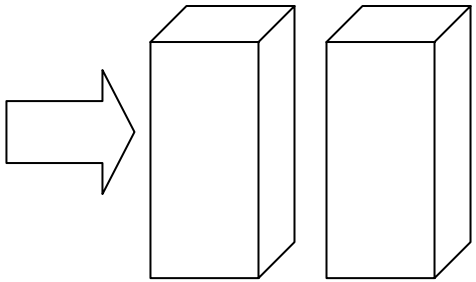
YAMAHA

感 動 を ・ と も に ・ 創 る

ヤマハ ネットボランチ
RTA55i & RT56v
～導入資料～

RTA54i



RTA55i　RT56v

ヤマハ株式会社
AV･IT事業本部
マーケティング室

2002年9月

目次

1) 市場動向
2) RTA55i&RT56v製品概要
3) インターネット電話機能
4) VPN機能

[付録資料]
・ヤマハルータについて
・ブロードバンドへの取り組み
　ブロードバンド、Internet VPN、インターネット電話(VoIP)
・ネットボランチRTA55iの機能や使い方
・ネットボランチの機能や使い方(無線LAN編)
・RTシリーズの機能や使い方
・機能解説
　構造、NATディスクリプタ、ファイアウォール、フィルタ型ルーティング

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)

「個人/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

↓

次に求められるものは、ネットワークを活用するアプリケーション

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]

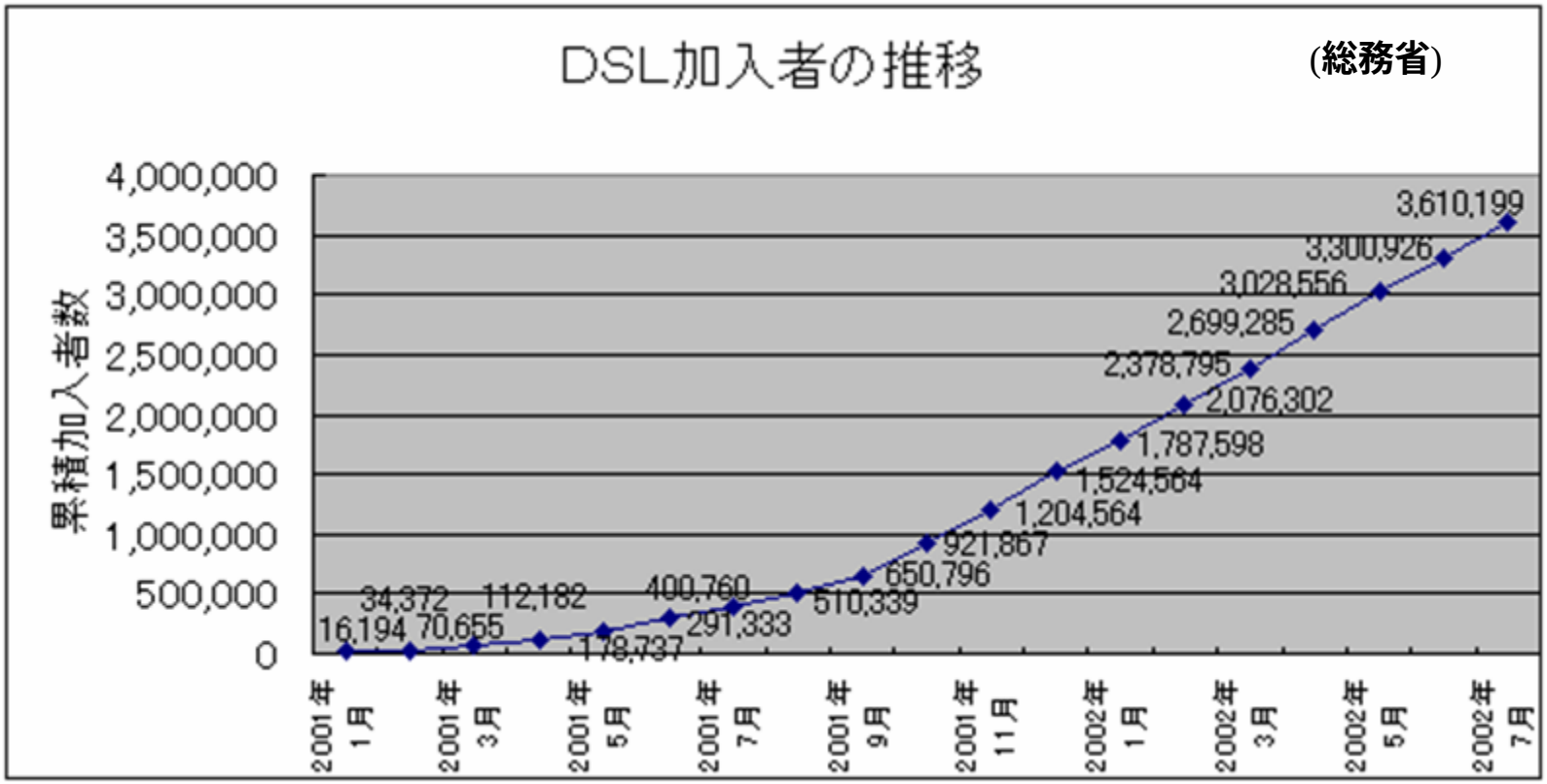
- 初期状態での高いセキュリティ性 (安全性)
- 品質: 安定性/信頼性/耐久性/環境対応性
- ブロードバンド時代の新しいアプリケーション対応

「使い易さの向上」

マニュアル/WWW設定機能の強化

豊富なドキュメントと手厚いサポート

ブロードバンド回線動向

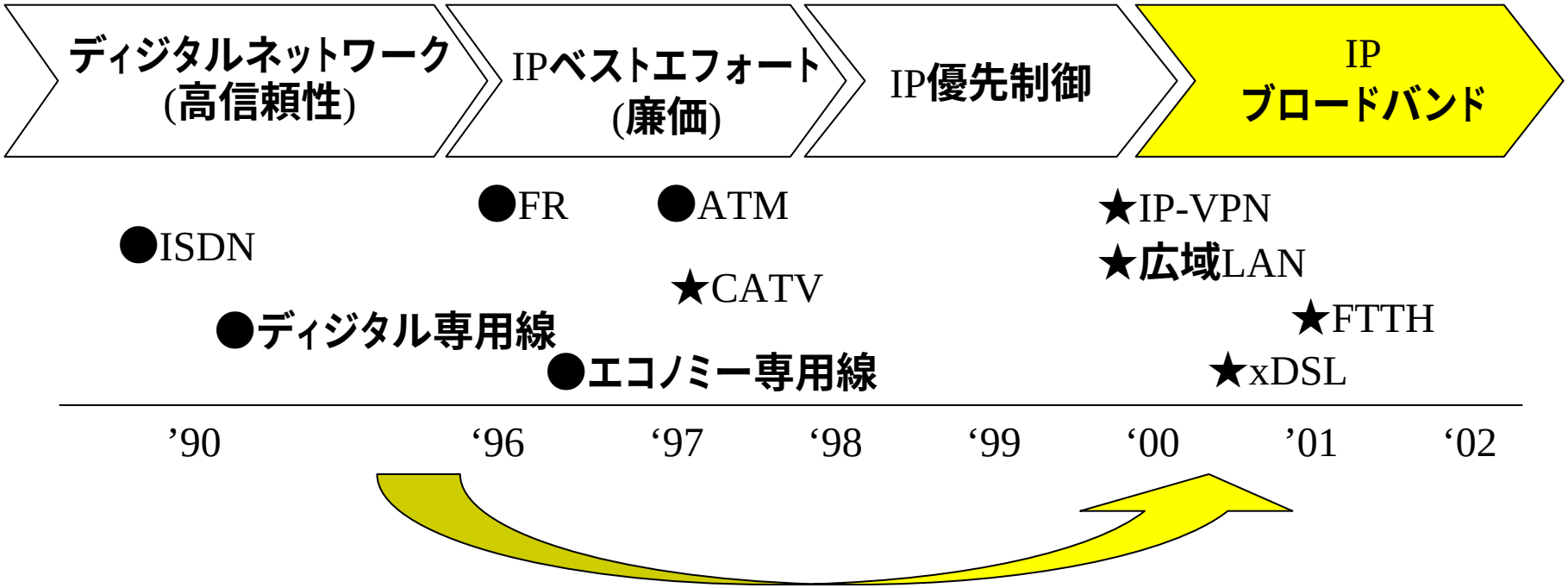


- 2002年7月末まで：DSLが約361万契約 (約30万/月ペース)
- 総務省による2002年度末の予測：1200万世帯 (出所:電波新聞)
  DSL:562万世帯、CATV:231万世帯、FTTH:404万世帯

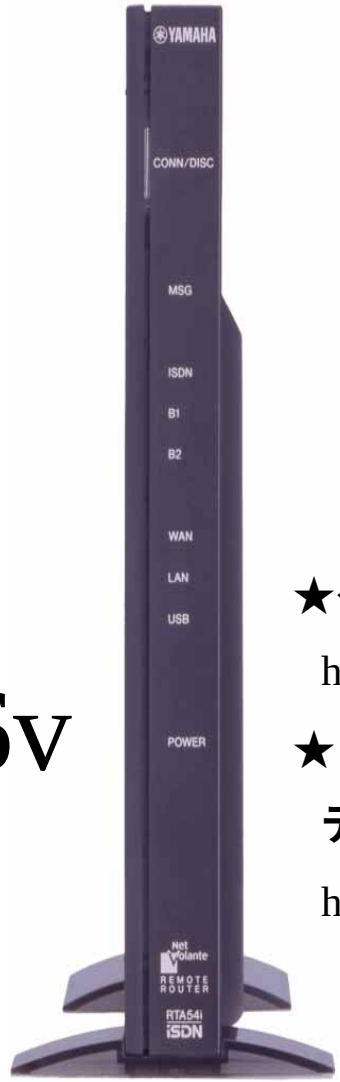
ブロードバンド回線増加の分岐点

時期	動向
2001/1〜	NTT：**フレッツ**・ADSL(**最大**1.5M)
2001/6〜	Yahoo!BB：**低価格**ADSL(**最大**8M)
2001/9〜	**各社**：ADSL(**最大**8M)
2002/1〜	NTT：**フレッツ**・ADSL(**最大**8M)
2002/**春〜**	**ブロードバンド時代の本格サービス到来** ・**インターネット電話**(VoIP)…ブロードバンドコミュニケーション ・**ネットワーク・エンターテイメント**…ゲーム、映画など ・IPv6**の一般向けサービスのはじまり**

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



RTA55i & RT56v
製品概要

(オープンプライス)

RTA54i

★グッドデザイン賞受賞

http://www.g-mark.org/

★日本インダストリアルデザイナー協会
デザインミュージアム 選考

http://www.jida.or.jp/jida/

RTA54iの評価

[+]評価	[-]評価
[+] モノリスをモチーフにしたデザイン ・グッドデザイン賞受賞 ・JIDA デザインミュージアムに選考 [+] 全国どこでもで使える守備範囲 (ISDNを含む多様なアクセス回線に対応) [+] かんたん設定ページ ISDNも活用した豊富な設定機能 多機能・多用途が統一操作でカンタン [+] デフォルトのセキュリティ・コンセプト [+] ファイアウォール機能 静的フィルタリング、動的フィルタリング、 不正アクセス検知、セキュリティレベル [+] 低価格帯でIPv6世界初搭載 IPv4/IPv6デュアルスタック [+] ビジネス用途に十分耐える安定性 [+] 機能のトータルバランス	[-] でかいACアダプタ [-] 高くて使えないISDN [-] 特定アプリケーション対応 ・DMZホスト機能 (だって、セキュリティホールが心配) ・NetMeeting 3.0対応 ・L.モード対応 ・VPN対応 [-] 高速対応 ・LAN側100BASE-TX対応 ・スループット (最大 6.0Mbps)

RTA55i & RT56vの製品コンセプト

「VoIPルーター」

ブロードバンド時代の新しい「コミュニケーション・ツール」

1) インターネット電話機能

ISDNルーターで培ったアナログ&VoIP技術

ネットボランチDNSサービスの電話アドレスサービス

2) セキュリティ機能

2-a) VPN(PPTP+RC4)機能

LAN間接続VPN、Windowsからのリモートアクセス VPN

ネットボランチDNSサービスのホストアドレスサービス

2-b) 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(ログ、ブザー、メール)

RTA55iとRT56vの特長

・ブロードバンド時代の新機能

a) ネットボランチDNSサービス (ホストアドレスサービス、電話アドレスサービス)
b) インターネット電話(VoIP)機能
c) PPTPによるVPN機能 (LAN間接続VPN、Windowsからのリモートアクセス VPN、RC4搭載)
d) アプリケーション対応 (DMZホスト機能、NetMeeting 3.0対応など)
e) WWWブラウザからのIPv6接続設定

・RTA54iを継承、さらに、使い易さの追求

a) 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)
　セキュリティレベルによるかんたんに高度なセキュリティ確保ができる。
b) 複雑になりがちな、3つのインターフェース(ISDNポート、WANポート、LANポート)を
　柔軟に操ることができるWWW設定機能　(ISDNポートは、RTA55iのみ)
c) ISDNダイヤルアップルーターの洗練された抜群の使い勝手を継承
d) 平易な文章、トラブルシューティングしやすいマニュアルや情報の提供

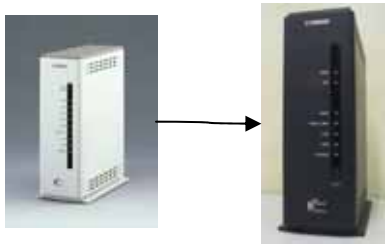
・RTA54iを改善

a) LAN側10BASE-Tハブを10BASE-T/100BASE-TXスイッチングハブに変更
b) 高速CPUを採用し、スループットを改善 (最大12Mbps)
c) ACアダプタの小型化　(RTA55iのみ)

RTA55iの仕様

ハードウェア	ソフトウェア
○ グッドデザイン賞の受賞筐体 ◎ 高速CPU(133MHz,1.66倍) ○ 100BASE-TX対応WANポート ◎ 100BASE-TX対応LANポート L2スイッチングHUB*4ポート MDI/MDI-X自動判別機能 ○ TELポート(2ポート) ○ DSU内蔵ISDNポート ○ USBポート ◎ 小型ACアダプタ	○ネットワーク・アプリケーション対応 NetMeeting3.0対応、UPnP対応(予定)など ◎ファイアウォール搭載 静的フィルタリング、動的フィルタリング、 不正アクセス検知、セキュリティレベル ◎VPN機能(PPTP)と暗号機能(RC4)を搭載 LAN間接続VPN、 Windowsからのリモートアクセス VPN ネットボランチDNSのホストアドレスサービス ◎インターネット電話(VoIP)搭載 ネットボランチDNSの電話アドレスサービス ○ブロードバンド向けプロバイダ接続機能 ○スループット：12Mbps(最大)

(◎:RTA54iからの変更点)　　(◎:コンセプト)



RT56vの仕様

ハードウェア	ソフトウェア
◎ 黒いRTW65系筐体 ◎ 高速CPU(133MHz,1.66倍) ○ 100BASE-TX対応WANポート ◎ 100BASE-TX対応LANポート L2スイッチングHUB*4ポート MDI/MDI-X自動判別機能 ◎ TELポート(3ポート) ◎ LINEポート	○ネットワーク・アプリケーション対応 NetMeeting3.0対応、UPnP対応など ◎ファイアウォール搭載 静的フィルタリング、動的フィルタリング、 不正アクセス検知、セキュリティレベル ◎VPN機能(PPTP)と暗号機能(RC4)を搭載 LAN間接続VPN、 Windowsからのリモートアクセス VPN ネットボランチDNSのホストアドレスサービス ◎インターネット電話(VoIP)搭載 ネットボランチDNSの電話アドレスサービス ○ブロードバンド向けプロバイダ接続機能 ○スループット：12Mbps(最大)

(◎:RTA54iからの変更点)　　(◎:コンセプト)

RTA55iとRT56vのハードウェアの違い

(アナログ回線でのインターネット電話機能に対応)

ISDN回線　　アナログ回線

	RTA55i	RT56v
ISDNポート	1	–
LINEポート	–	1
TELポート	2	3
WANポート	1	1
LANポート	4	4
USBポート	1	–
ACアダプタ	小型化	大型

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

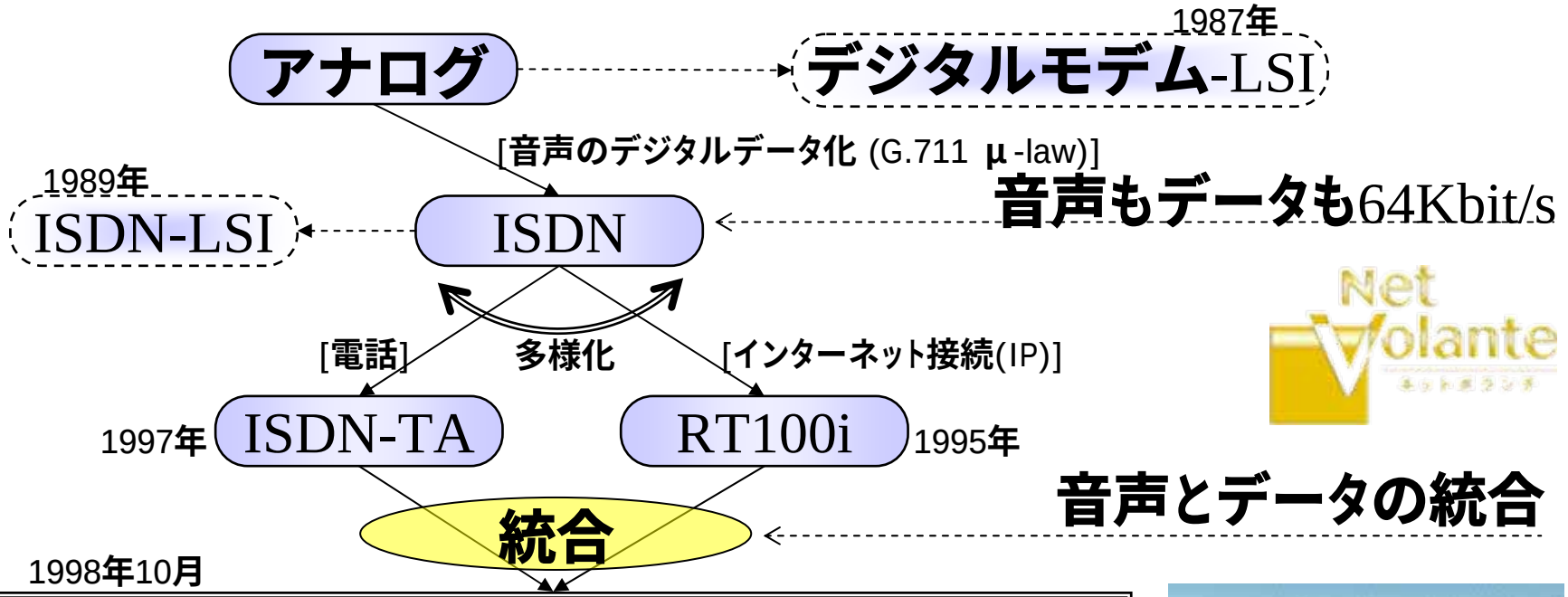
2002年5月 RTA55i発売。
RTA54i/RT60w/RTW65iにてIPv4/IPv6版SIPによるVoIP機能の
β2版ファームウェアの提供開始

