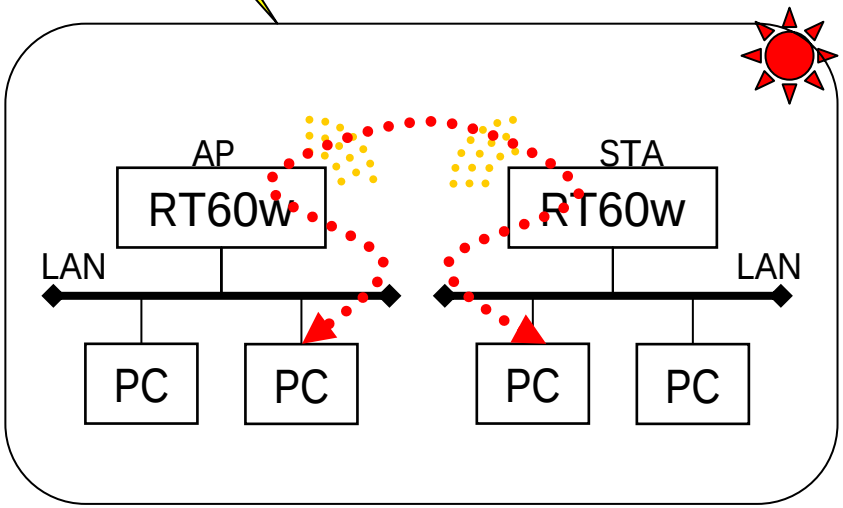


プロバイダ接続+リモートアクセスサーバ

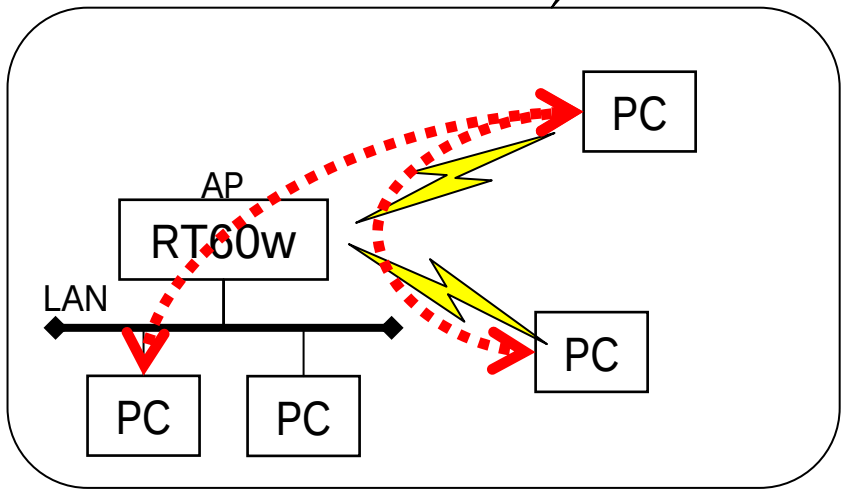


プロバイダ接続+LAN間接続

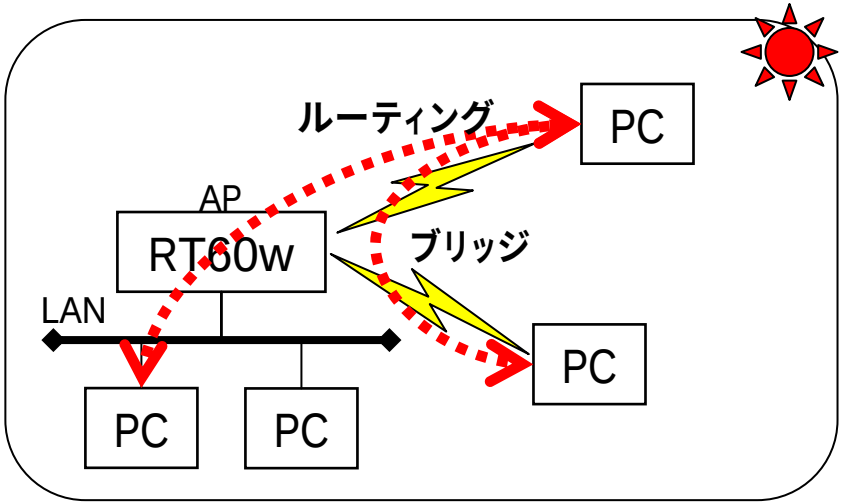
RT60wの無線LAN機能



無線ブリッジ機能(離れた有線LAN間を接続)