2002年7月 RT56v発売。

・MGCP:Media Gateway Control Protocol、RFC2705

・SIP:Session Initiation Protocol、RFC2543

1998年10月ネットボランチが生まれた



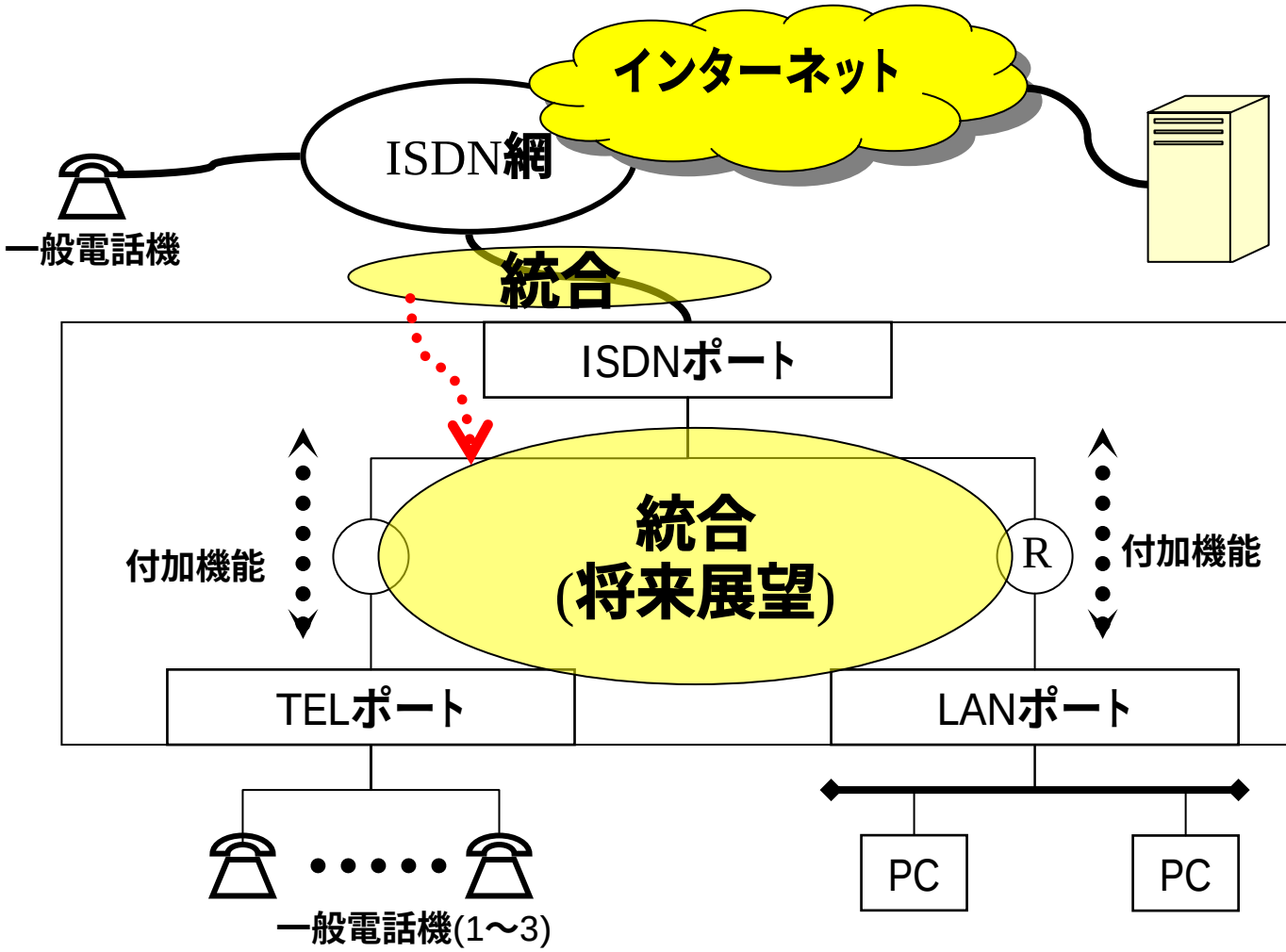
[ネットボランチRTA50i]

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

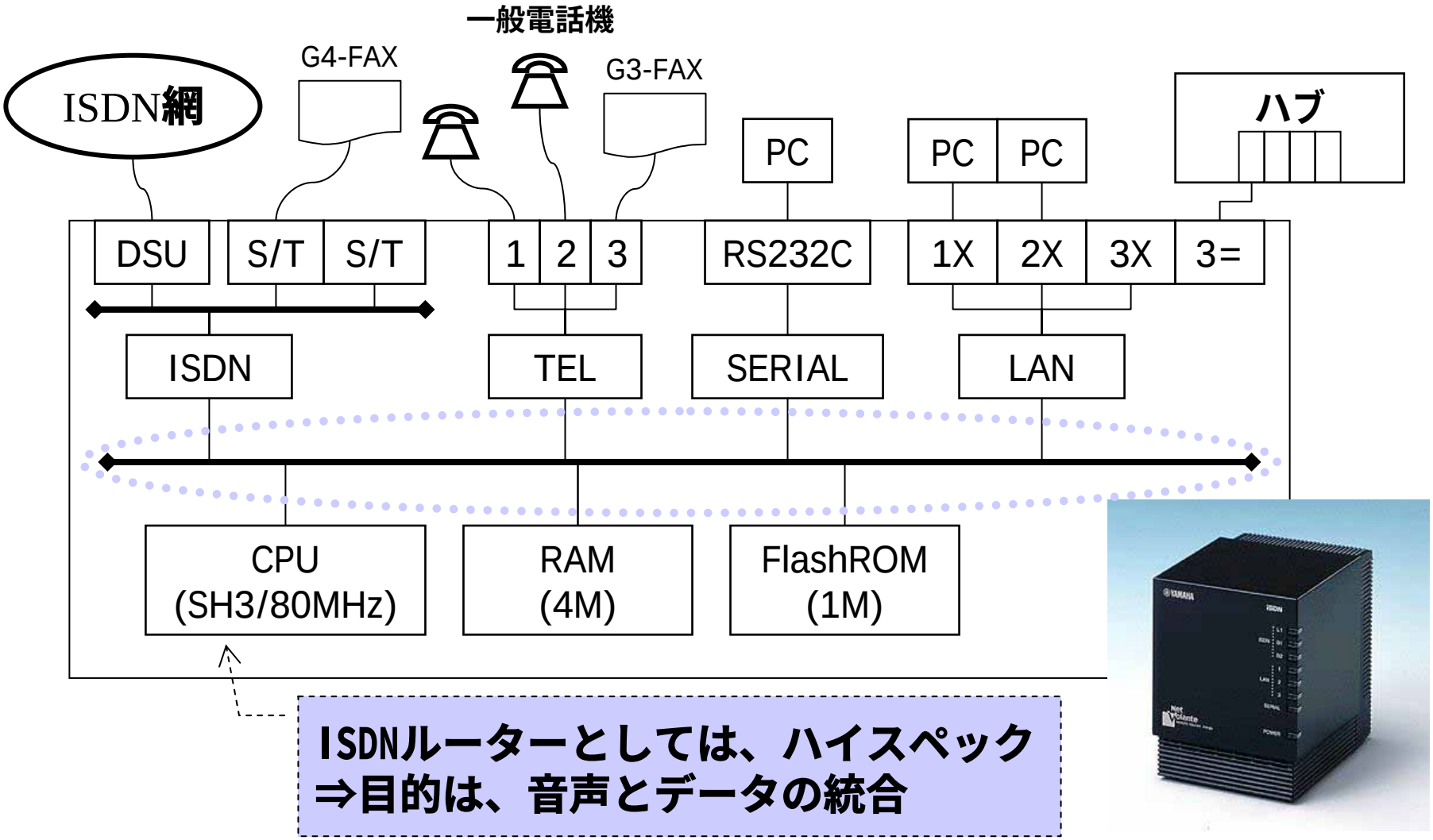
ヤマハ ネットボランチ

ISDNルーターの構成(音声とデータの統合)



RTA50i

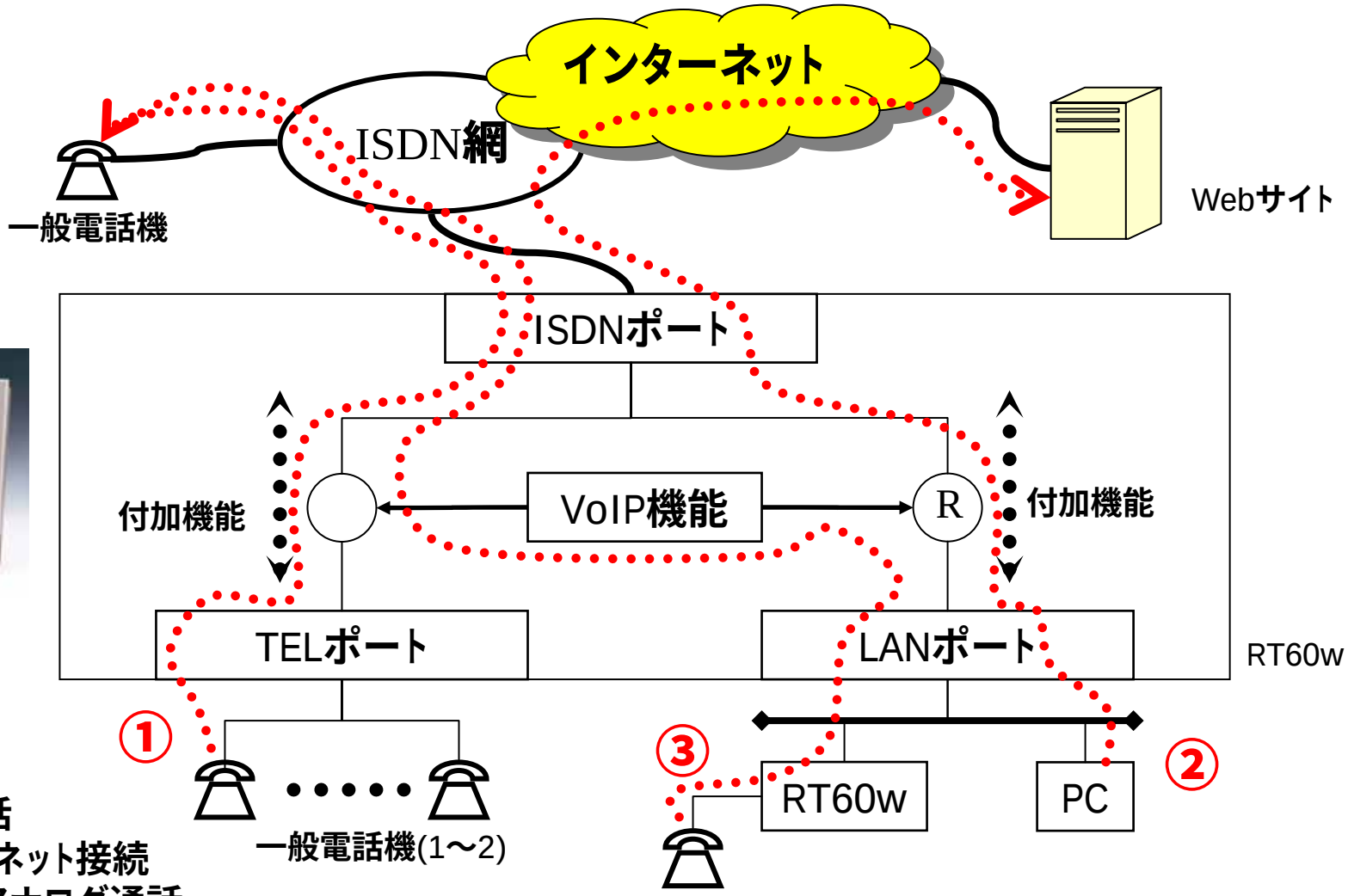
ネットボランチ RTA50iのアーキテクチャ



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

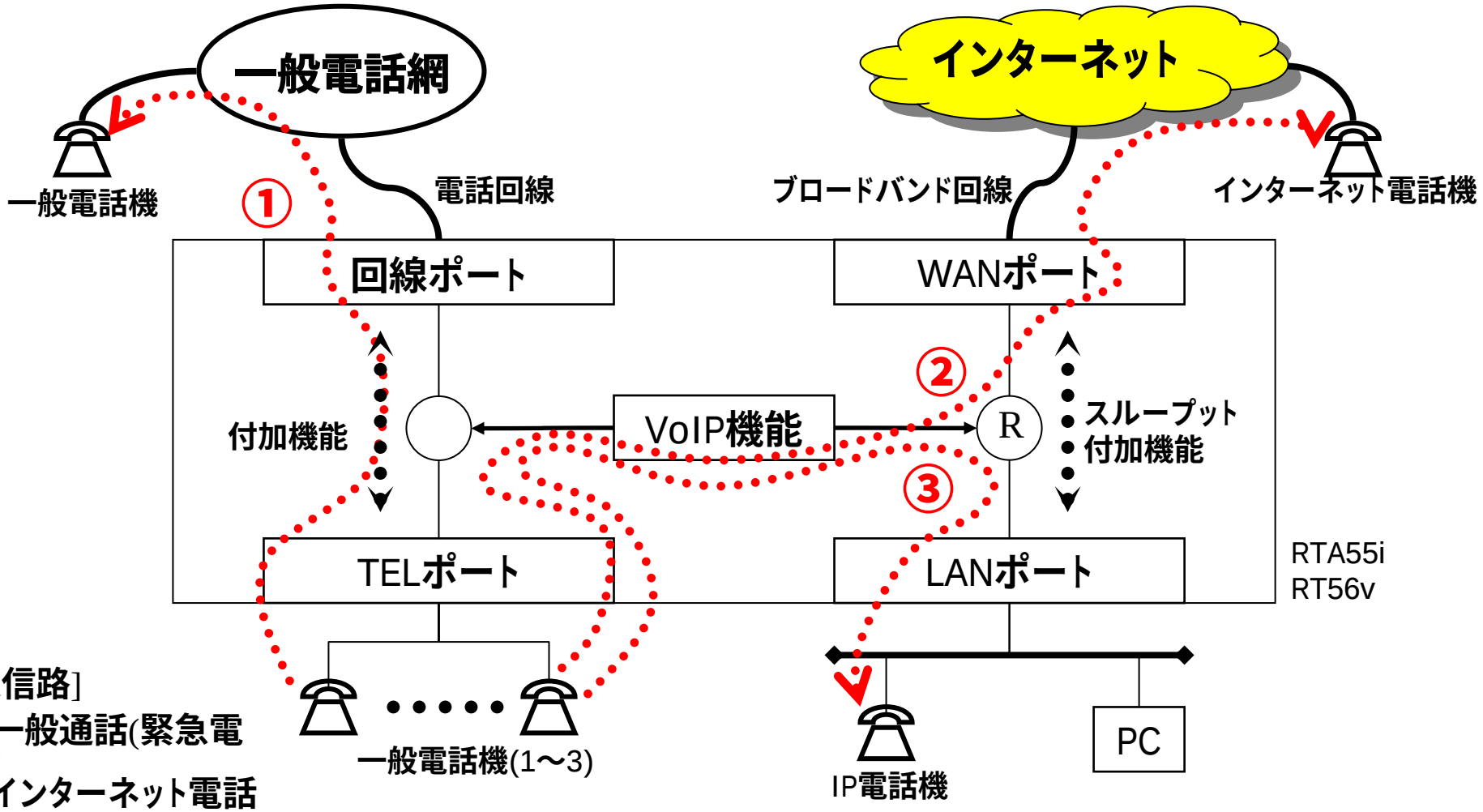
・ビジネスホン/ホームテレホンの要素

・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)

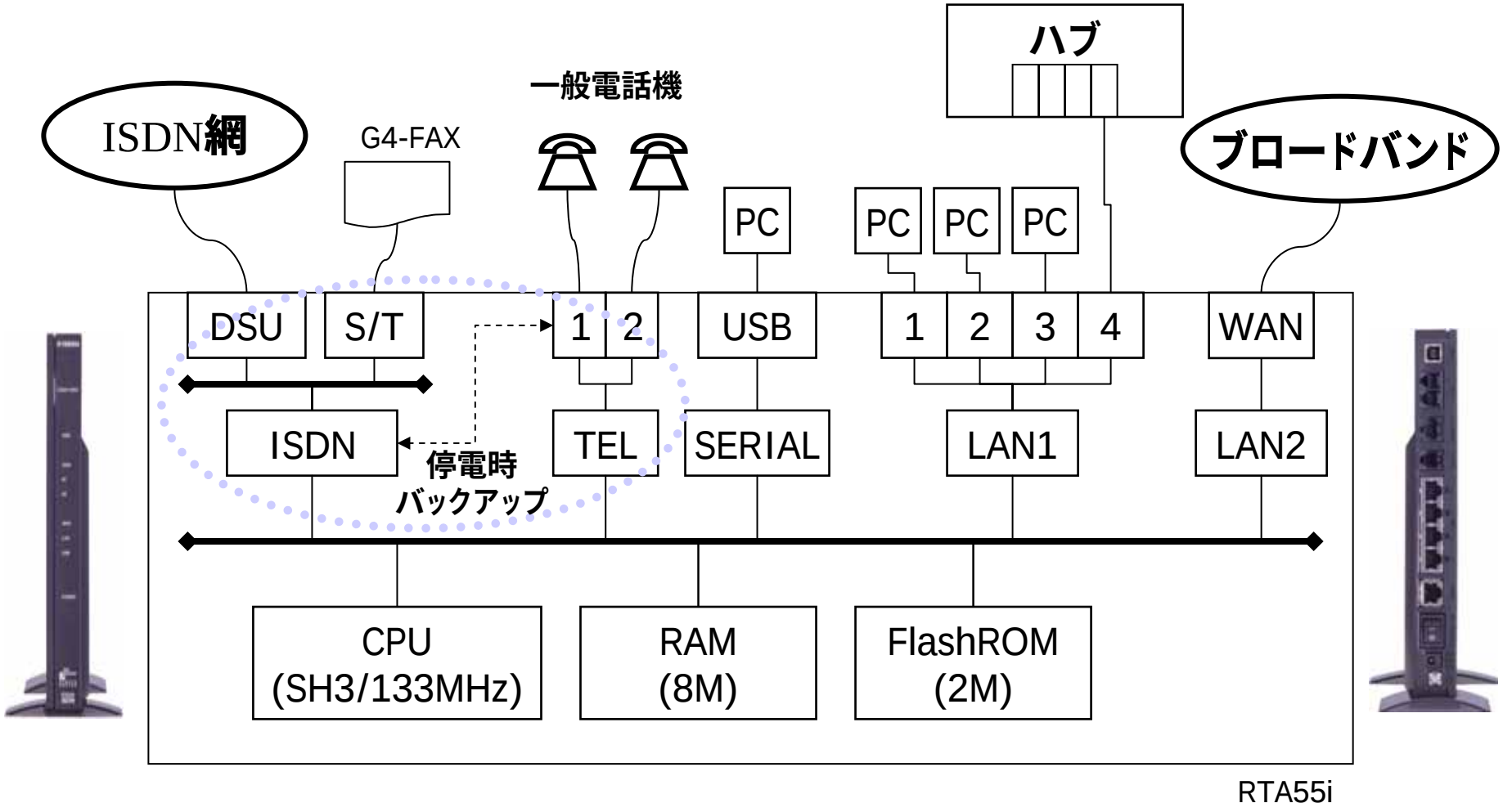
SIP:Session Initiation Protocol、RFC2543



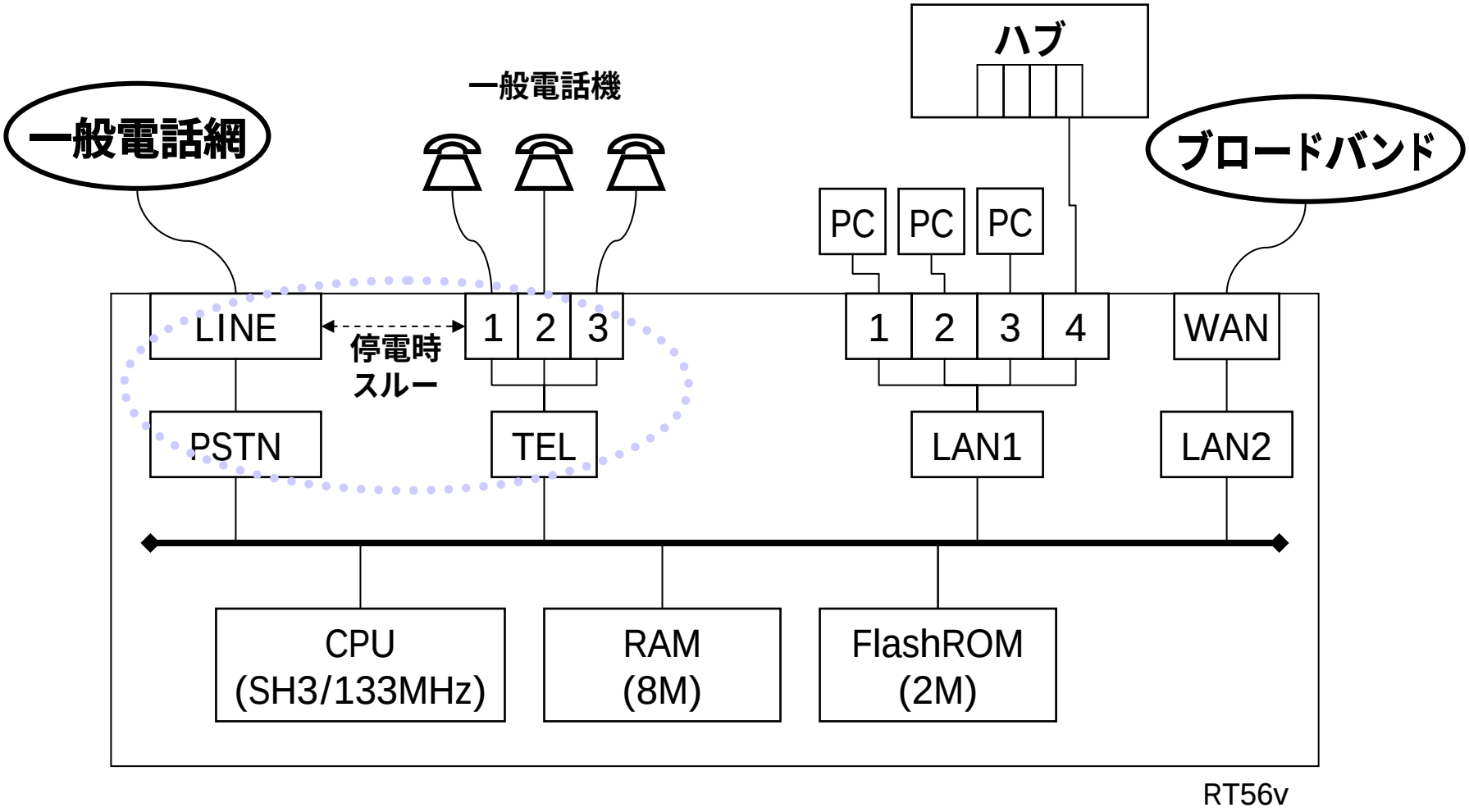
[通信路]
①一般通話(緊急電話)
②インターネット電話
③内線のIP電話

http://www.yamaha.co.jp/news/01121201.html

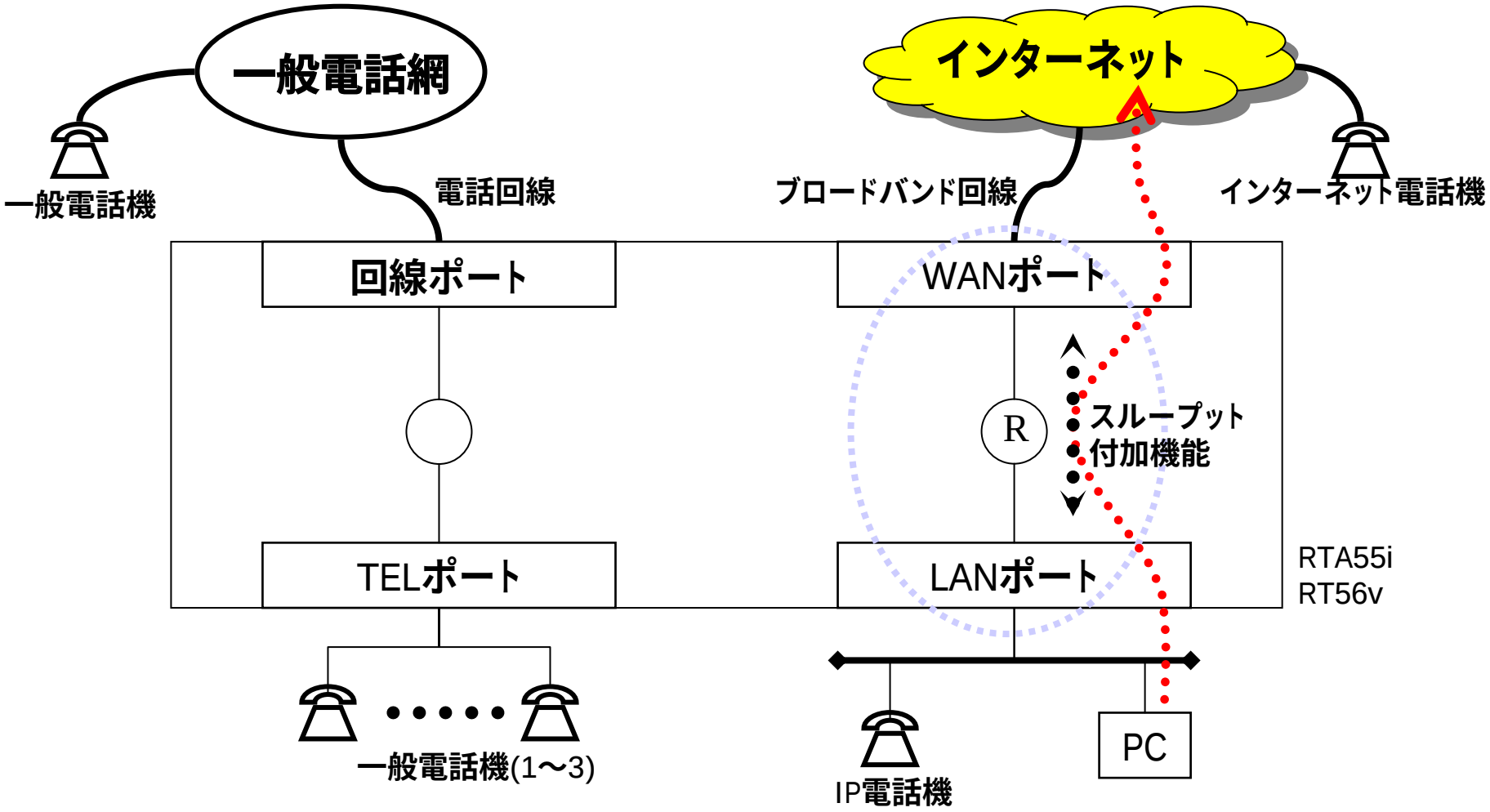
ネットボランチ RTA55iのアーキテクチャ



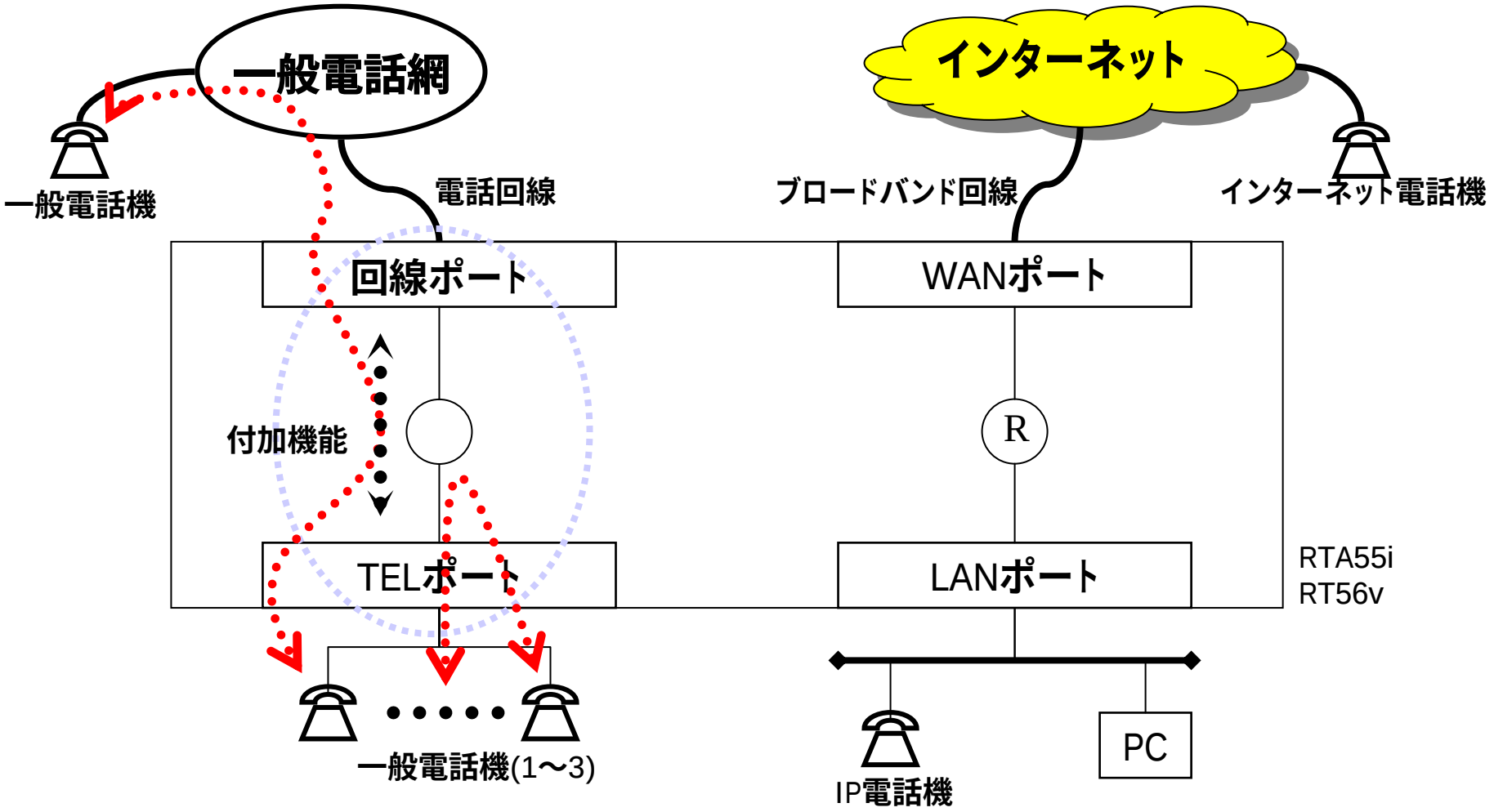
ネットボランチ RT56vのアーキテクチャ



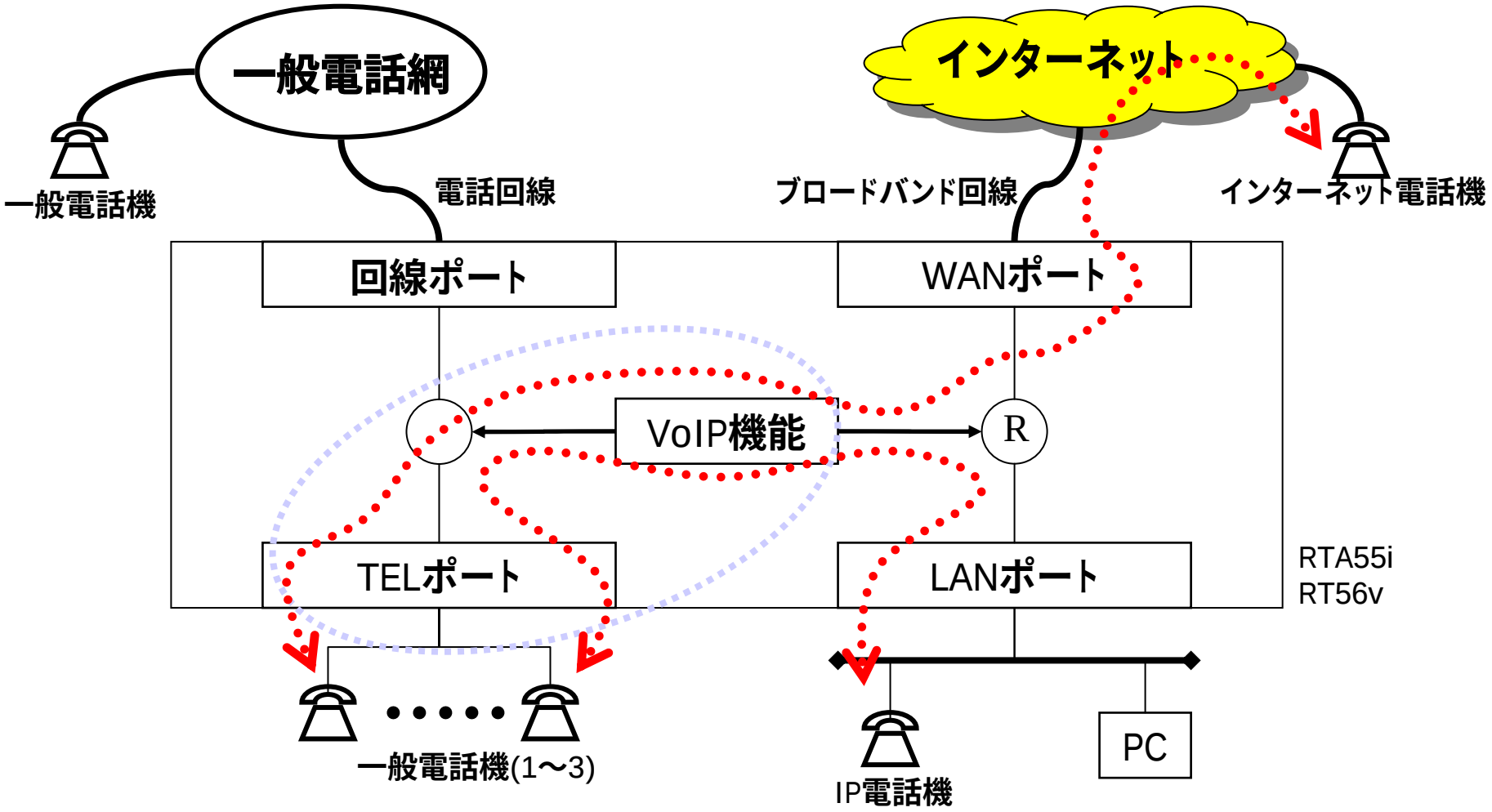
ブロードバンドルータの要素



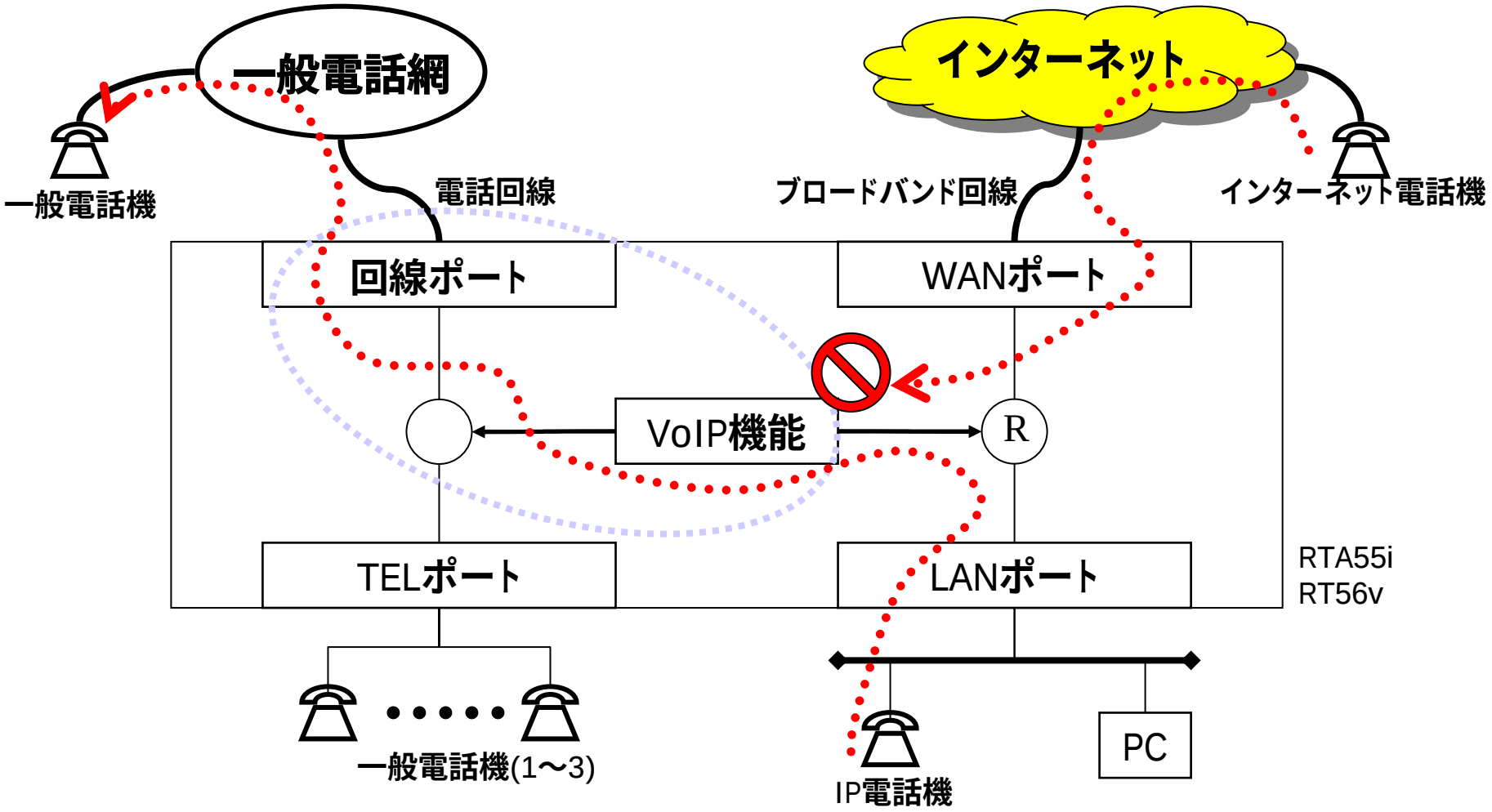
ビジネスホン/ホームテレホンの要素



インターネット電話(VoIP-TA)の要素

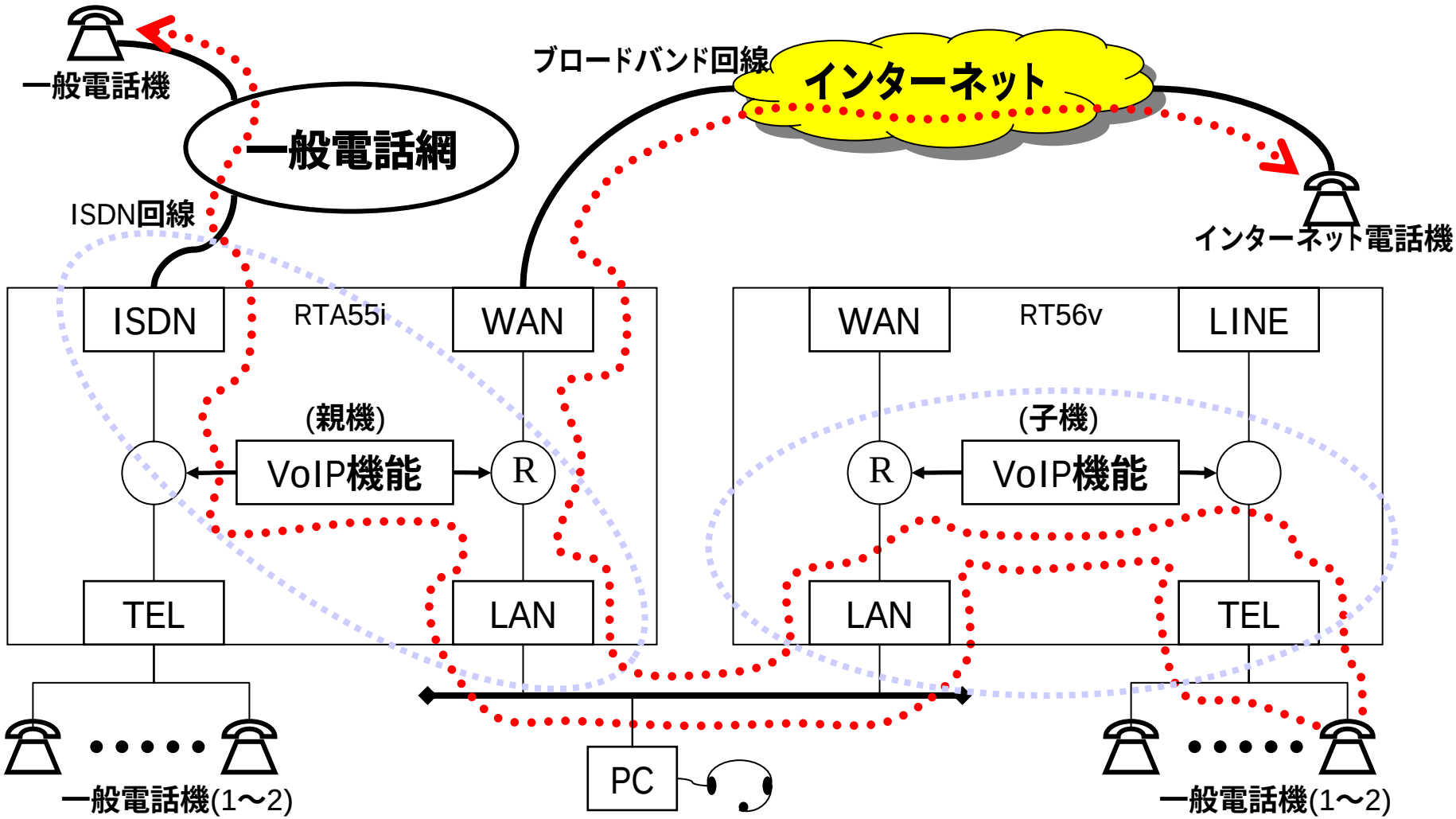


VoIPゲートウェイの要素(提供未定)