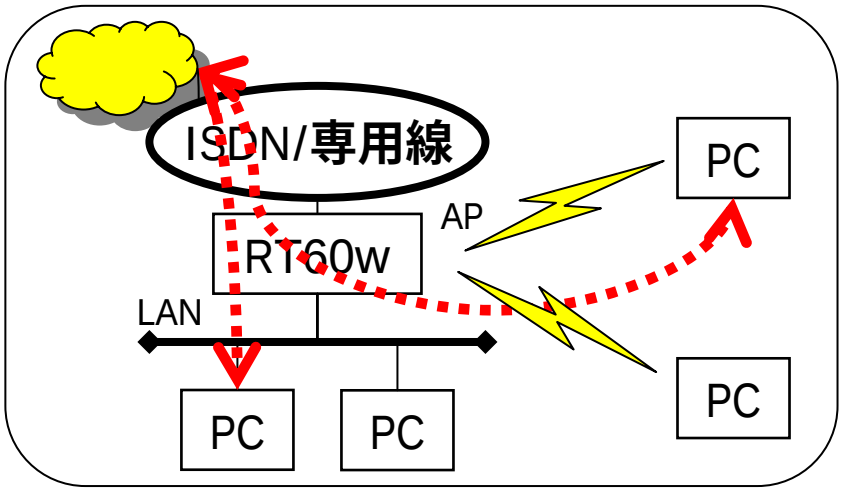


有線LANと無線LANのブリッジ機能

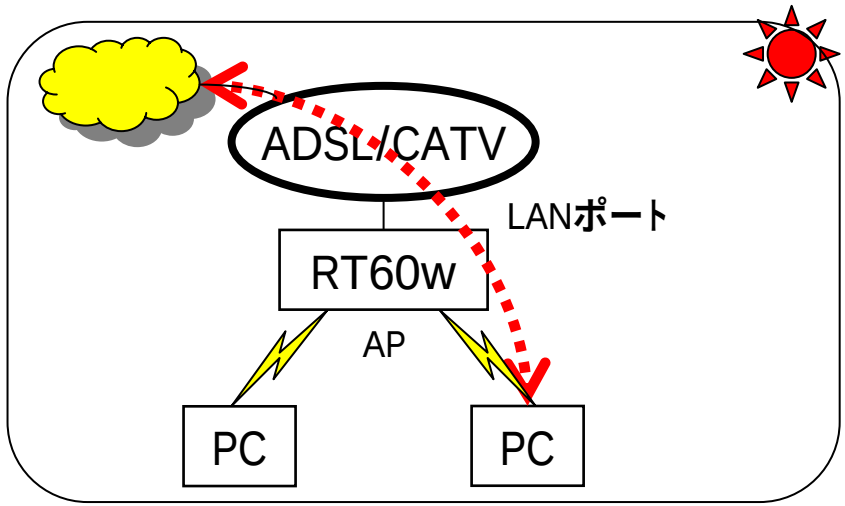


有線LANと無線LANのルーティング機能

RT60wの無線LAN機能の応用

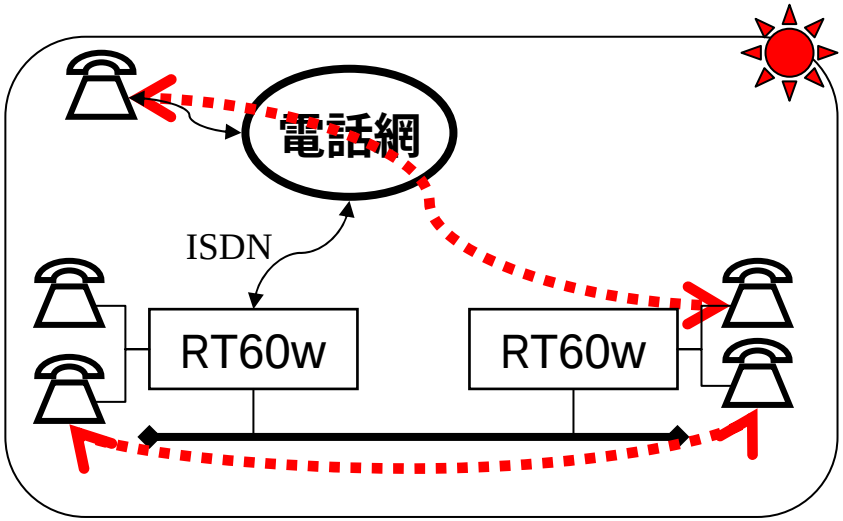


ISDN/専用線によるプロバイダ接続

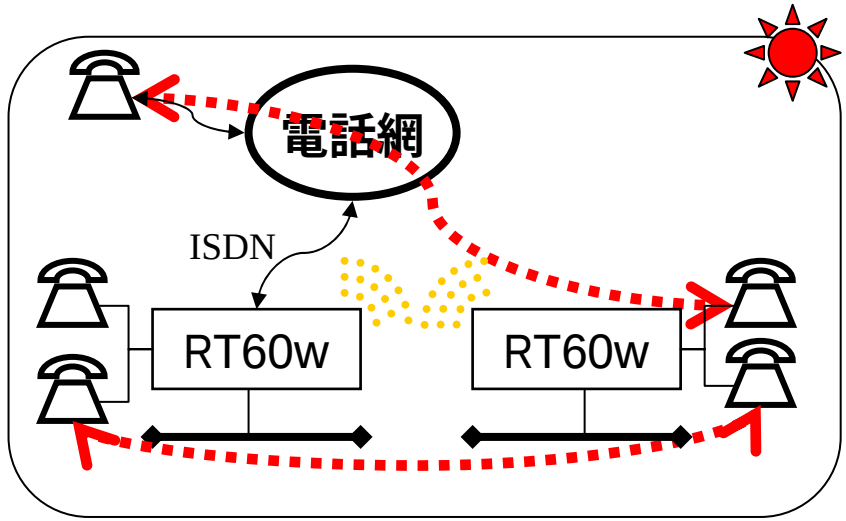


ADSL/CATVによるプロバイダ接続

かんたんPBX(機器間アナログ通話…MGCP)



かんたんPBX(有線LAN)

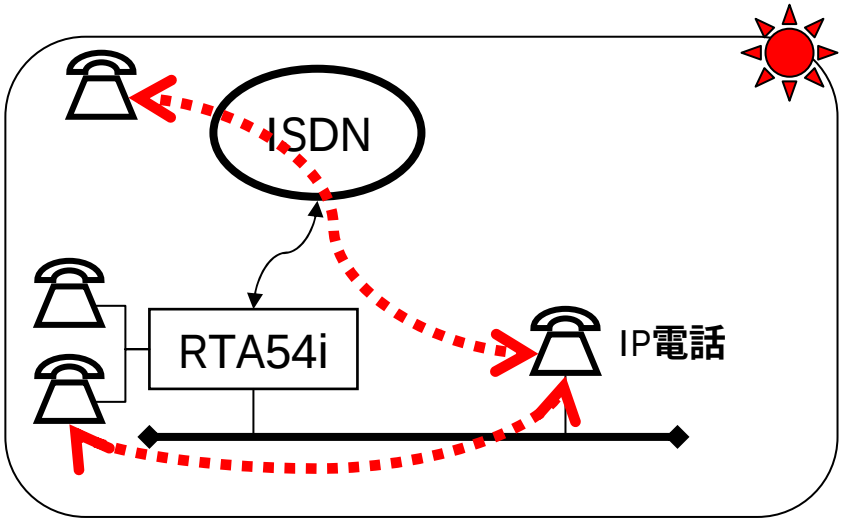


かんたんPBX(無線LAN)

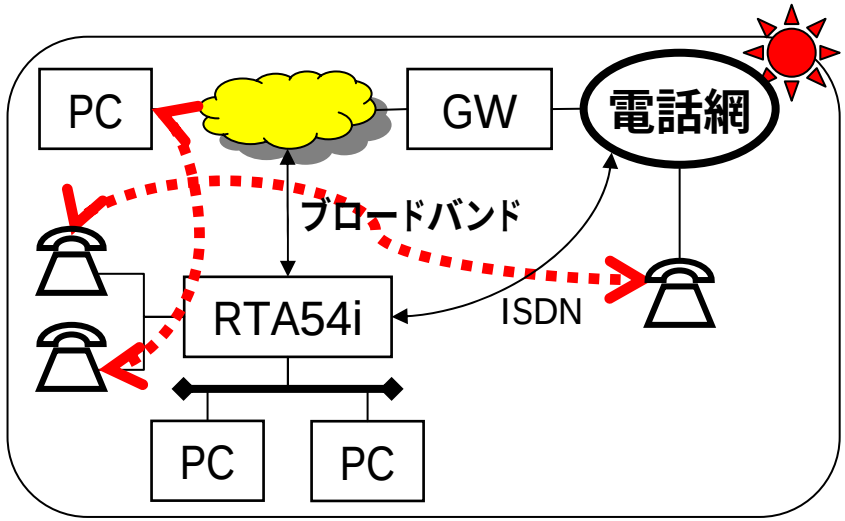
2000年12月「機器間アナログ通話機能(MGCP)」をRT60wに提供
2001年6月 Networld + Interop Tokyo 2001会場にて
　RTA54iを使用した「IPv6版MGCP」をデモンストレーション
2001年8月 IPv6対応版MGCPをRT60wに提供
2002年1月 RTA54iにてIPv4/IPv6版MGCPによるかんたんPBX機能の
　β版ファームウェアの提供開始予定

・MGCP:Media Gateway Control Protocol、RFC2705

VoIP機能の可能性



ISDNへのVoIPゲートウェイ機能(SIP)

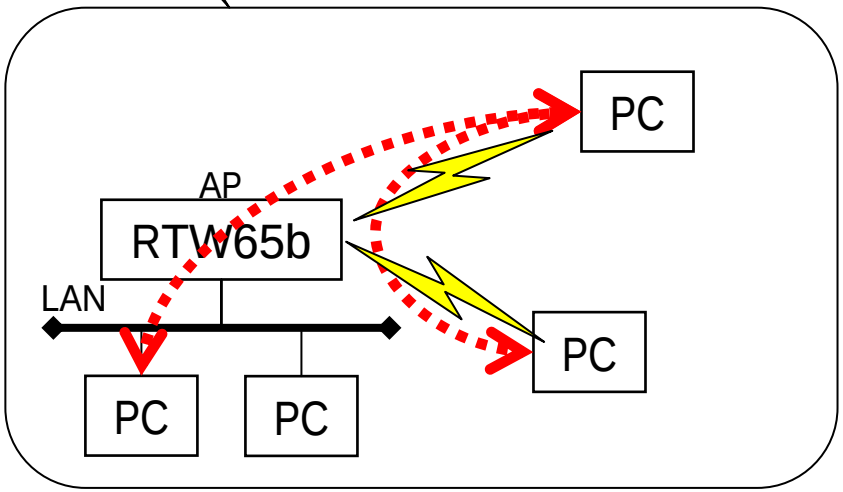


IP電話(MGCP,SIP)

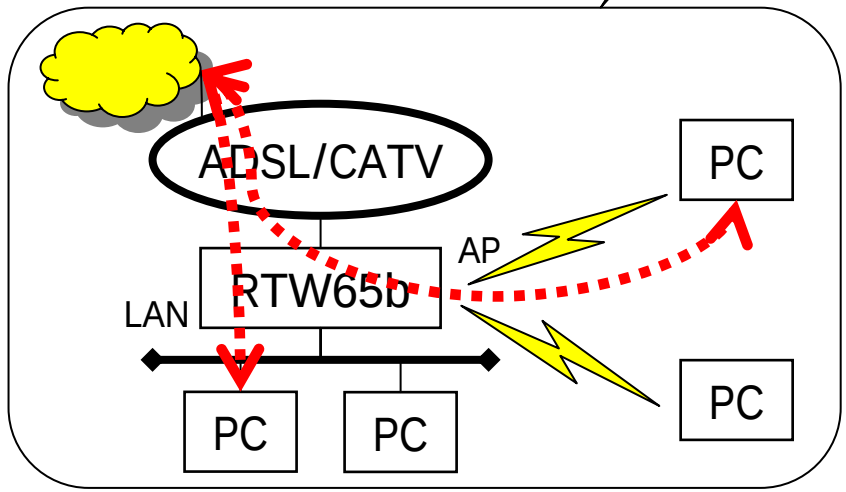
2000年12月「機器間アナログ通話機能(MGCP)」をRT60wに提供
2001年6月 Networld + Interop Tokyo 2001会場にて
RTA54iを使用した「IPv6版MGCP」をデモンストレーション
2001年12月 RTA54i/RT60wにてIPv4/IPv6版SIPによるVoIP機能の
β版ファームウェアの提供開始予定