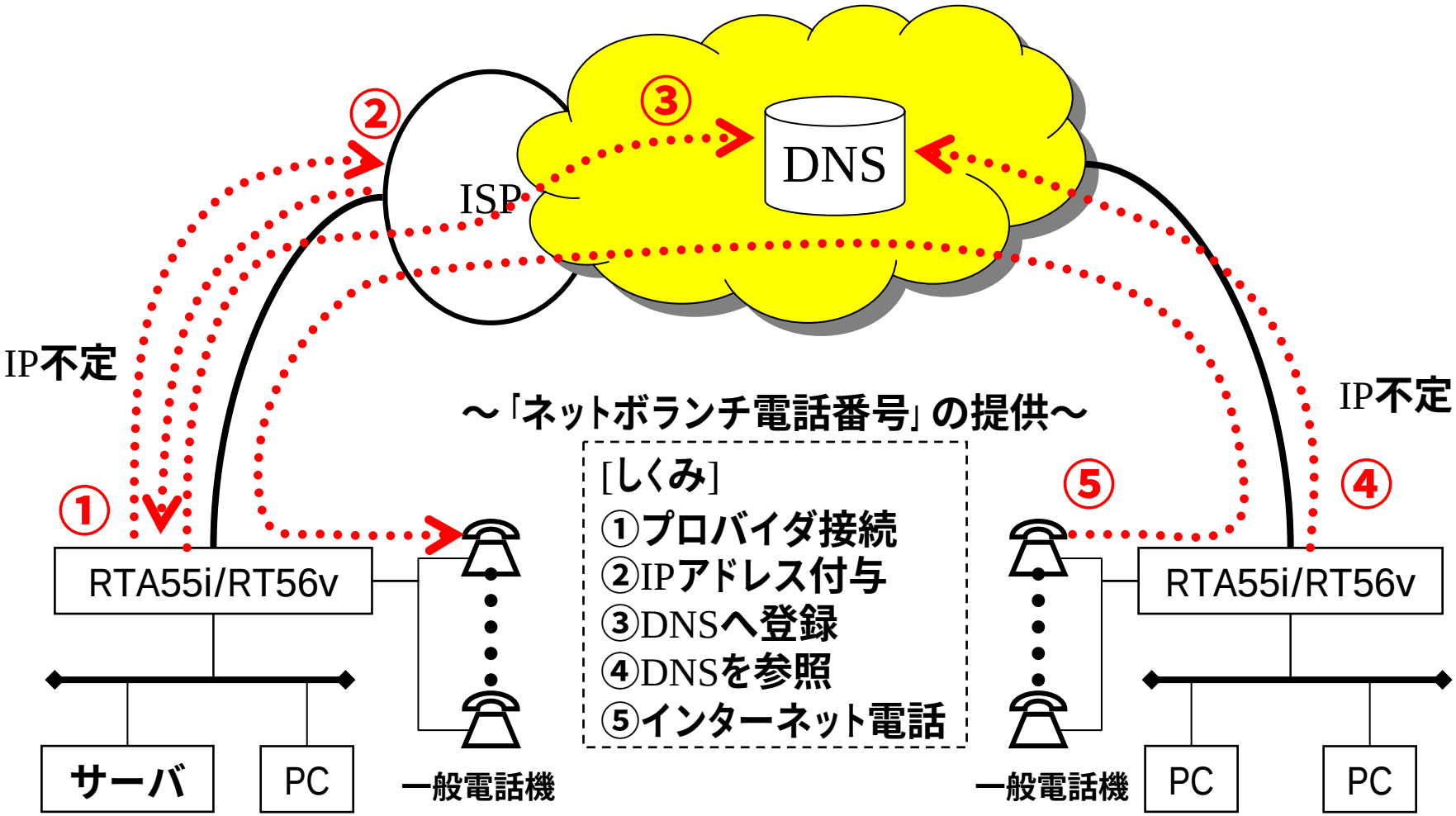


機器間アナログ通話(TELポートの増設)

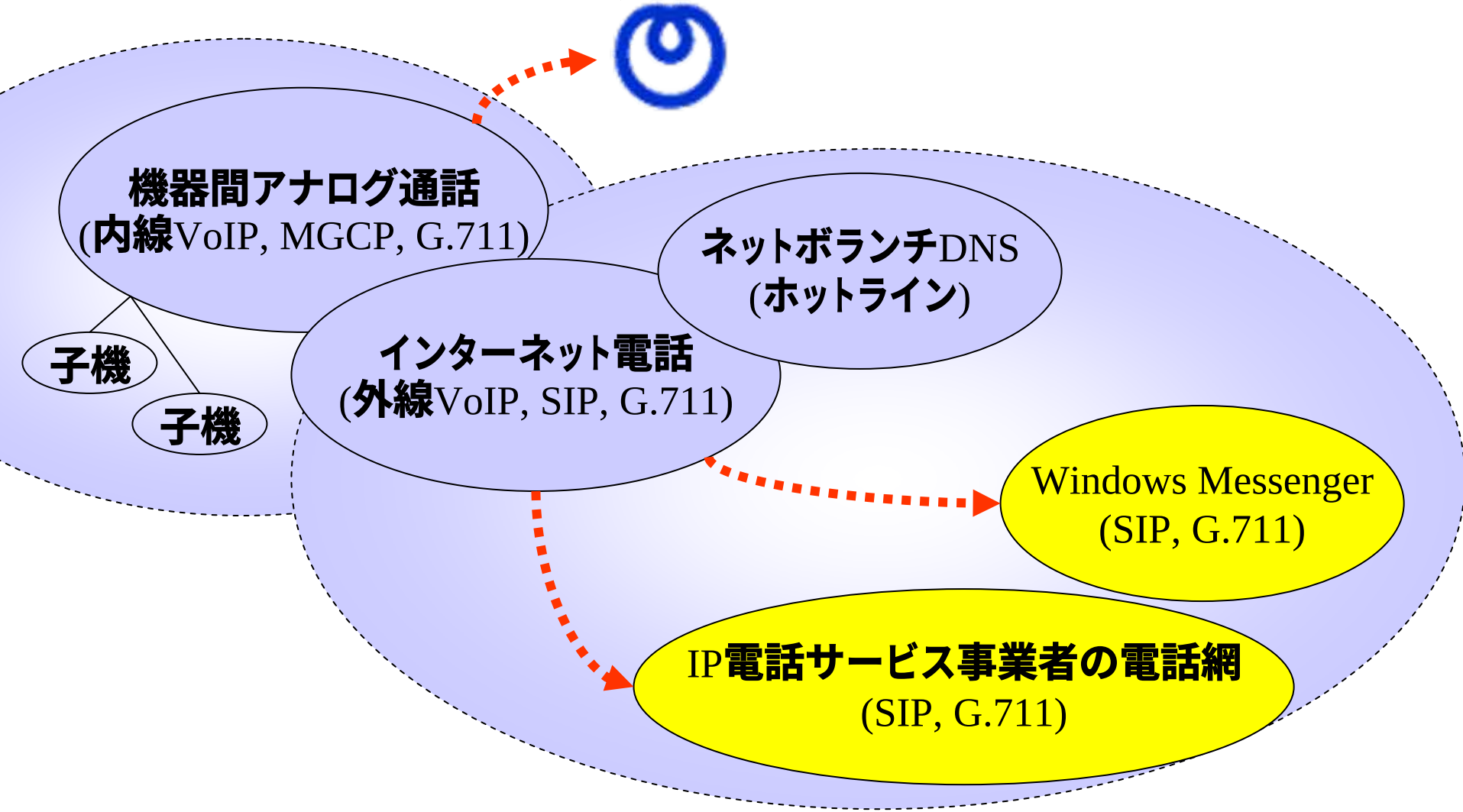
MGCP:Media Gateway Control Protocol、RFC2705
SIP:Session Initiation Protocol、RFC2543



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/L2TPによるVPN機能をRTシリーズで提供予定

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(RT300i、RT140シリーズ、RT105シリーズ)など

Microsoft Windows系OS(Microsoft VPN Adapter)

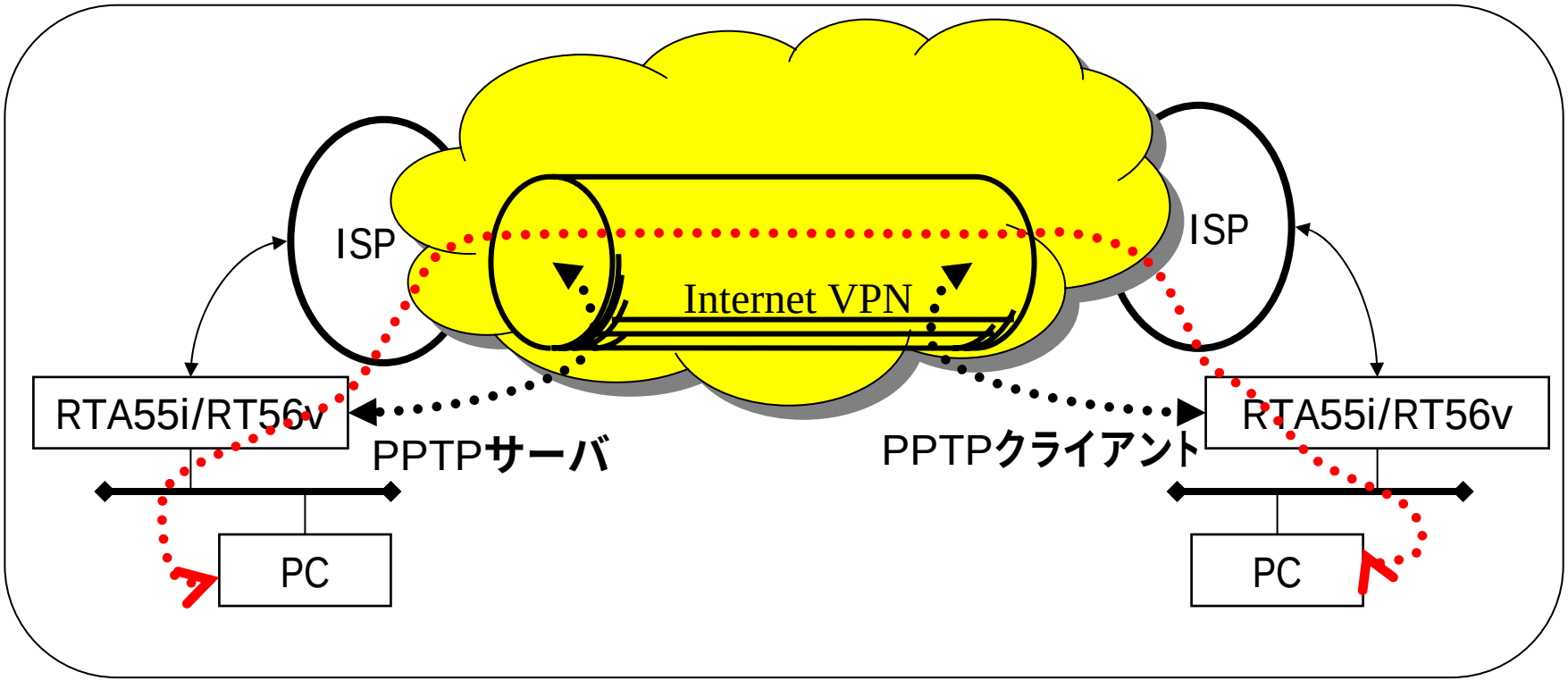
◎ 暗号機能:RC4 (RSAセキュリティ社よりライセンス)

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

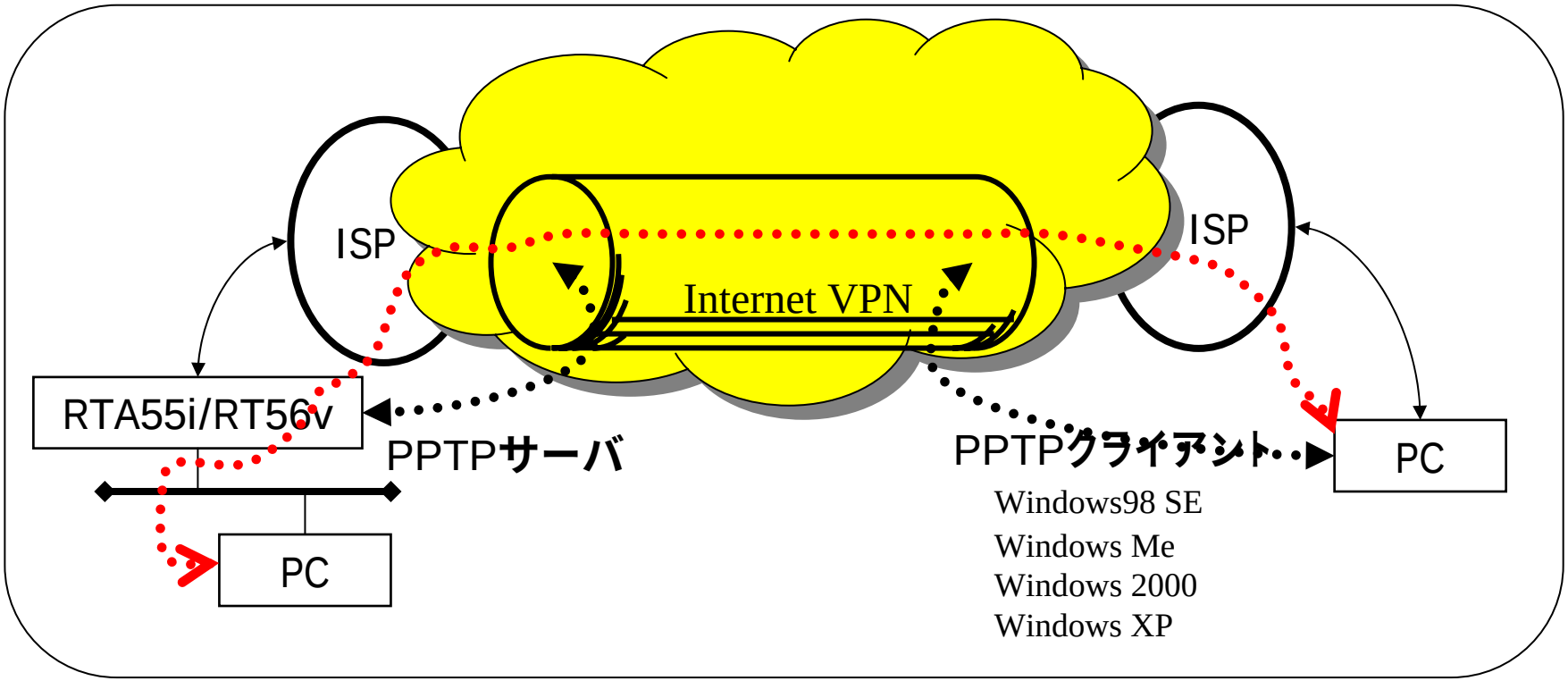
- LAN間接続VPN
- リモートアクセスVPN

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。**

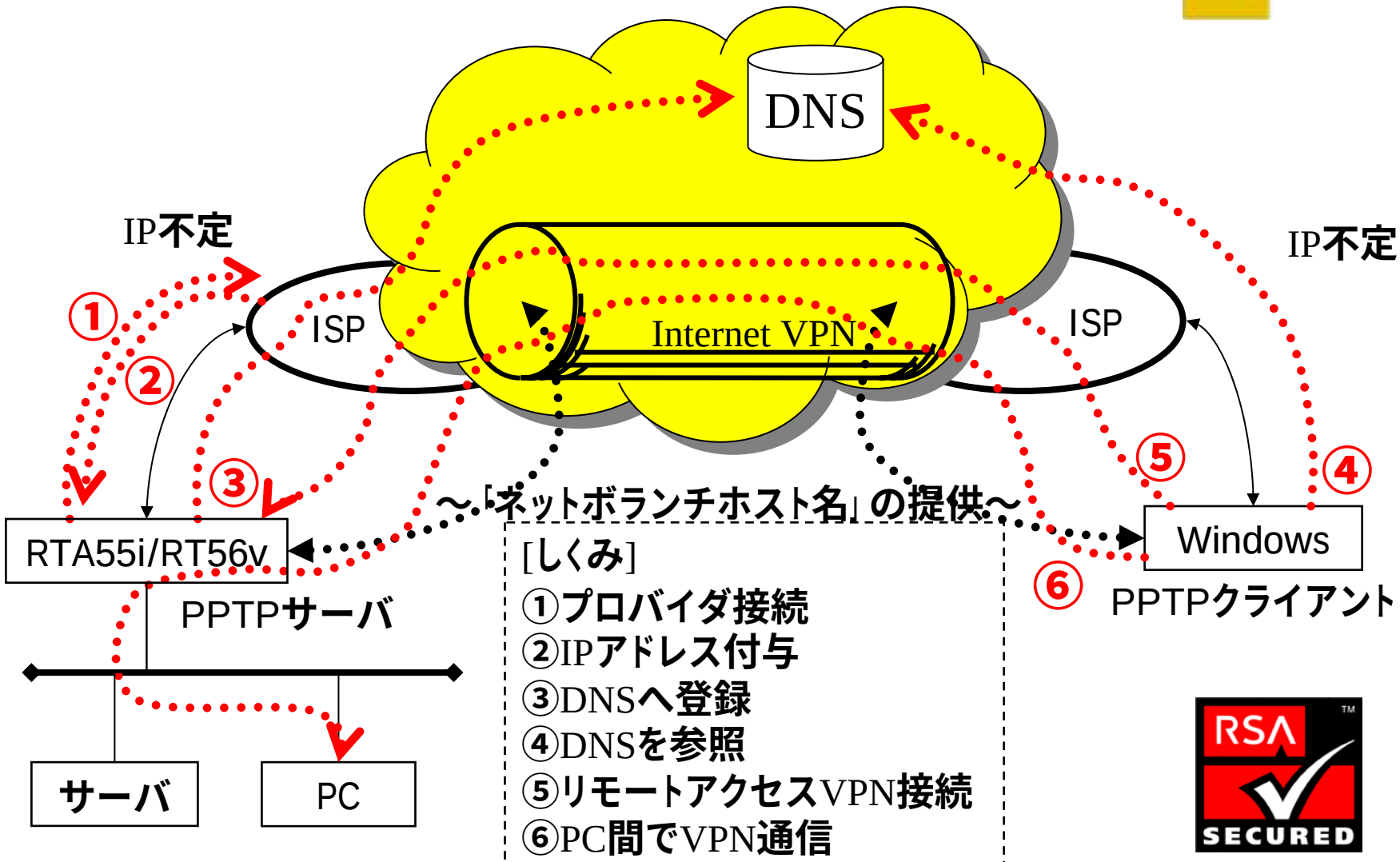
リモートアクセスVPN (PPTP+RC4)



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
対応予定






	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	○	－	○	○	－	－
ネットボランチ DNS	○	○	○	○	○	○
インターネット電話 (VoIP)	○	○	－	○	○	○
VPN (PPTP+RC4)	－	－	○	○	○	○