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

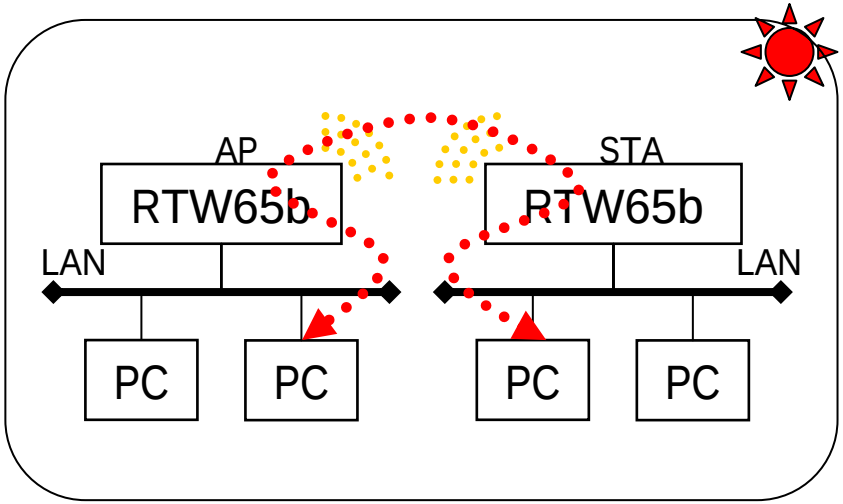
RTW65bの無線LAN機能



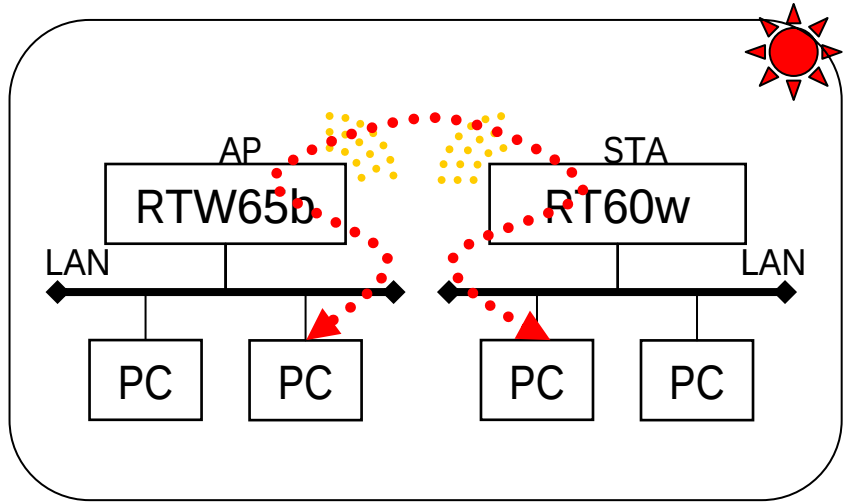
有線LANと無線LANのブリッジ機能



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)

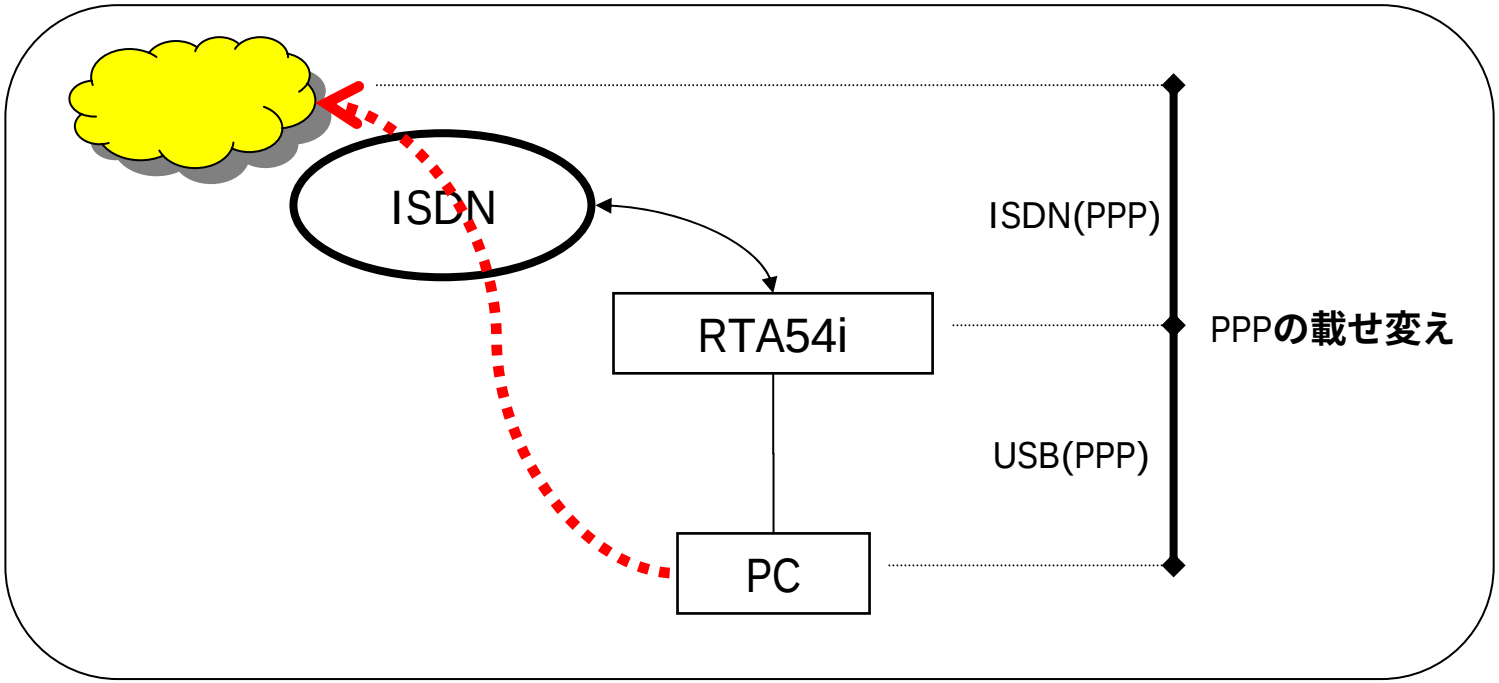


RT60wとの相互接続

ネットボランチのネットアプリ対応

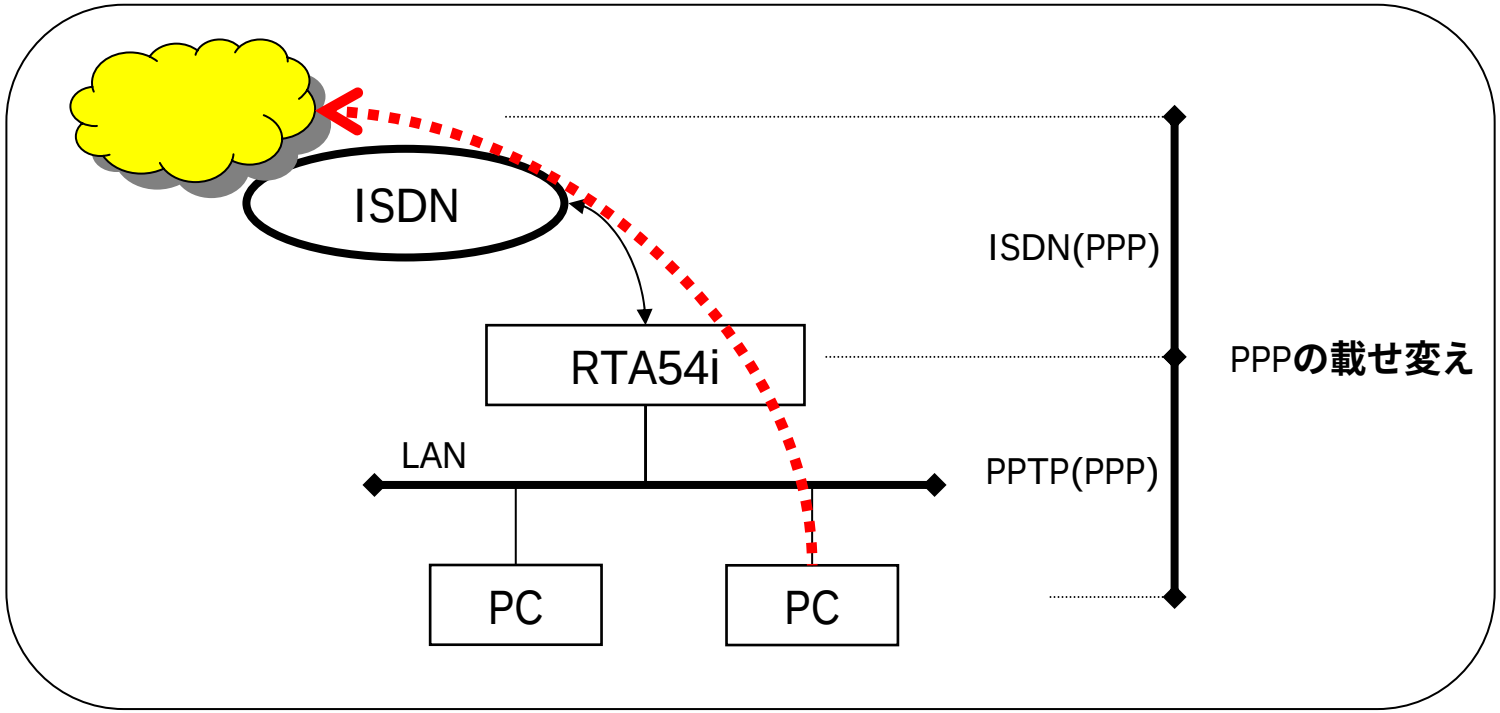
1) ISDN-TA(RTA54i)
2) LAN-TA機能(RTA54i)
3) ブロードバンドTA(RTA54i/RTW65b)
4) IPマスカレード対応
   - 静的IPマスカレード
   - IPマスカレードの例外処理(パケット書き換えなど)
     FTP,CU-SeeMe,NetMeeting Version 3.0
5) DMZホスト機能(IPマスカレードのimcoming処理選択)