参考資料

インターネット電話(VoIP)とは？

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

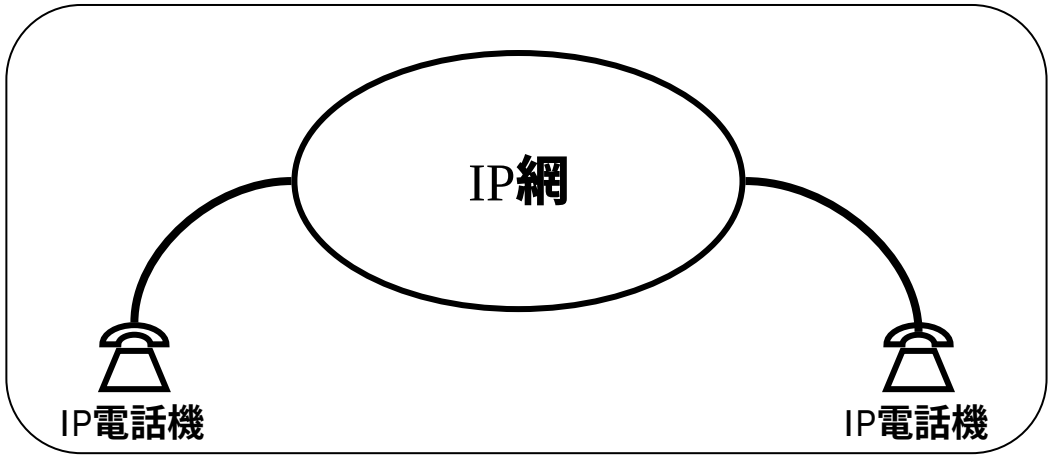
IP電話やインターネット電話を実現する技術の総称

プロトコルには、H.323、MGCP、SIPなどいくつかある。

「ITSP」：Internet Telephony Service Provider

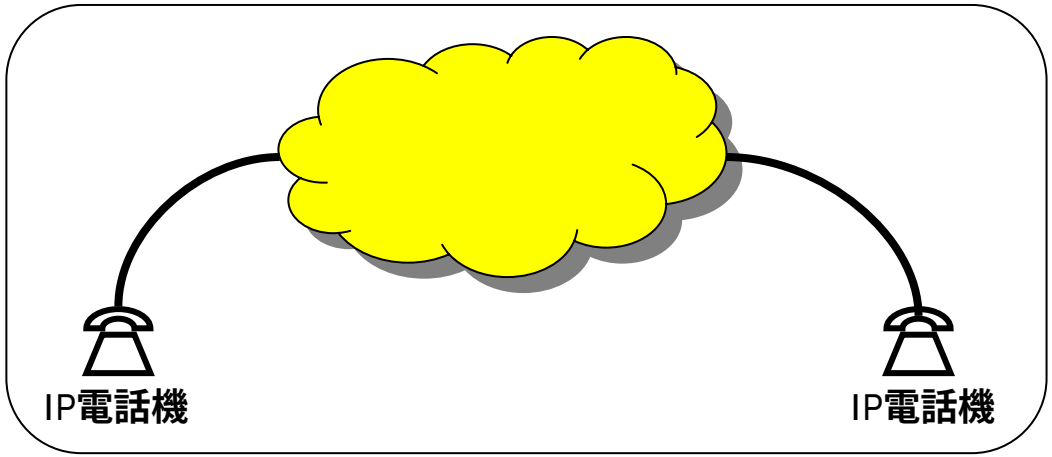
IP電話やインターネット電話サービスを提供する事業者

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。

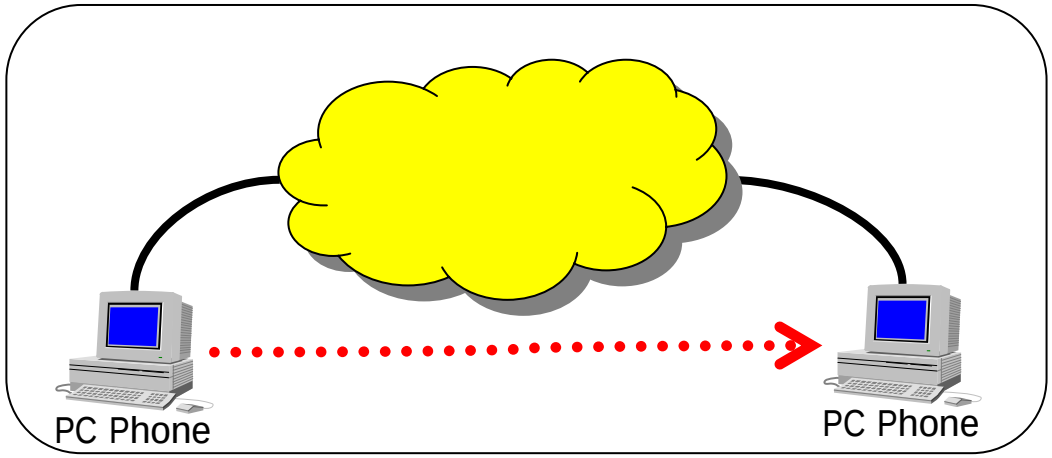
「Phone-to-Phoneタイプの IP電話サービス」：

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」：

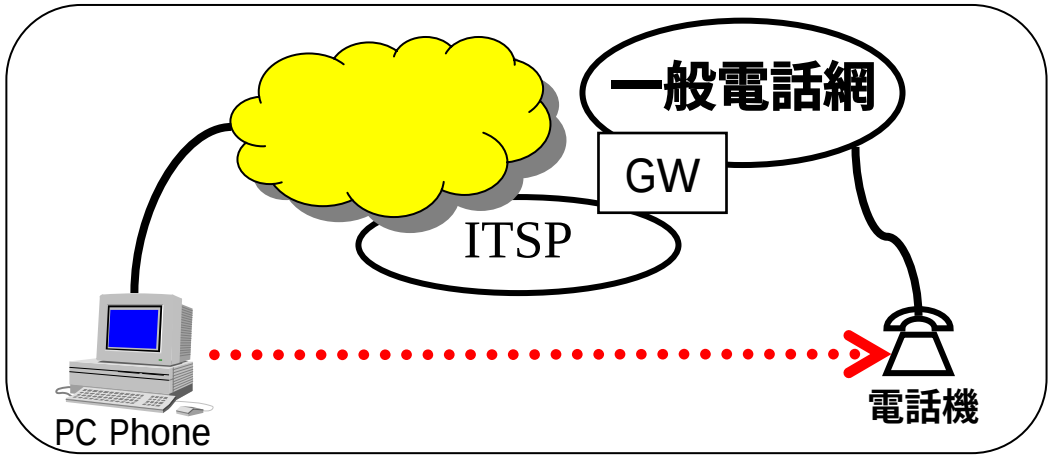
PCの電話番号、常時接続されたPC、などの課題があり実際に提供されるサービスは無い。

「PC-to-PC」と「PC-to-Phone」



PC-to-PC

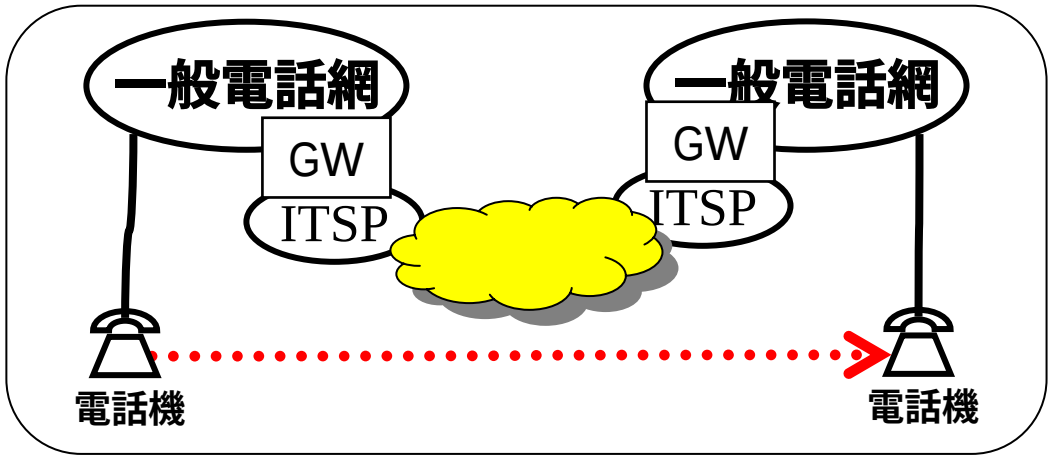
[回線の特徴]
・1994年～
・ダイヤルアップによる
インターネット接続環境
(-) 低音質、パソコン必須
(+) 低コスト



PC-to-Phone

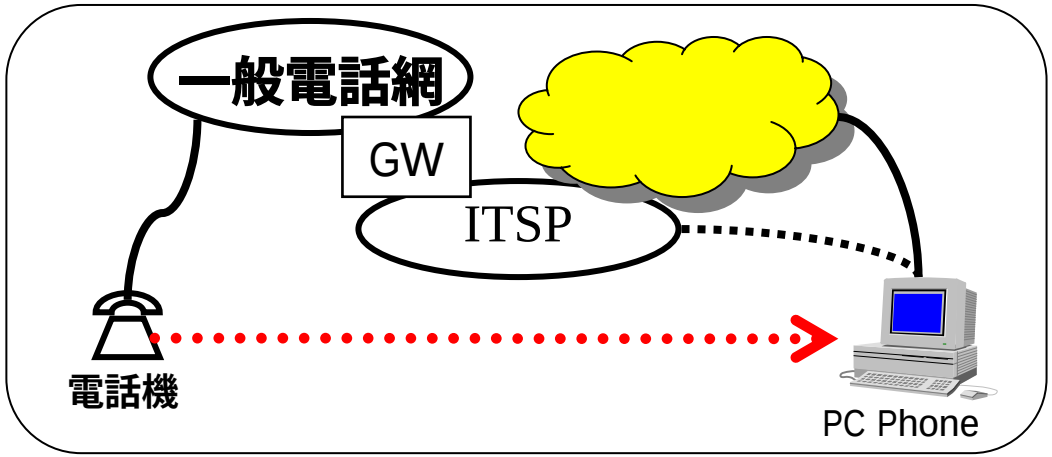
[回線の特徴]
・1996年～
・ダイヤルアップによる
インターネット接続環境
(-) 低音質、パソコン必須
(+) 低コスト

「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

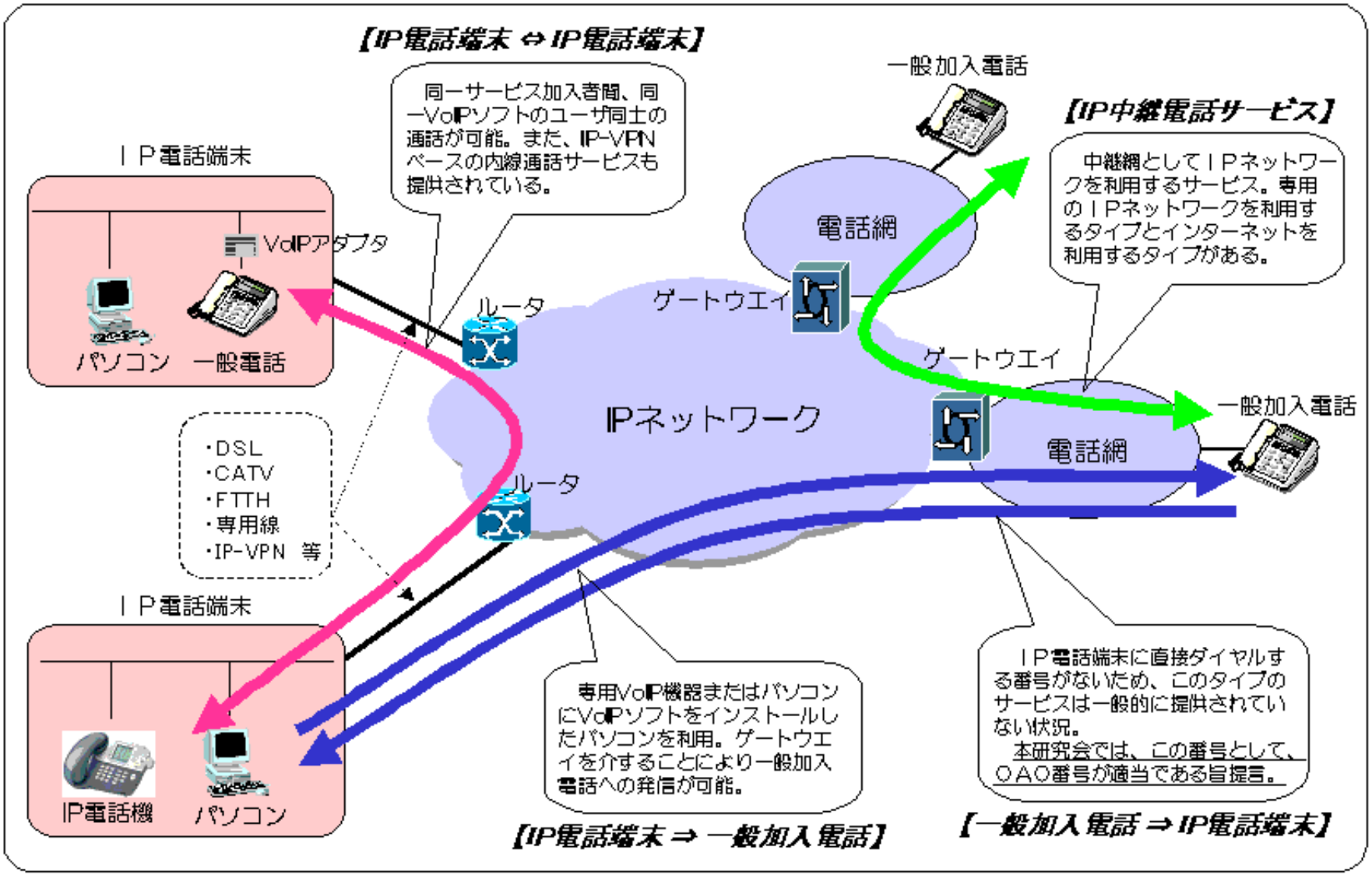


Phone-to-PC

[回線の特徴]
・未提供
(-) 常時接続性、電話番号

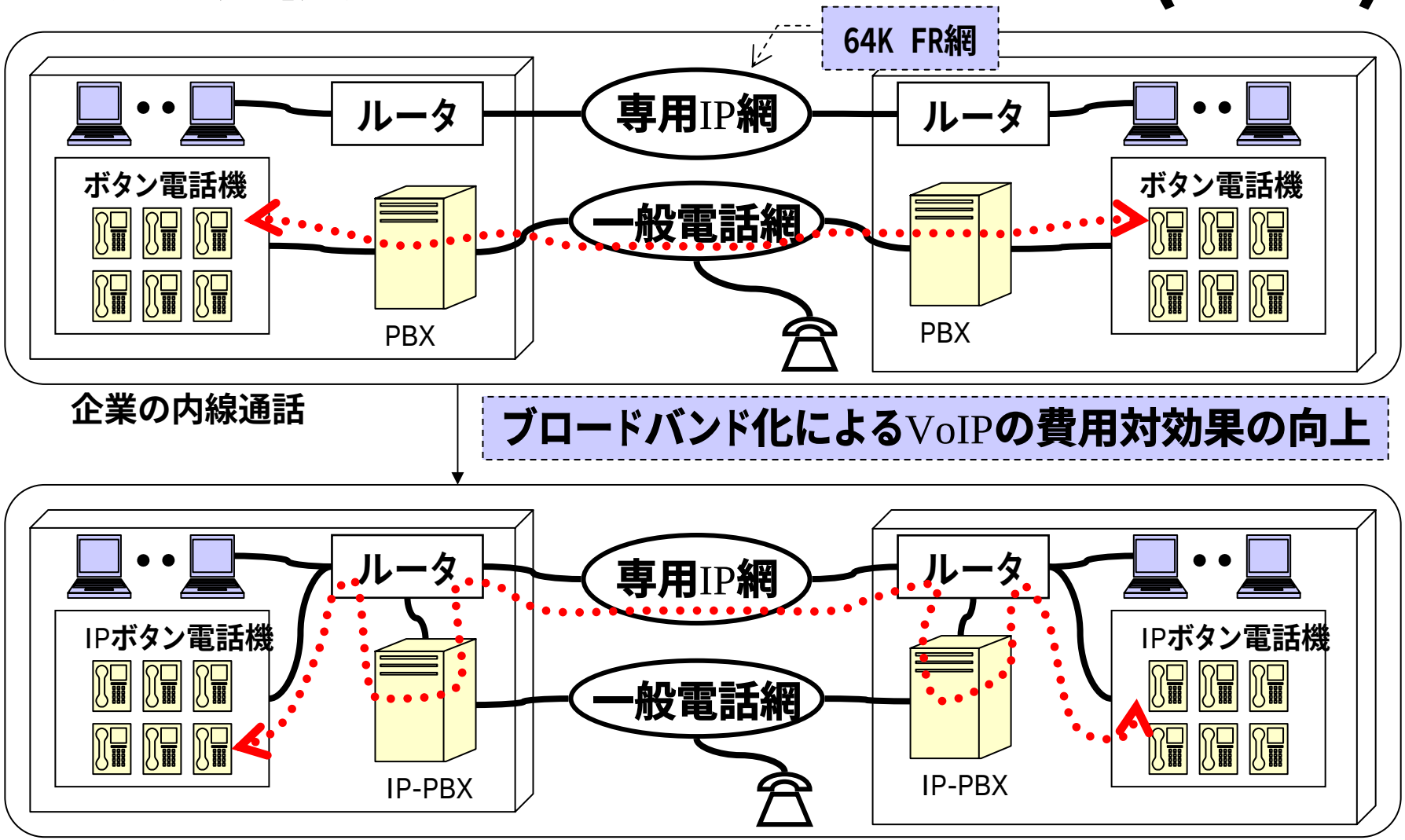
ブロードバンド化による IP電話サービス

(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

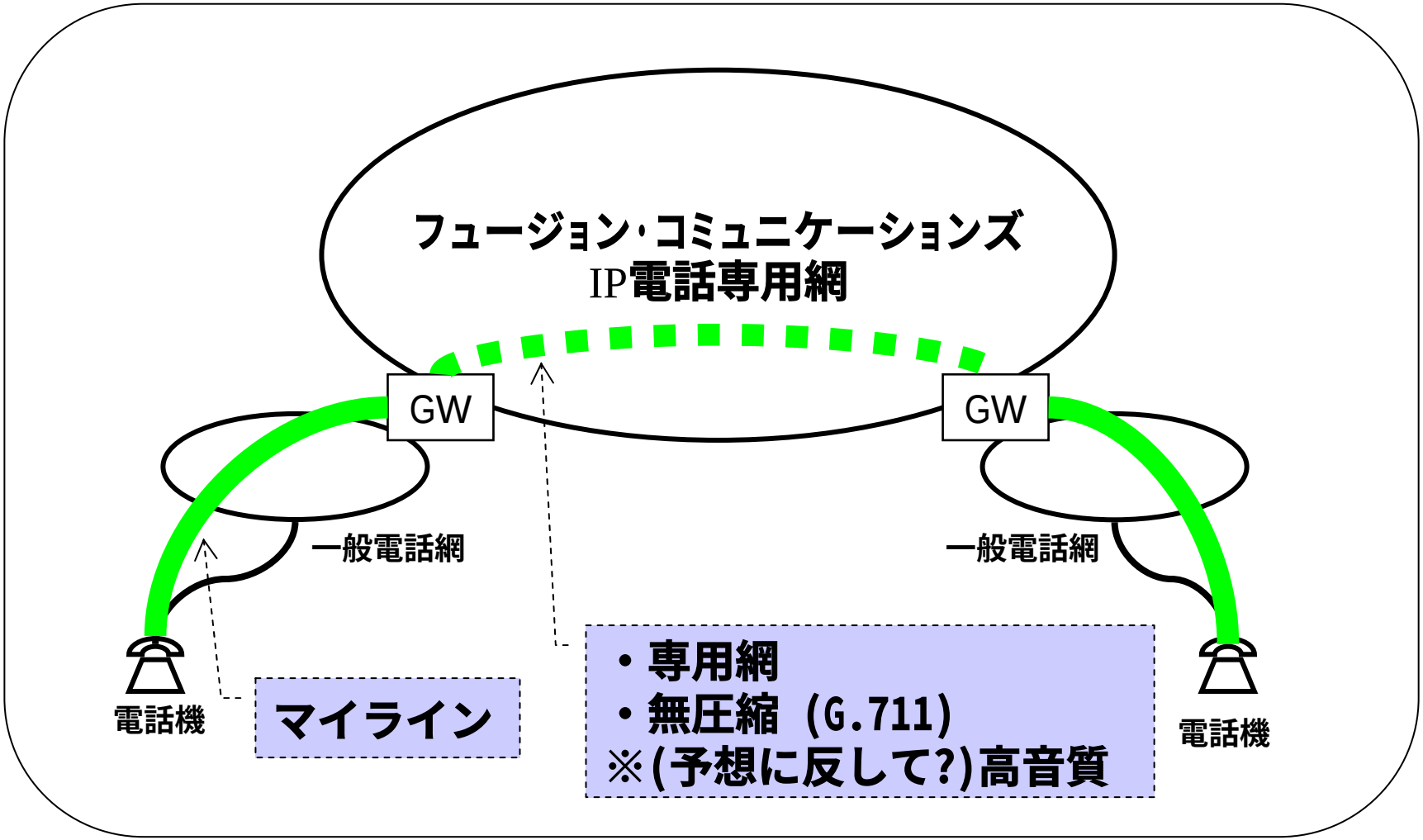


※ 本研究会では、これらすべてのタイプのIP電話サービスにおいて、ユーザが容易に理解できるようなエンドトゥエンドの品質を表示することが適当であるとし、また、それぞれのサービスの品質が適正に比較できるように、IP電話の品質評価方法等の標準化作業を官民が協力して推進していくことが必要である旨提言。

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

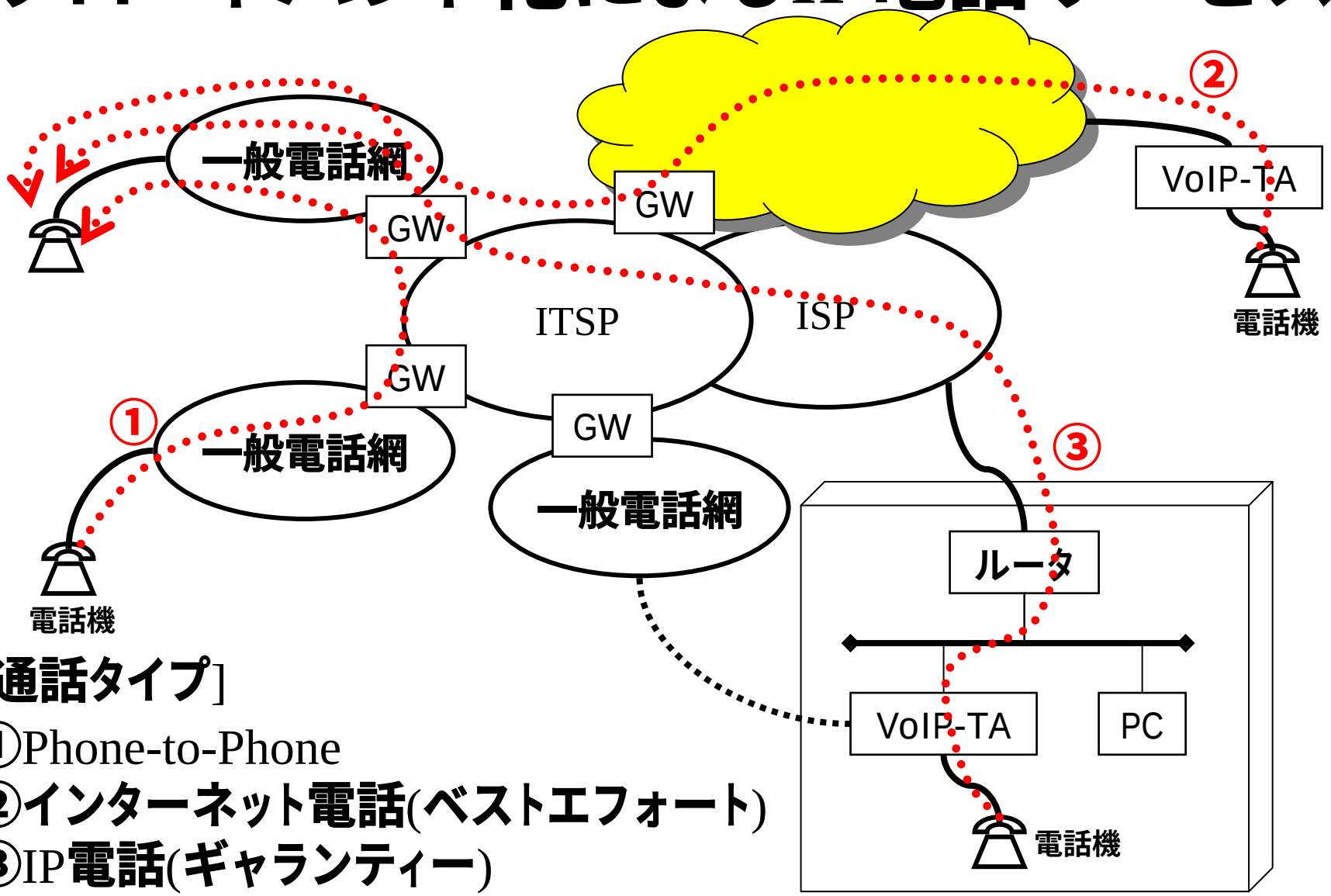
[ブロードバンド]
- 広帯域
- 低廉性
- 常時接続環境

[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

ブロードバンド化によるIP電話サービス



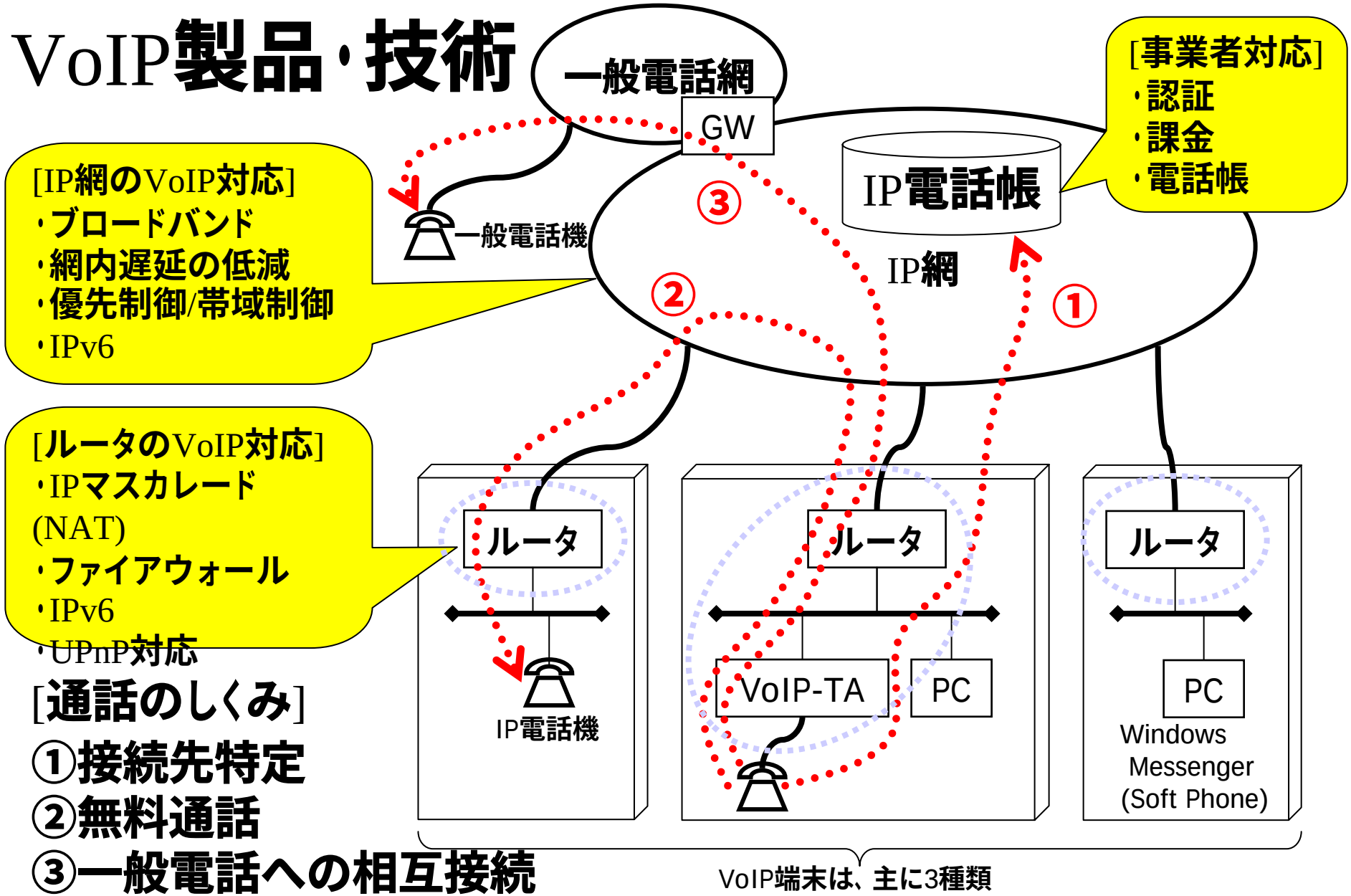
[通話タイプ]

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)

VoIP製品・技術



[通話のしくみ]

①接続先特定

②無料通話

③一般電話への相互接続

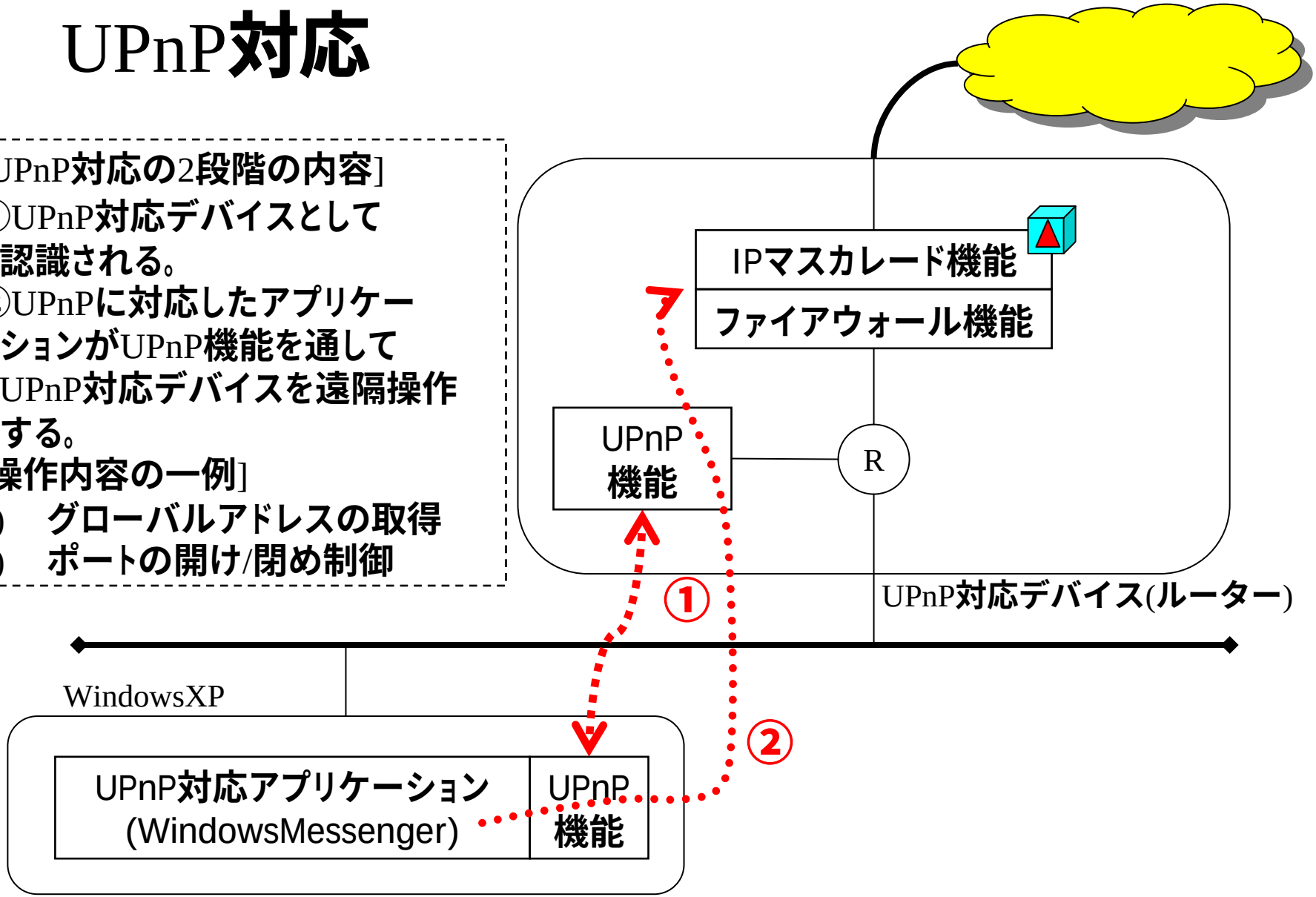
UPnP対応とWindowsMessenger

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

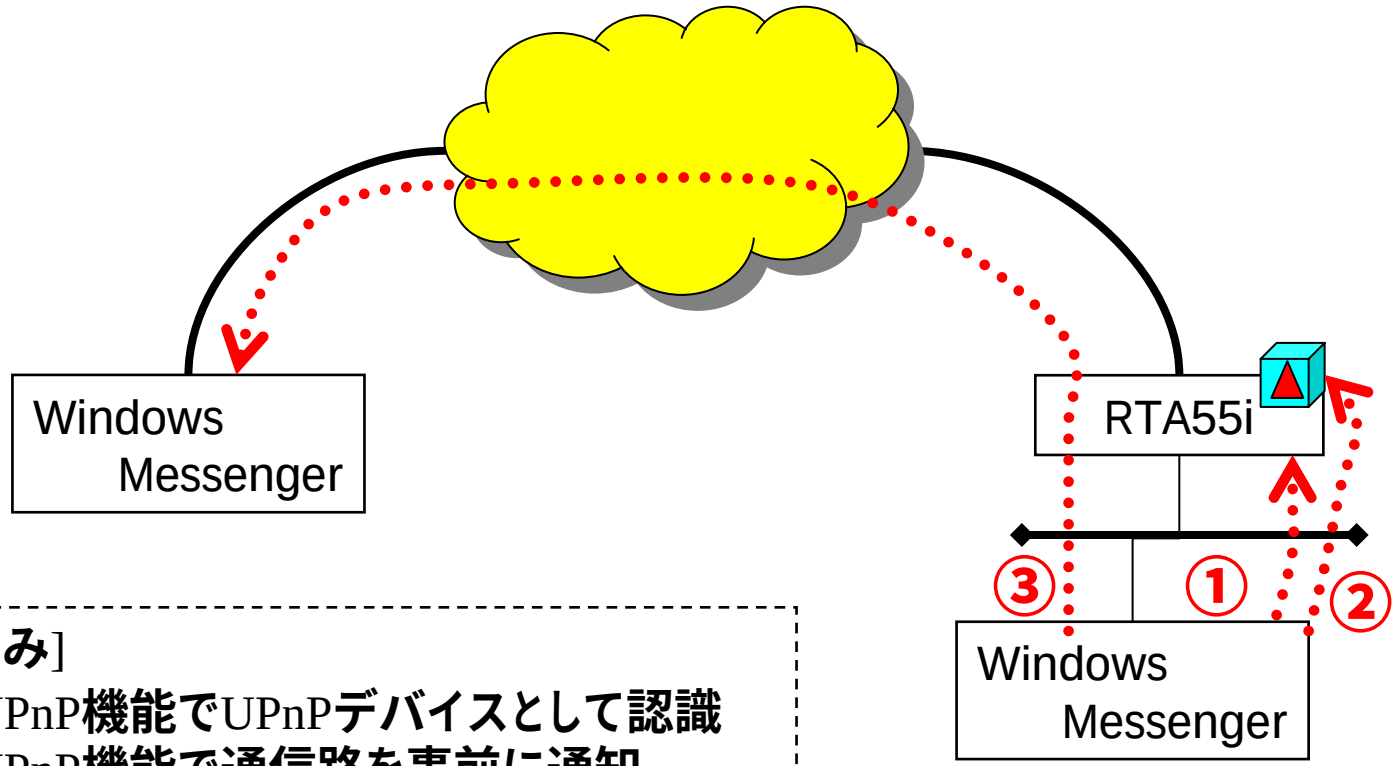
[UPnP対応の2段階の内容]
①UPnP対応デバイスとして認識される。
②UPnPに対応したアプリケーションがUPnP機能を通してUPnP対応デバイスを遠隔操作する。
[操作内容の一例]
1) グローバルアドレスの取得
2) ポートの開け/閉め制御



Windows Messenger対応とは？

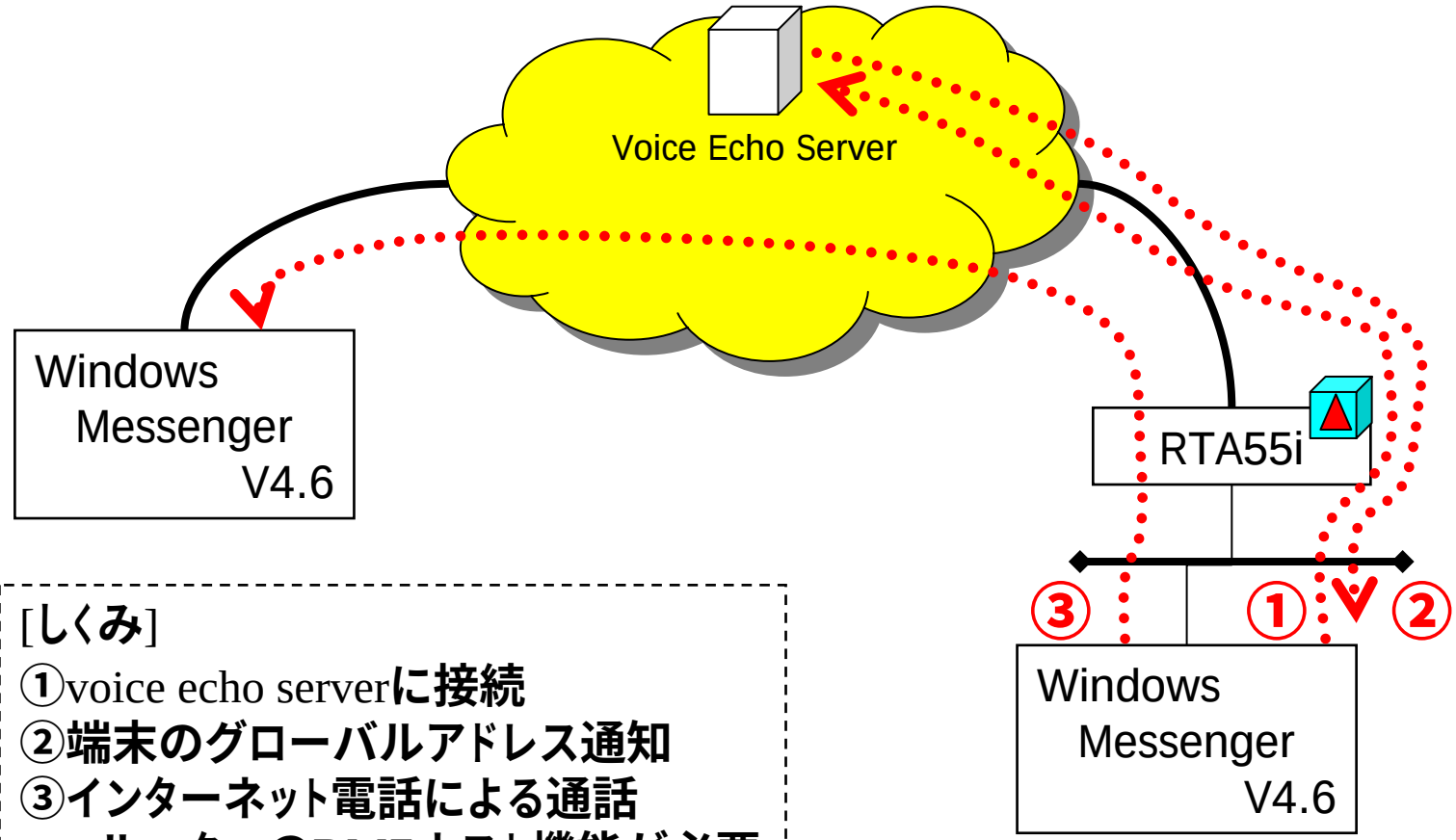
[やりたいこと]
・IPマスカレード利用環境でWindowsMessengerの
　機能を確実に使いたい。
[手段]
1) UPnP機能による対応
2) WindowsMessenger V4.6のNAT Traversal機能
　＋　DMZホスト機能
3) IPマスカレードでSIPのアドレス書換えによる対応

Windows MessengerのNAT越え#1
(UPnP機能対応)