ISDN-TA(データ通信)



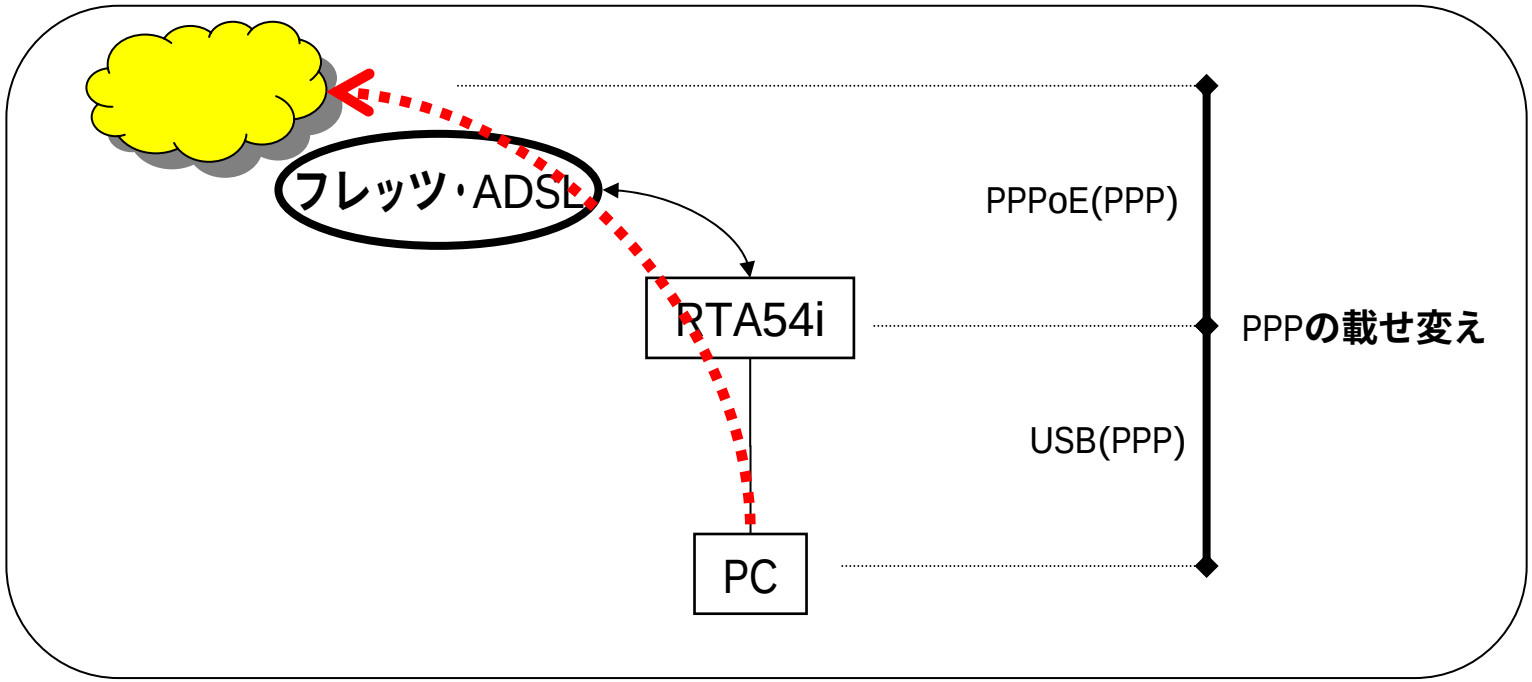
モデムと同等のPPP接続(PPP Adapterおよびダイヤルアップネットワーク)が可能となる機能

LAN-TA機能



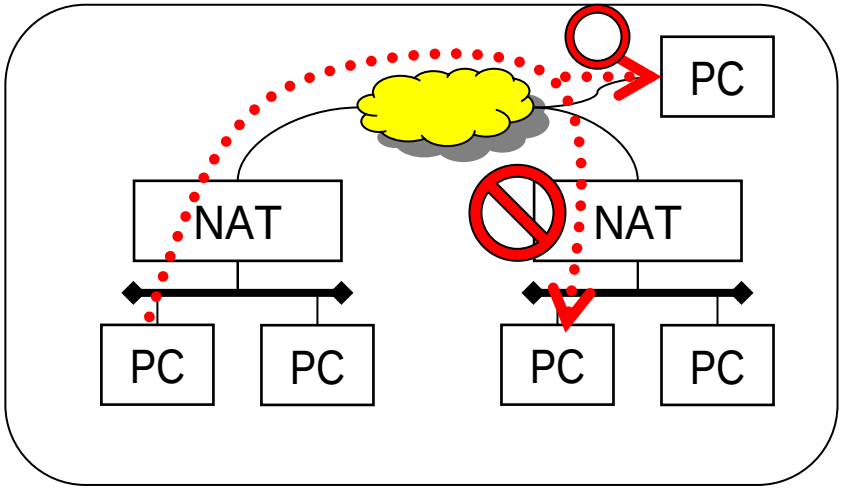
Microsoft社のWindows95やWindows98などの「Microsoft (R) VPN Adapter/マイクロソフト(R)仮想プライベートネットワーク」という機能を利用して、LAN上の端末(Windows)からISDN-TAやモデムなどと同等のPPP接続(PPP Adapter およびダイヤルアップネットワーク)が可能となる機能

ブロードバンドTA

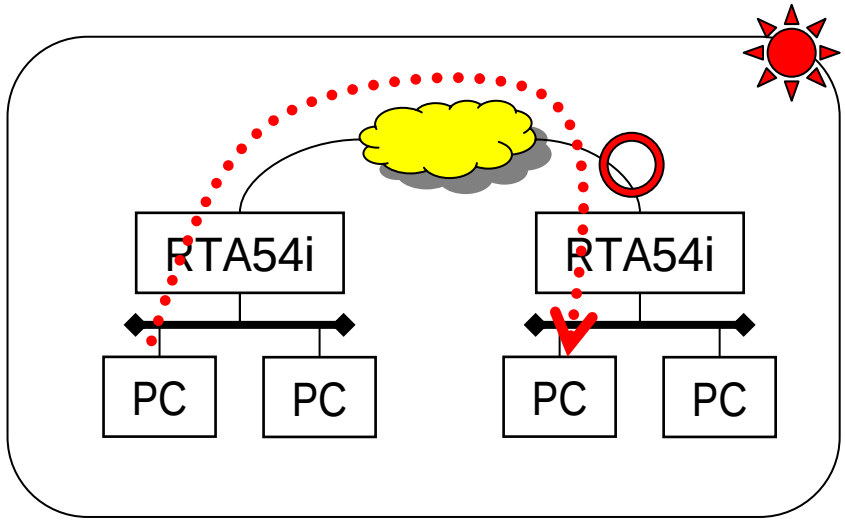


フレッツ・ADSLやBフレッツなどで利用されるPPPoEをISDN-TAやモデムなどと同等のPPP接続(PPP Adapterおよびダイヤルアップネットワーク)が可能となる機能

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ホスト機能のみによる対応では、通信相手に制限がある。
  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。