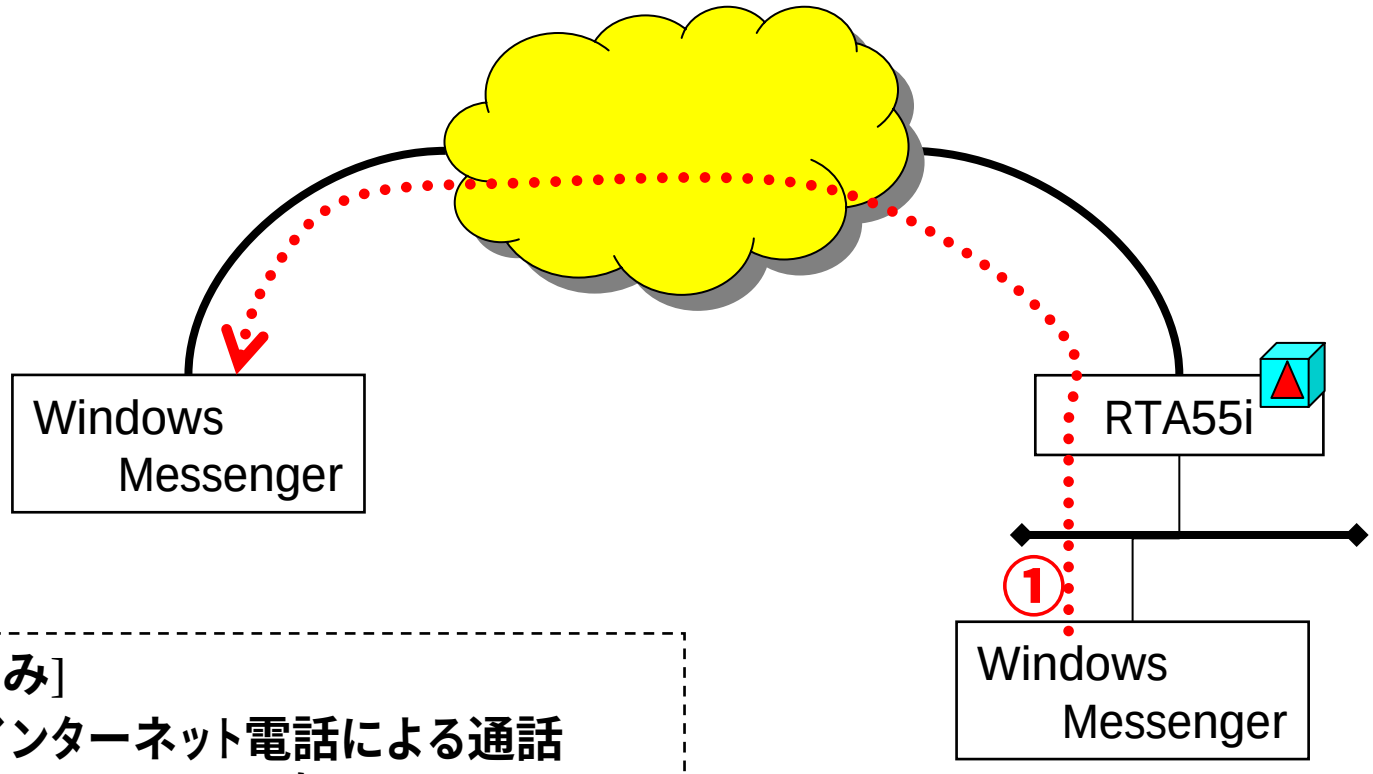
[しくみ]
①UPnP機能でUPnPデバイスとして認識
②UPnP機能で通信路を事前に通知
→ルーターが通信路の開閉
③インターネット電話による通話

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

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

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。

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)

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]

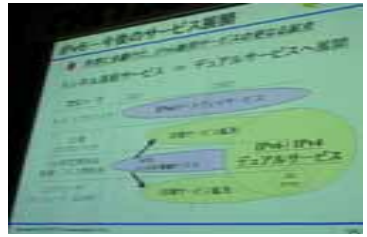
・Windows XPのリモートデスクトップを利用する場合には、静的IPマスカレードで「TCPの3389番ポート」を通すように設定する必要があります。

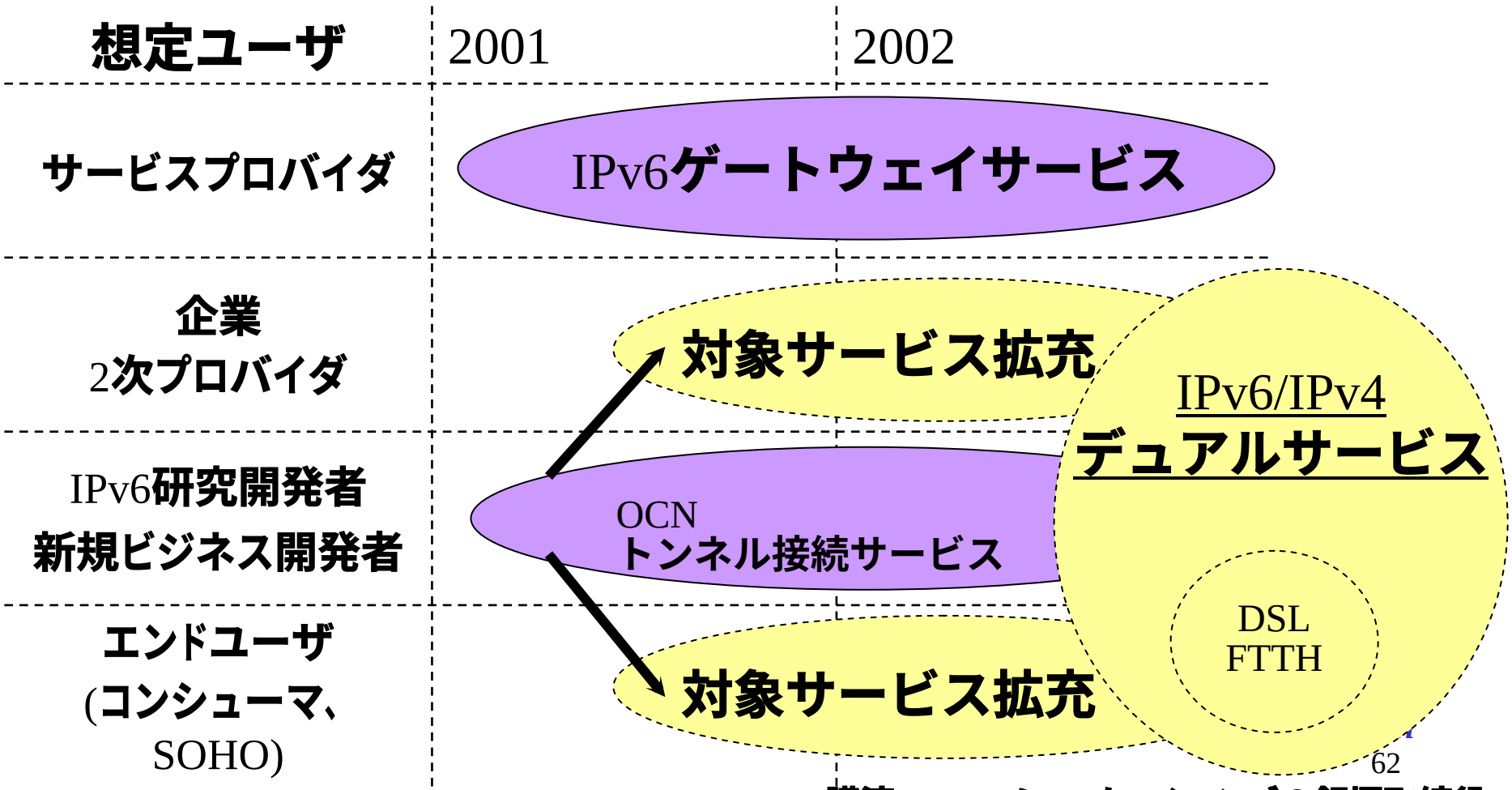
http://www.microsoft.com/japan/windowsxp/pro/business/remote/remotedesktop.asp

NTTコミュニケーションズのIPv6サービス展開

●世界に先駆けた、IPv6商用サービスの更なる拡充

トンネル接続サービス ⇒デュアルサービスへ展開





(NET&COM 2002講演: NTTコミュニケーションズの飯塚取締役)

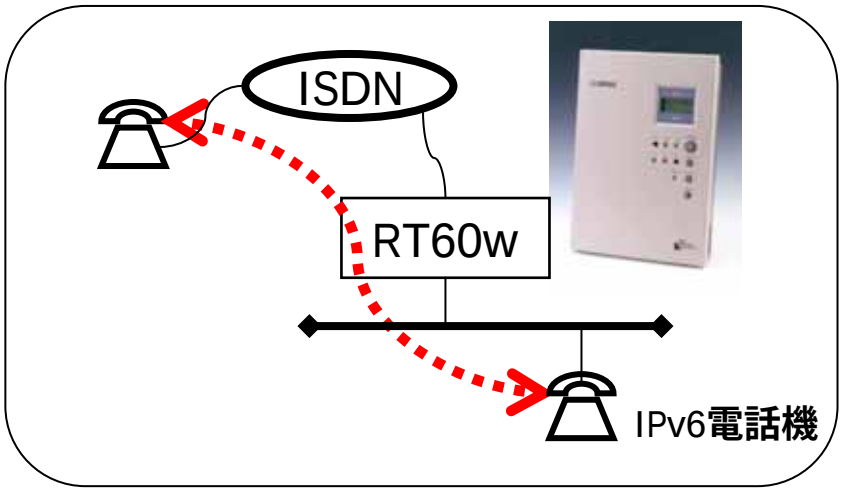
IP電話機のプロトタイプ (ソフトフロント)

http://www.softfront.co.jp/

[特長]

・プロトコル:SIP、IPv6

※RT60wをISDN回線へのIPv6対応VoIPゲートウェイとして利用しプロモーション展開



IPv6対応VoIPゲートウェイ+ IPv6対応IP電話機

IPv6対応IP電話機のプロトタイプ

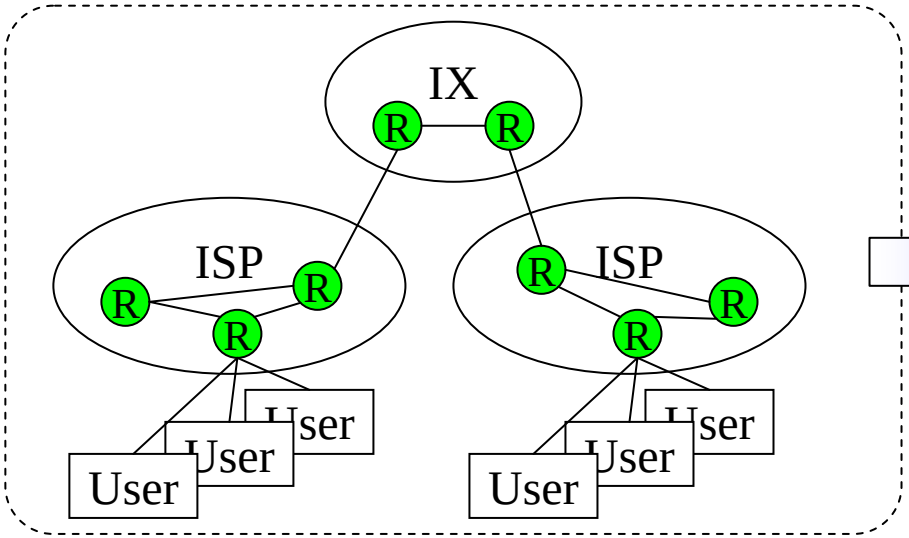
固定グローバルIPアドレスの価値

(NTTPCコミュニケーションズ – InfoSphere の場合)

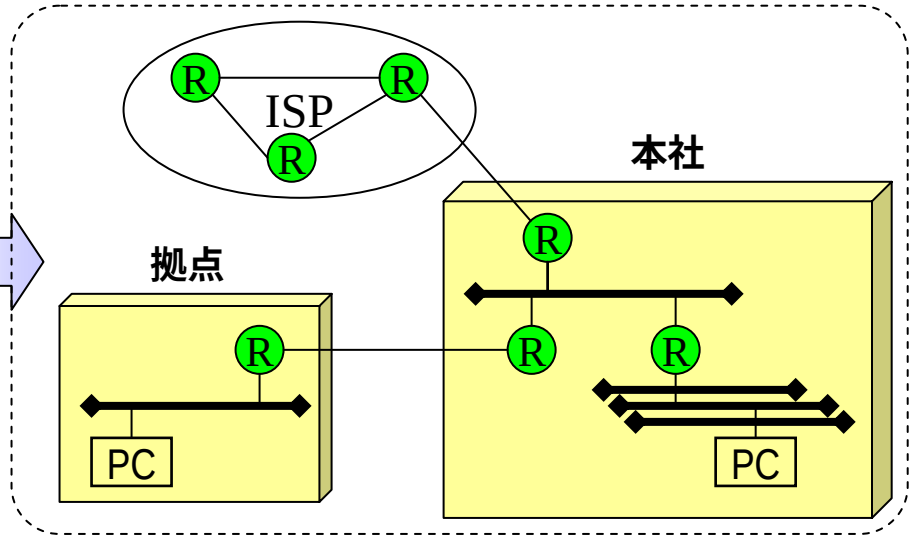
サービス	XpertADSL		Biz ADSL 1	Biz ADSL 8	Biz ADSL 16
支払い方法	クレジットカード	請求書 口座振替	請求書 口座振替	請求書 口座振替	請求書 口座振替
初期費用	無料	2,000円	2,800円	12,000円	12,000円
月額基本料	1,800円	2,600円	6,700円	11,500円	19,800円
IPアドレス割当仕様	不特定の1個を接続時に割り当てる		固定で1個	固定で8個 (実質5個)	固定で16個 (実質15個)
固定料 (1個分)	–	0円	+4,100円	1,780円	1,147円

付録資料

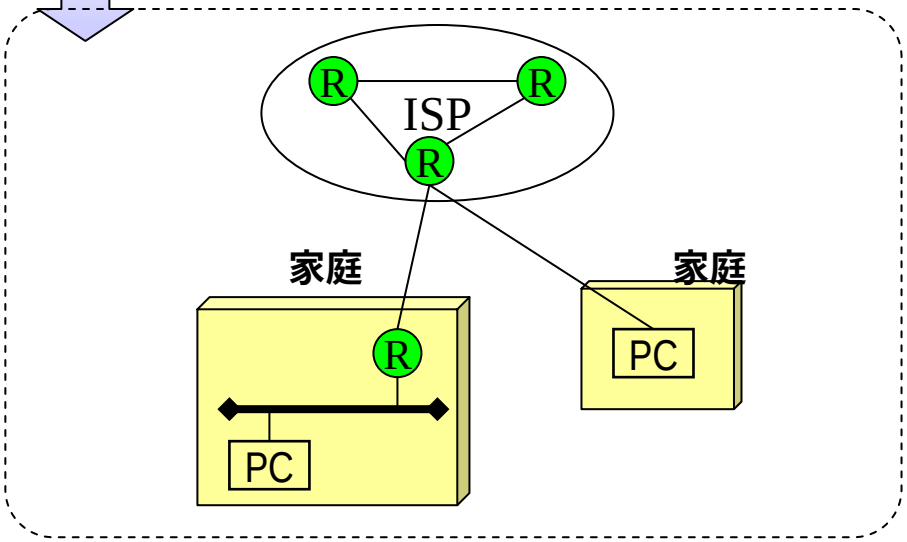
ルーターとは？



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。

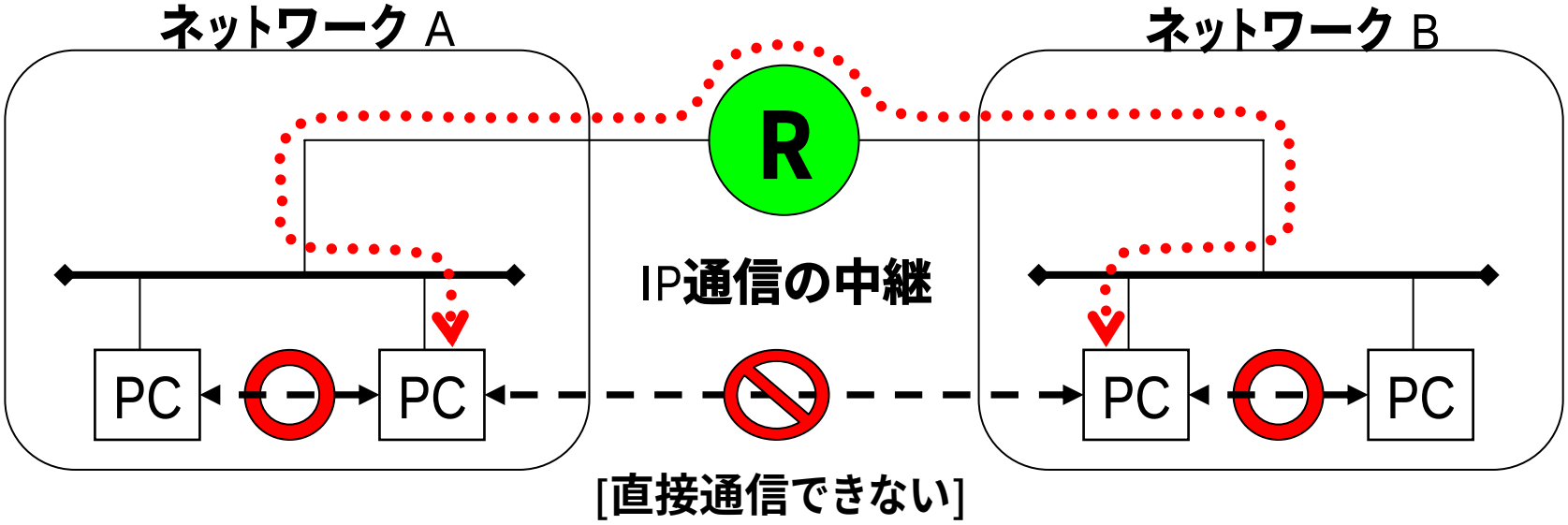
IX: Internet eXchange

JPIX→http://www.jpix.co.jp/

ISP: Internet Service Provider

®: Router

ルーターとは？



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

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
  - 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

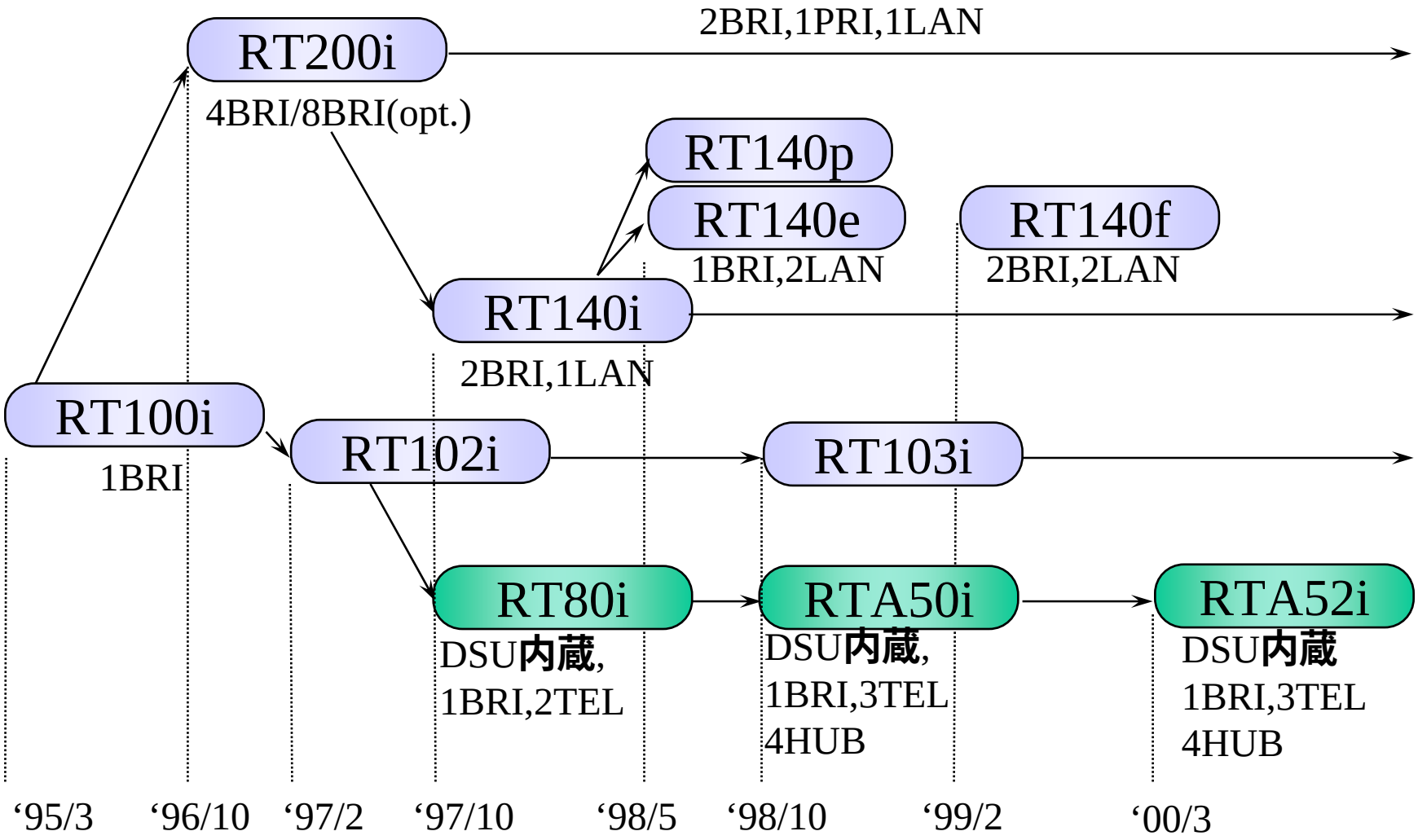
[ネットボランチシリーズ...RTA55i]