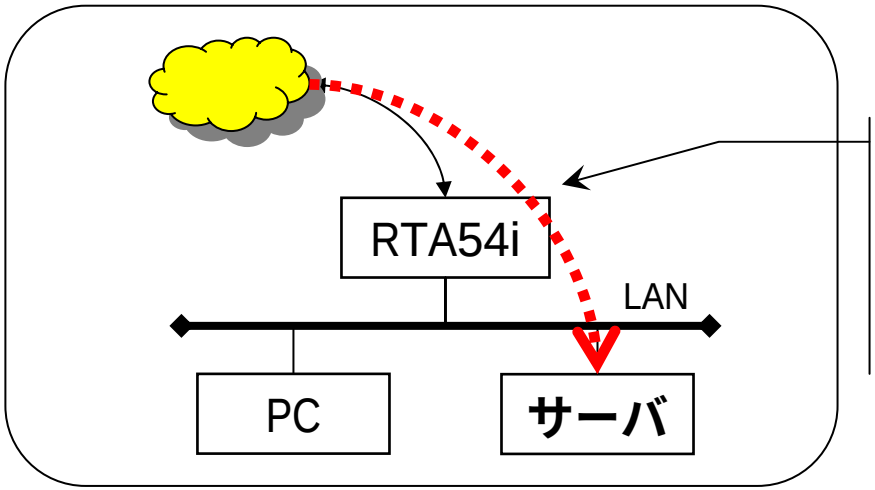
- NetMeeting Version 3.0
- ビデオ、音声、チャット、ホワイトボードの動作を確認済み
- ディレクトリサービスに対応しない
- 複数の端末がNATの外側へ同時に接続することはできない
- NATの外側から内側の端末へ接続するためには、下記のような静的 IPマスカレードの設定が必要

(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
```


RTA54i Rev.4.04.06β リリースノートより

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ホスト機能のコマンド仕様

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

スループット

- スループット測定方法
- スループット値

スループット測定方法

a) RFC1944/RFC2544に準拠した測定(SmartBitsなどの測定器)
　企業向けルータの標準的測定方法
　a-1) パケット処理能力 (PPS = Packets Per Second)
　　1秒間に64バイト長のパケットを通せる数
　a-2) 最大スループット
　　パケットサイズを変化させてもっとも転送レートの高い数値を
　　「パケット処理能力(PPS)*パケットサイズ→最大スループット」
　　という場合が多いだろう。

b) ユーザの利用環境に近い測定方法
　b-1) ローカルルータとして設定/動作させたときのftpの転送速度 (最大速度)
　　「ローカルルータ動作」
　　→フィルタリングやNAT/IPマスカレードは利用しない。
　b-2) CATV接続用ルータとして設定/動作させたときのftpの転送速度 (実効速度)
　　「CATV接続型セキュリティレベル4」
　　→セキュリティフィルタとIPマスカレードを使用する。

RFC1944のテスト項目:Throughput, Latency, Frame loss rate, Back-to-back

スループット値

機種	リビジョン	最大	実効
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

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)

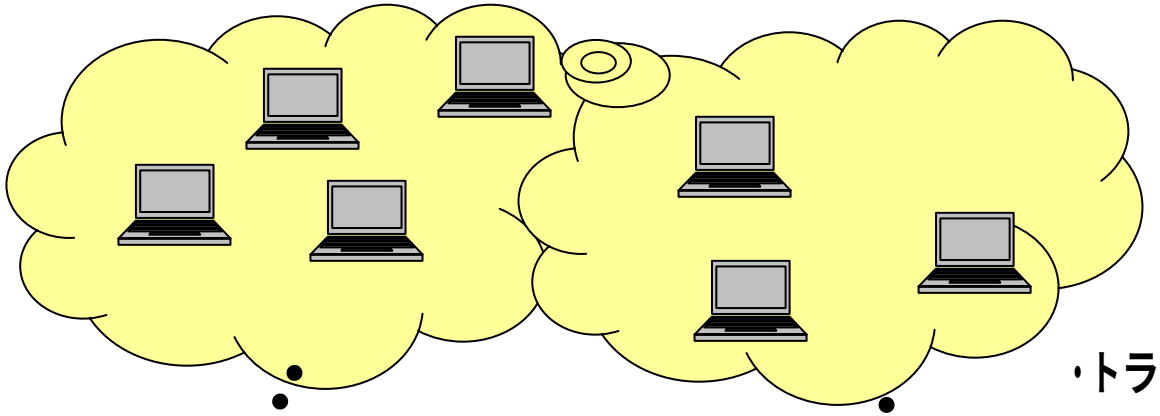
実効: アドレス変換あり、フィルタ設定あり(CATV型セキュリティレベル4)

※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。

ヤマハルータ
の
いろいろな使い方
「RTシリーズ」

ネットワーク分割



ルータによるネットワーク分割

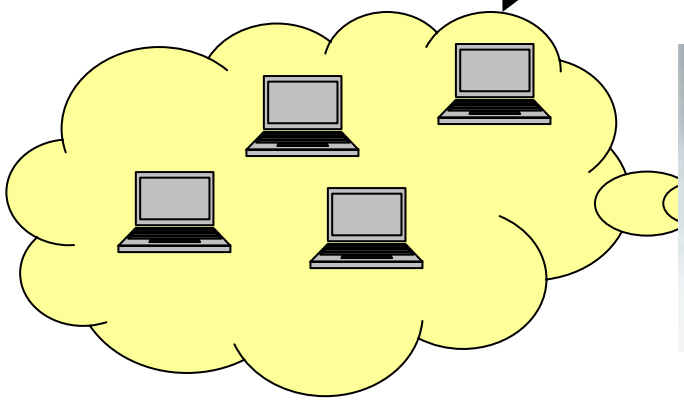
・トラフィック軽減

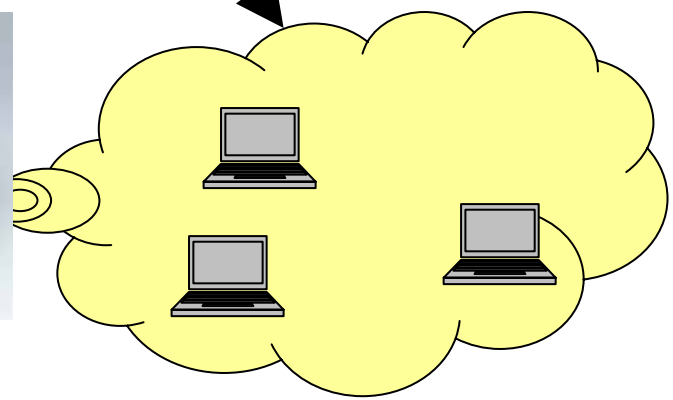
・セキュリティ向上

・組織/グループ分け

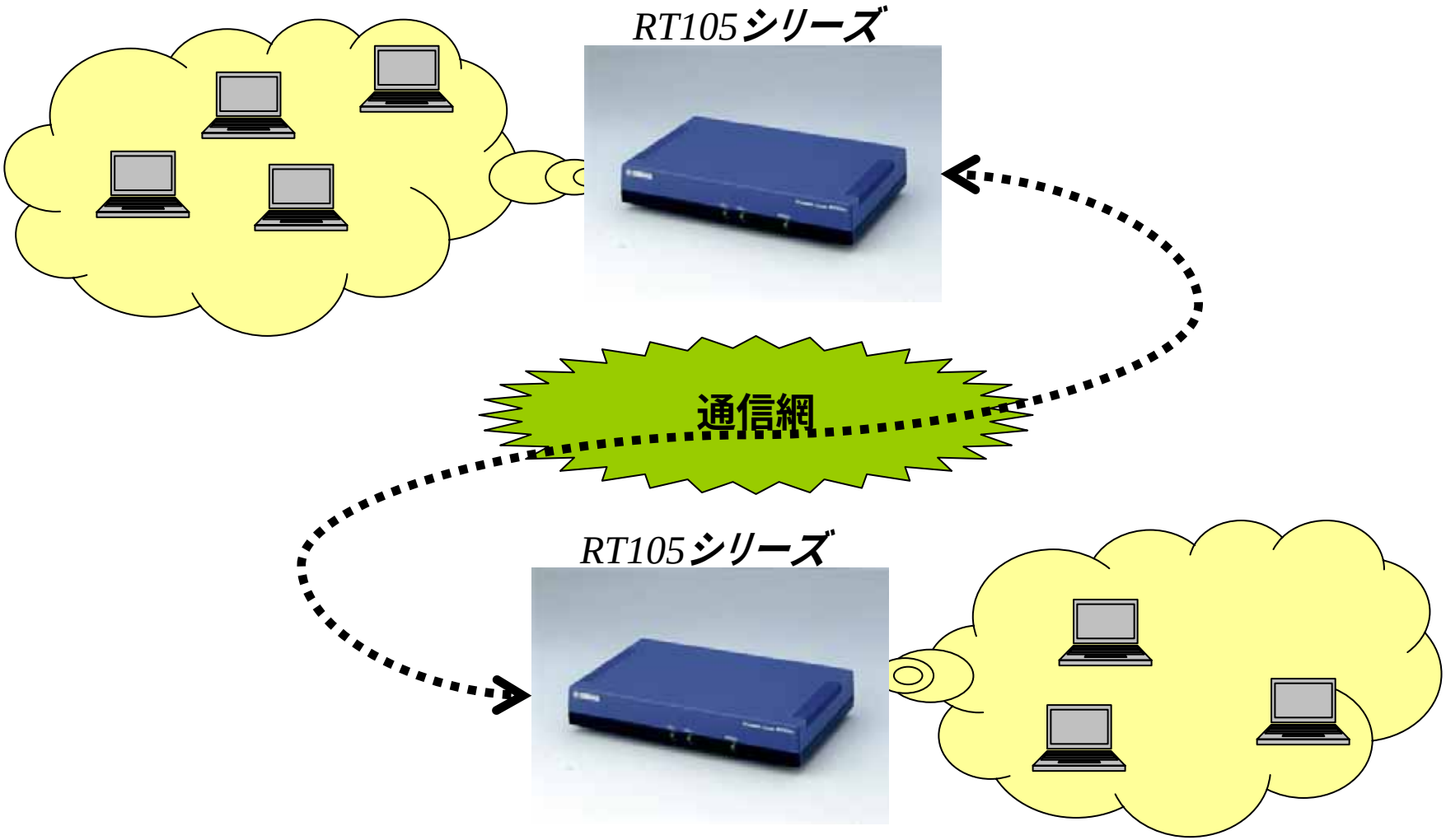
RT105e

(ローカル・ルータ)



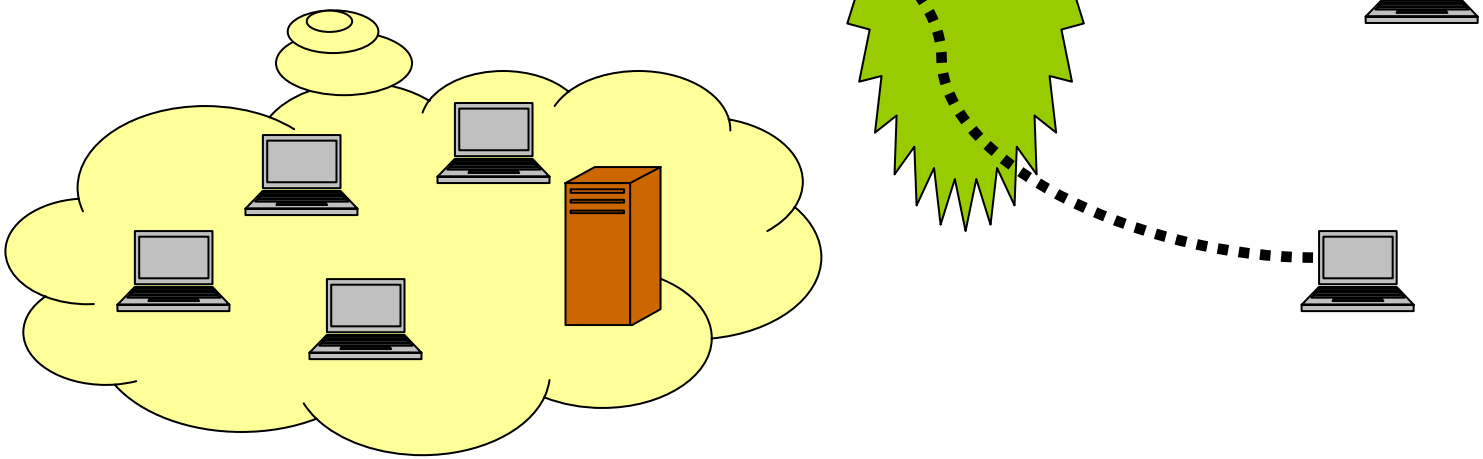


遠隔地とのLAN間接続

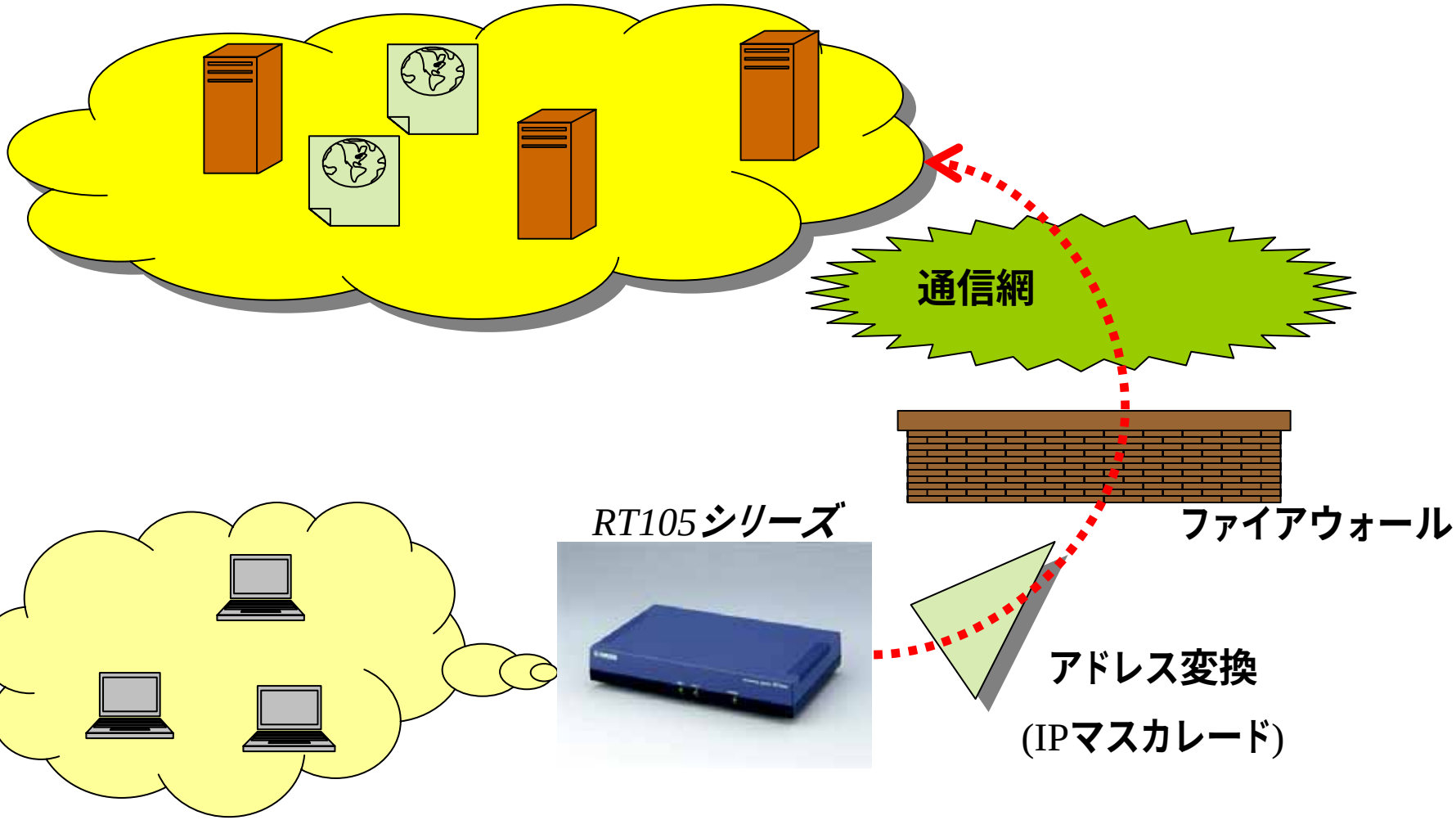


ダイヤルアップサーバ

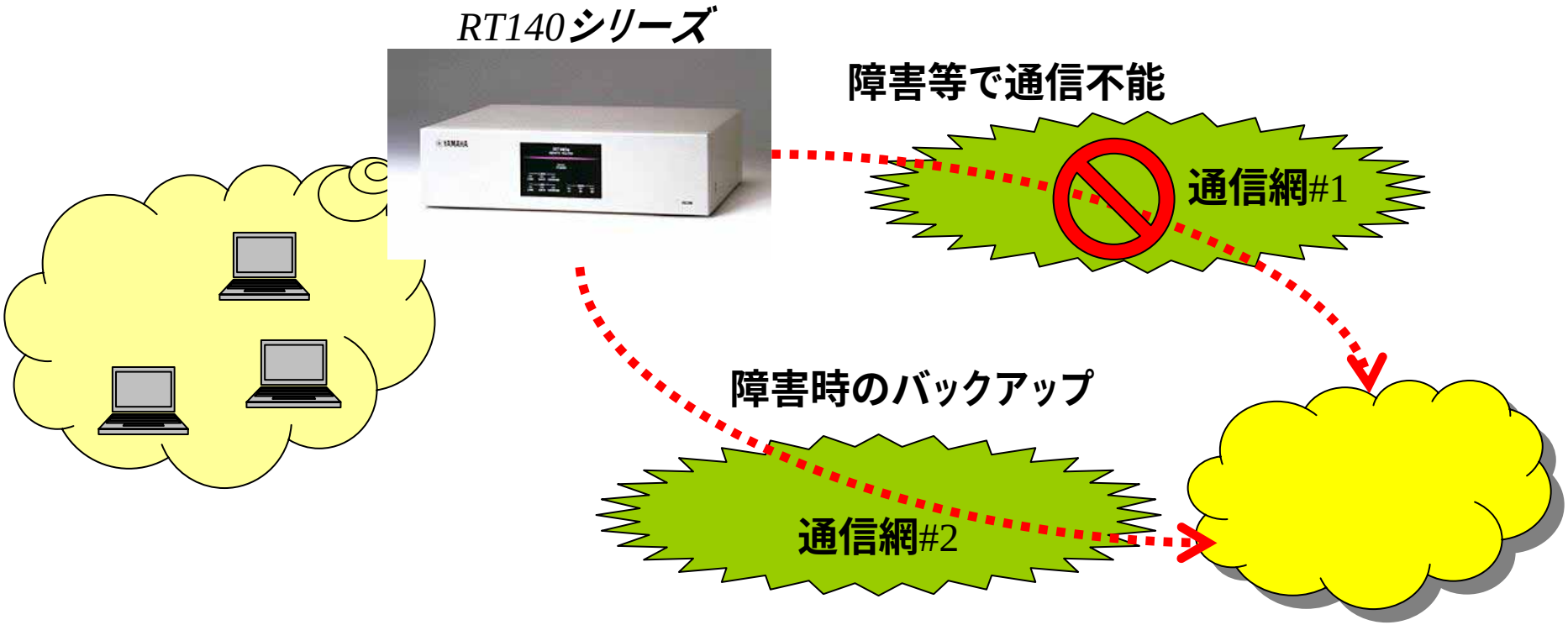
*RT300i + **オプションモジュール***



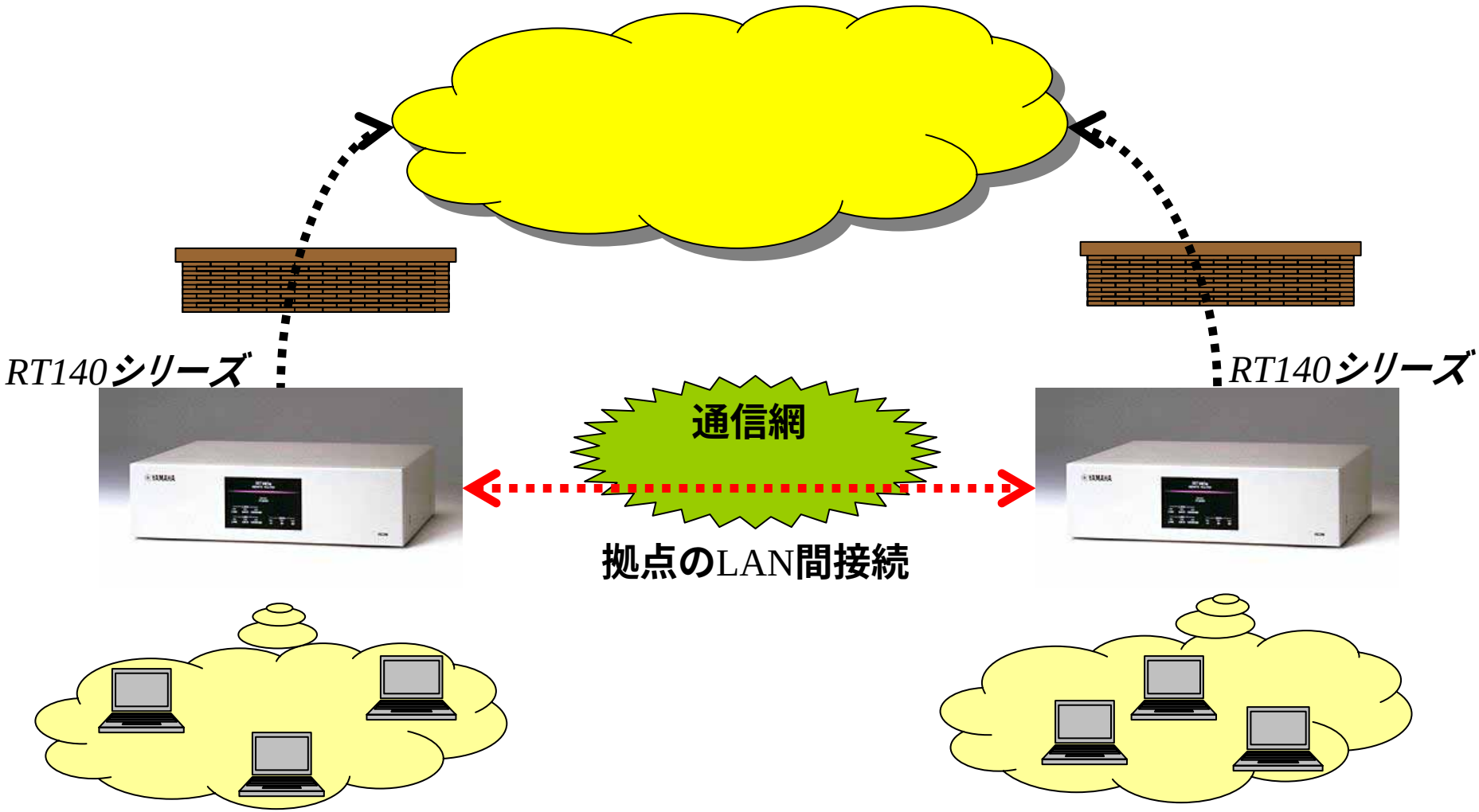
プロバイダ接続



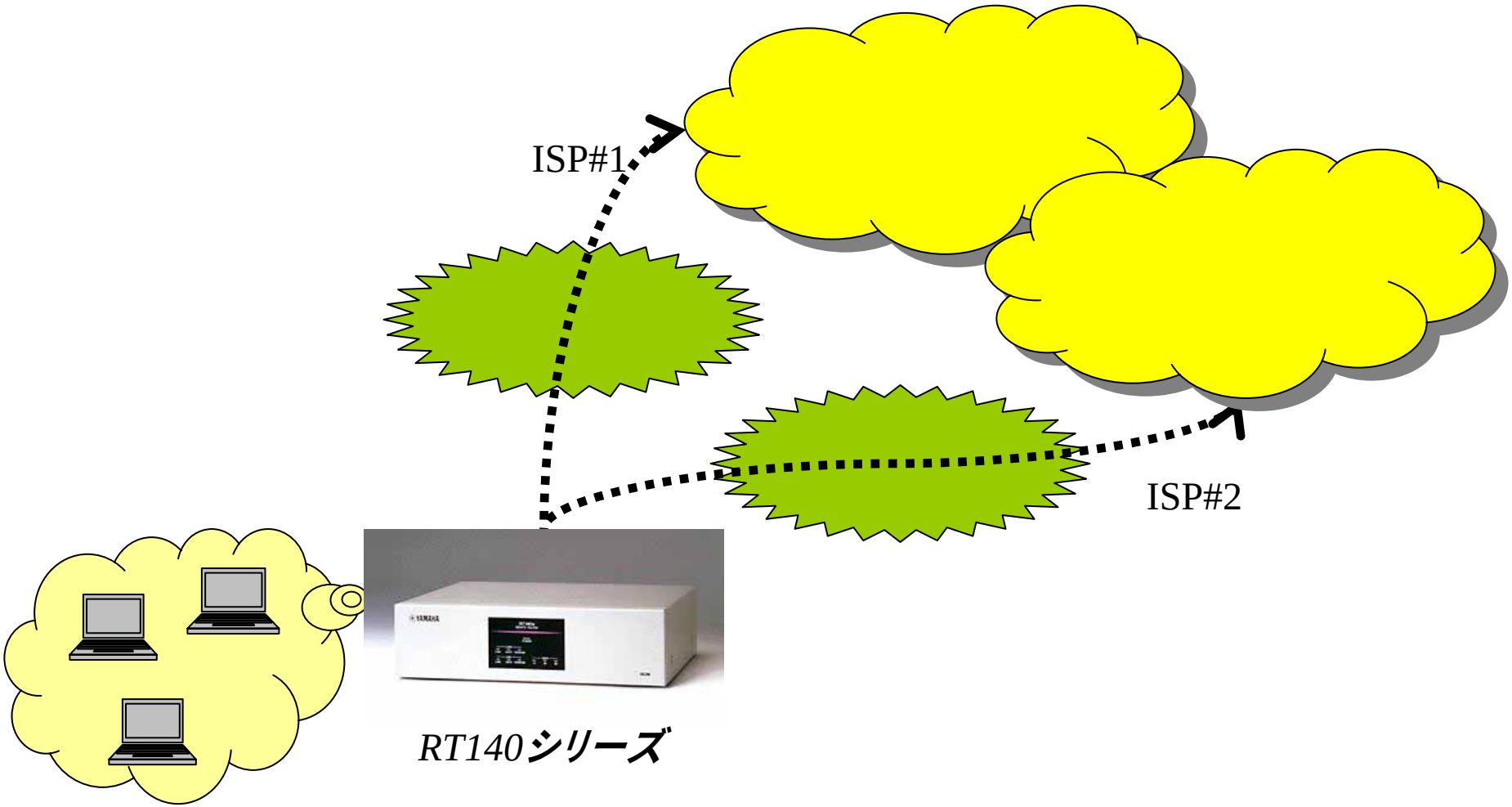
プロバイダ接続のバックアップ



プロバイダ接続+LAN間接続

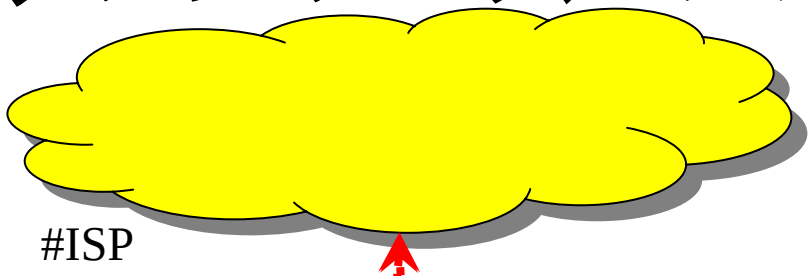


マルチホーミング

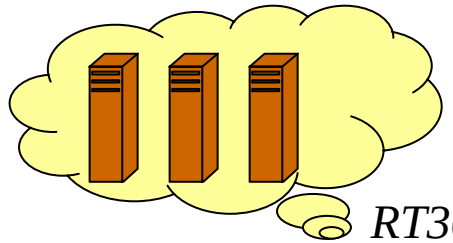


RT140シリーズ

フレッツシリーズ+フレッツオフィス



#ISP



RT300i

フレッツ・ISDN
フレッツ・ADSL

フレッツ網

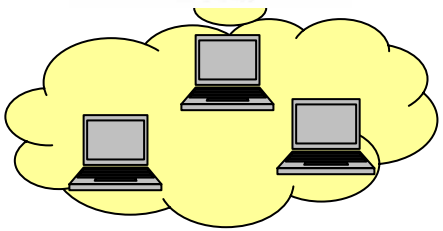
フレッツ・オフィス

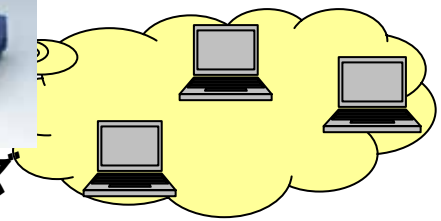
・接続先切り替え
・同時接続

フレッツ・ADSL
Bフレッツ

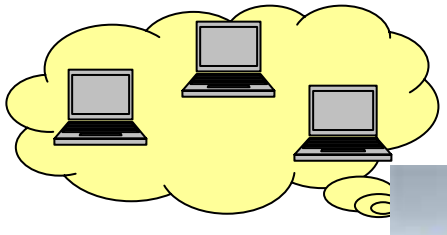
RTA54i

RT105シリーズ





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

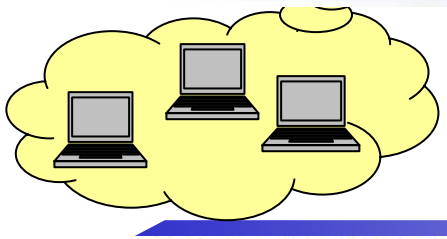
RT105シリーズ

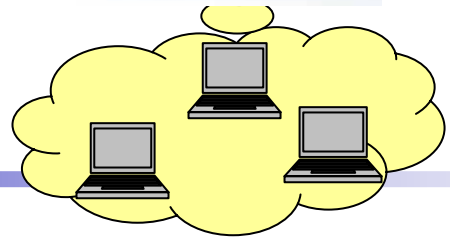
IP-VPN網

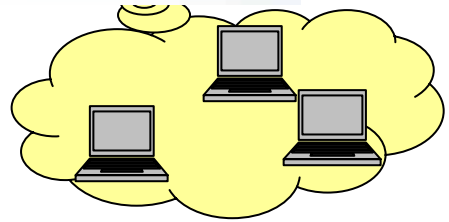
RT105シリーズ

RT105シリーズ

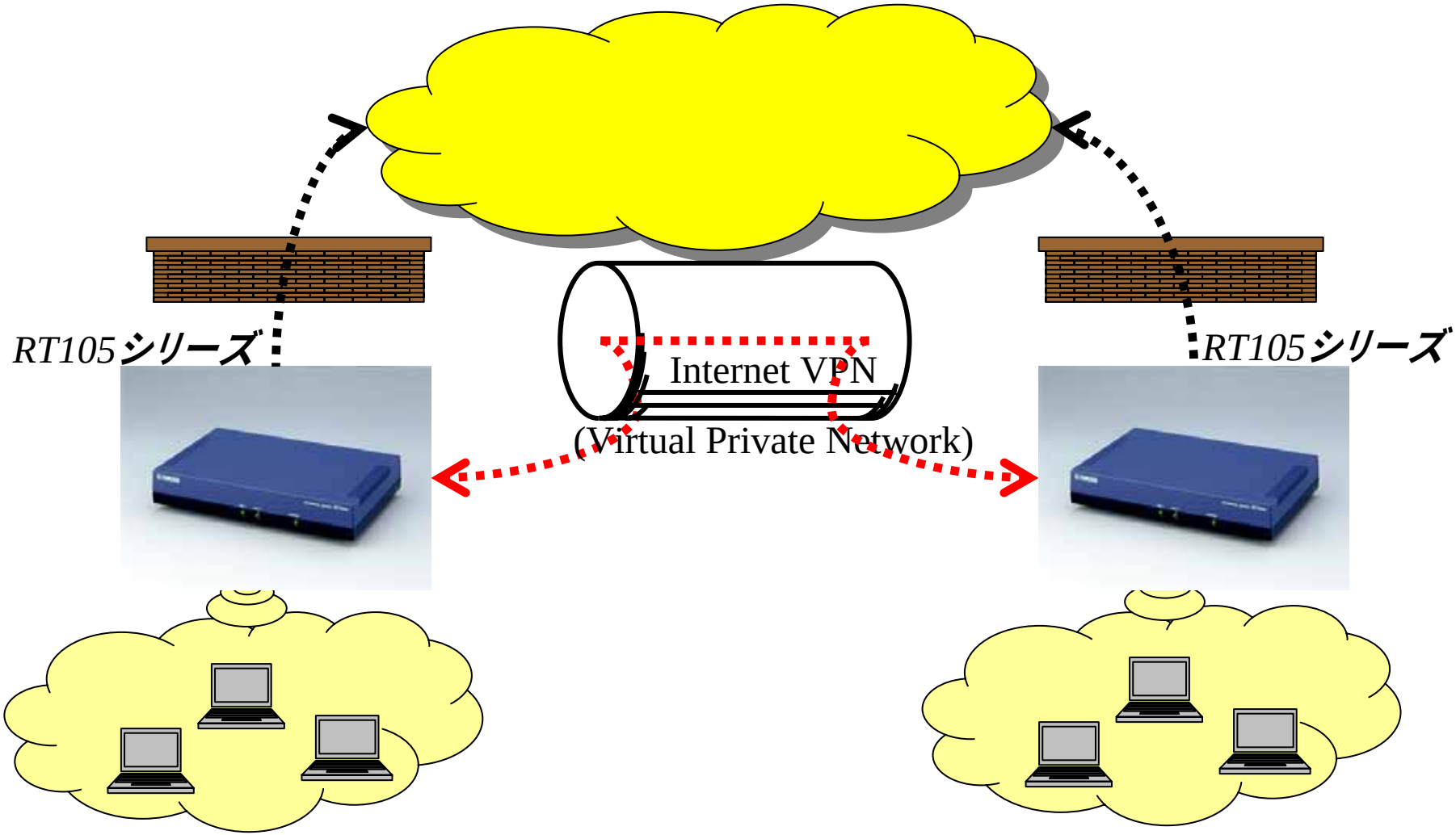
RT105シリーズ







プロバイダ接続+Internet VPN



Internet VPNのISDNバックアップ