- 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)

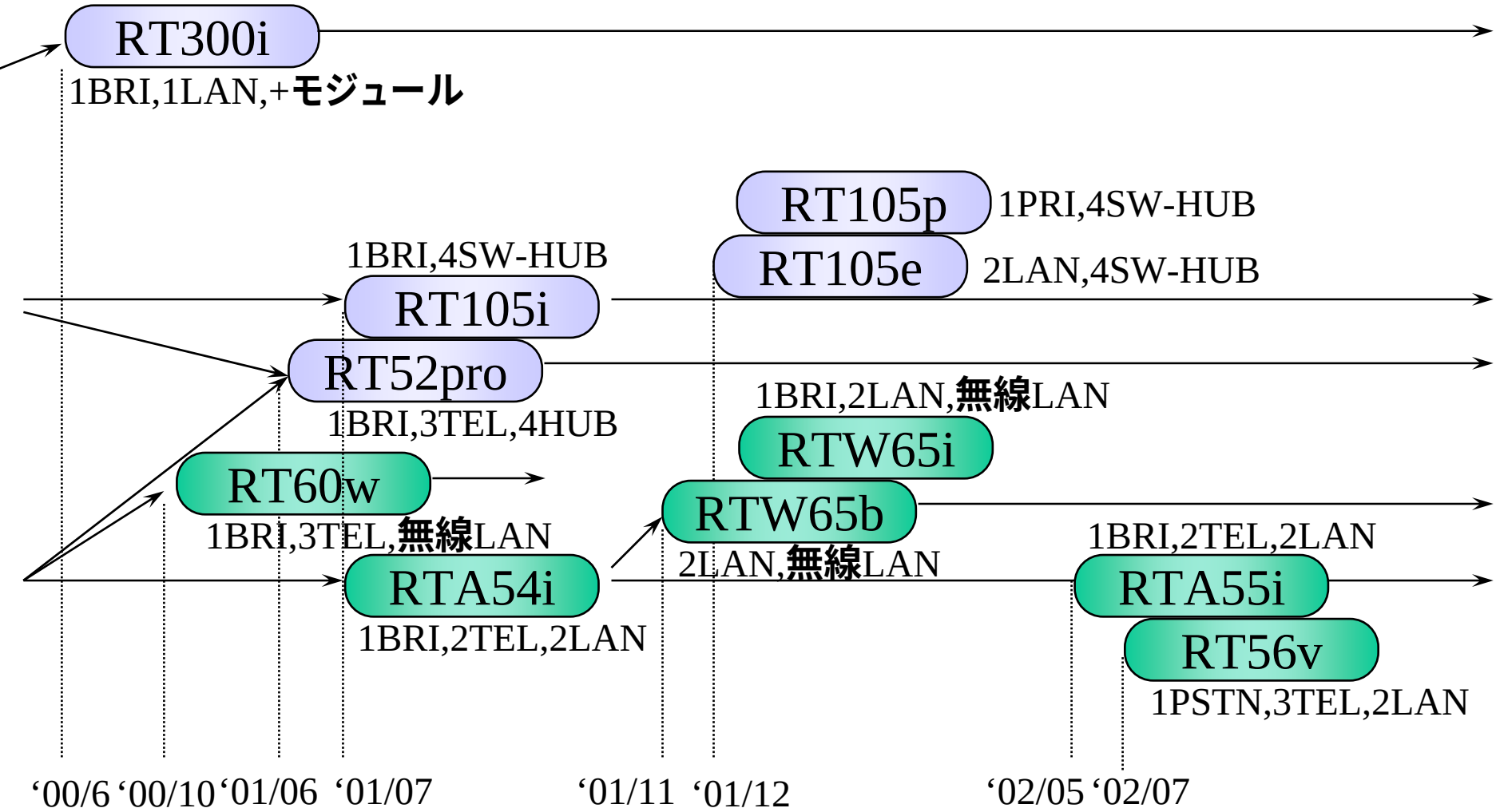
[RTシリーズ]

- 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

ヤマハルータの歩み#1



ヤマハルータの歩み#2



high-end

mid-range

1,000,000

Low-end

200,000

SOHO

個人

企業向けから個人、SOHO向けまで
信頼性と使い易さの実績

RT300 series

RT140 series

RT105 series

Net volante series

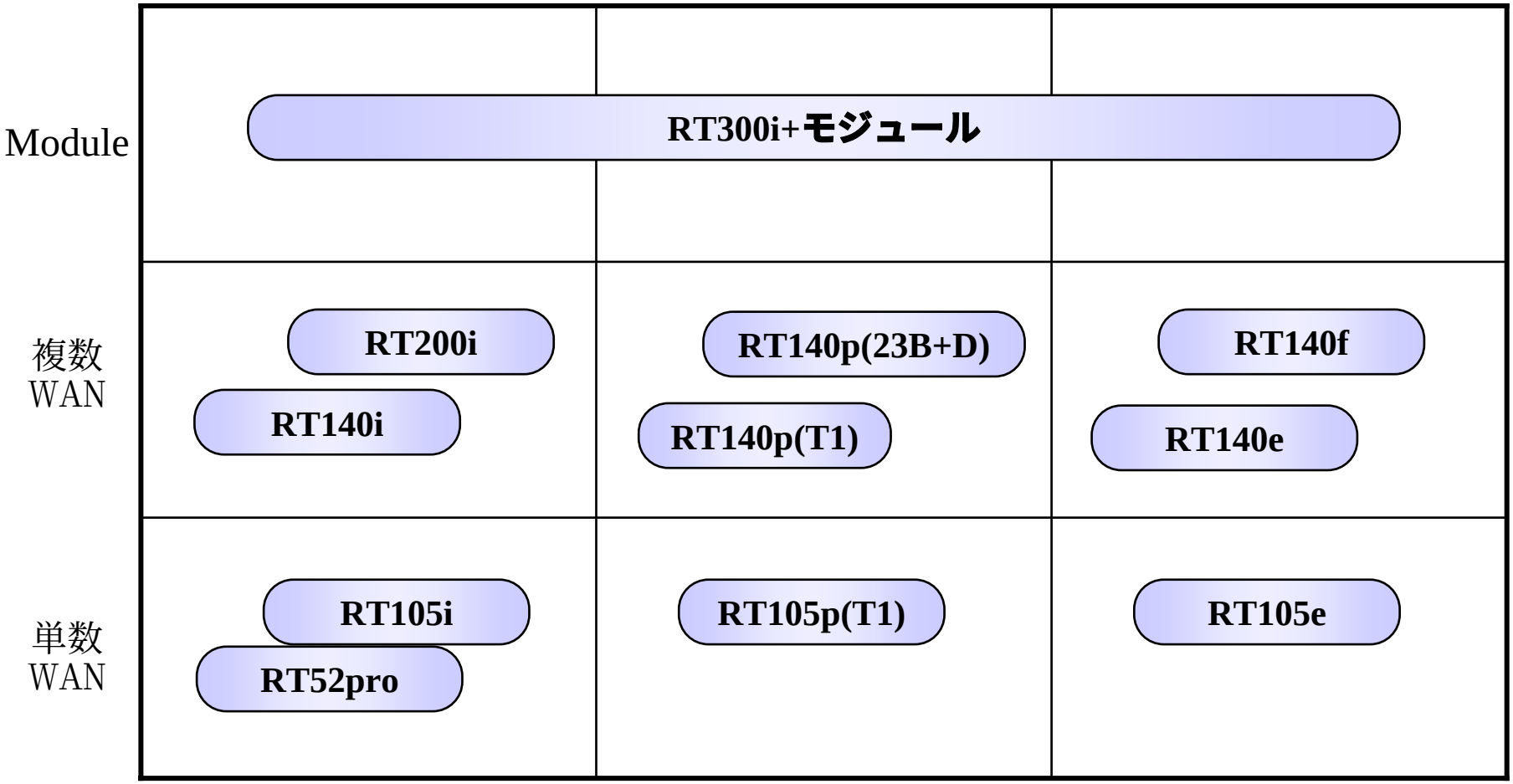
ネットボランチの位置付け

[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)

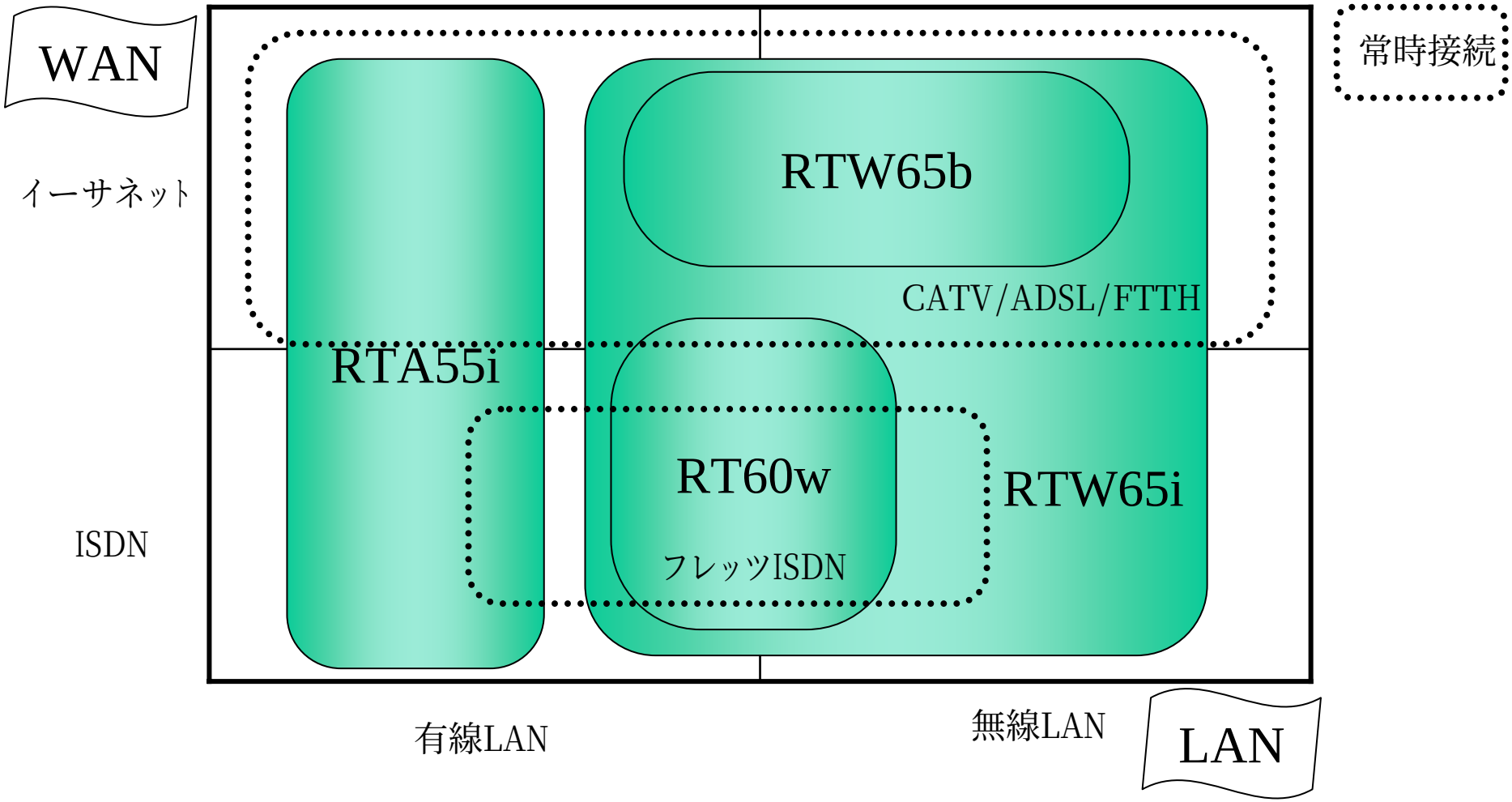
[RT100iの2つの顔]
a) プロバイダ接続用ルータ
b) 拠点側ルータ

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



ブロードバンドへの取り組み

1) ブロードバンド戦略
2) ブロードバンドへの取り組みとネットボランチ
3) Internet VPNへの取り組みとネットボランチ
4) インターネット電話(VoIP)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
- ルーターに求められるセキュリティ・ゲートウェイ機能

「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

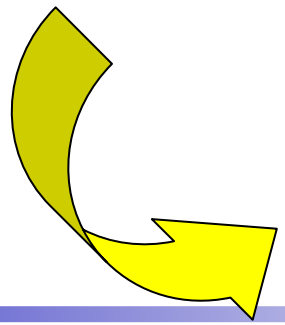
※柔軟性と多機能→トータルバランス

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
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
2002年1月		○RTW65i発売 ・RT105e/RT105p発売
2002年5月		○RTA55i発売

ネットボランチの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
- …



[ネットボランチ]
- インターネット電話(VoIP)
- 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

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年春		・VPNプロトコル: PPTP/L2TP対応

IPsec Version 2 RFC:RFC2401～RFC2409、RFC2451

ネットボランチのInternet VPNの要素

[必須]
- VPNプロトコル:PPTP
- 暗号アルゴリズム:RC4
- 相互接続性
  Microsoft VPNアダプタ

・LAN間接続VPN
・リモートアクセスVPN

[ネットボランチ]
- ファイアウォール機能
- VPNパススルー
- RTシリーズへのキャリアパス
  IPsec Version 2 RFC対応

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4月		・ネットボランチDNSサービス β版
2002年5月		○RTA55i発売(予定)

http://www.yamaha.co.jp/news/01121201.html

ネットボランチ RTA55i&RT56v の 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

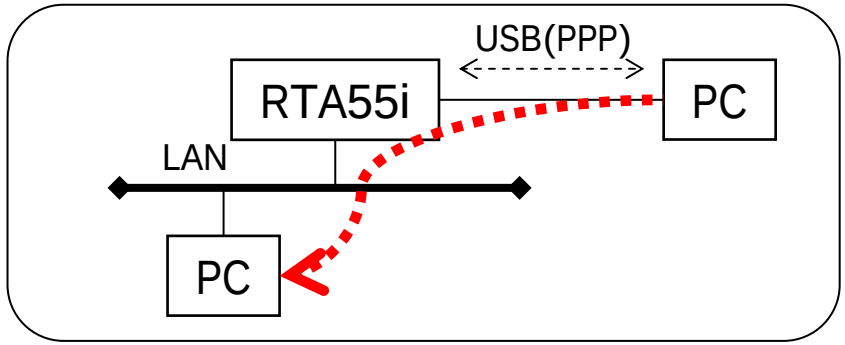
	RTA55i	RT56v	RTW65b	RTW65i
ISDN回線	1	–	–	1
アナログ回線	–	1	–	–
TELポート	2	3	–	3
WANポート	1	1	1	1
LANポート	4 (スイッチ)	4 (スイッチ)	1	1
無線LAN (IEEE 802.11b)	–	–	1	1
USBポート	1	–	1	1
LED	8(前)+4(後)	6(前)+5(後)	7	9

NetVolanteにおけるUSBポート

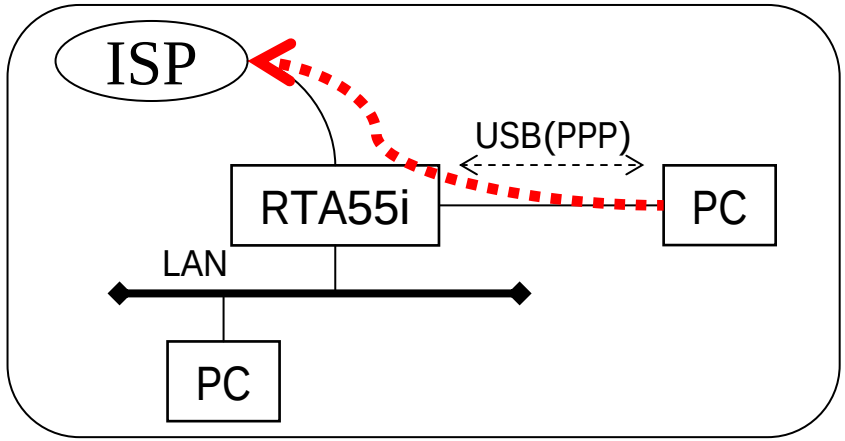
[用途]

- **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	×

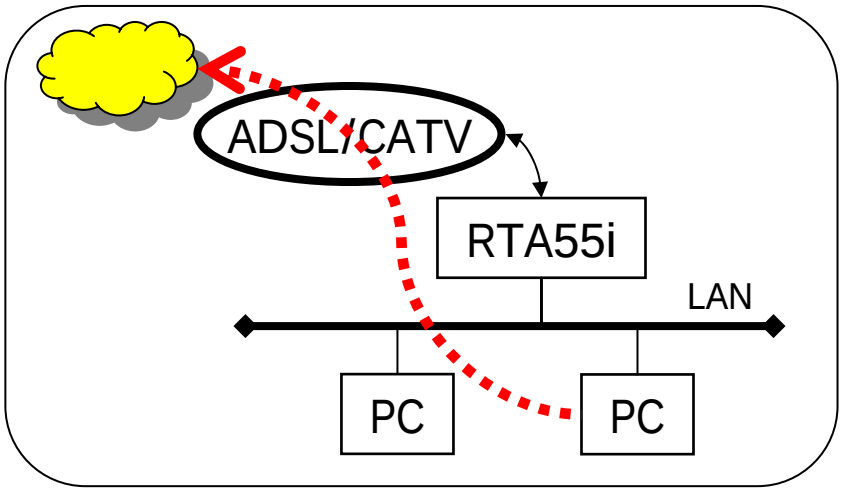


USBの擬似LAN→LANアクセス

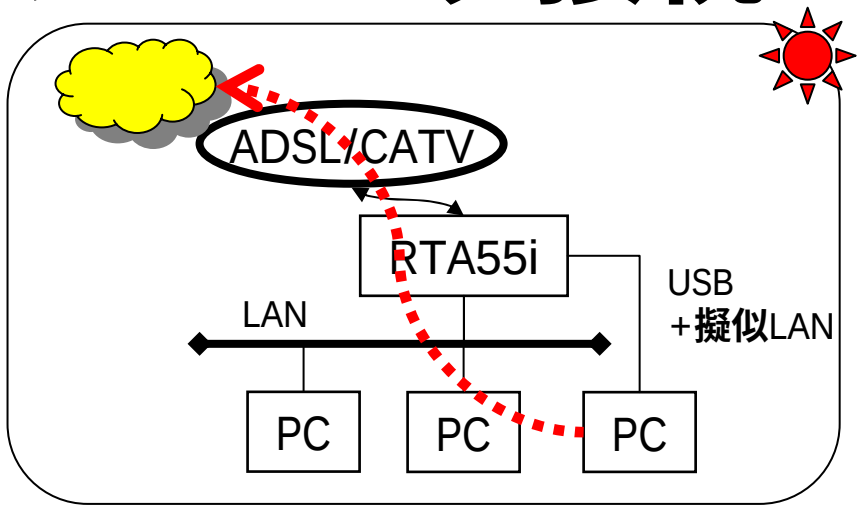


USBの擬似LAN→インターネットアクセス

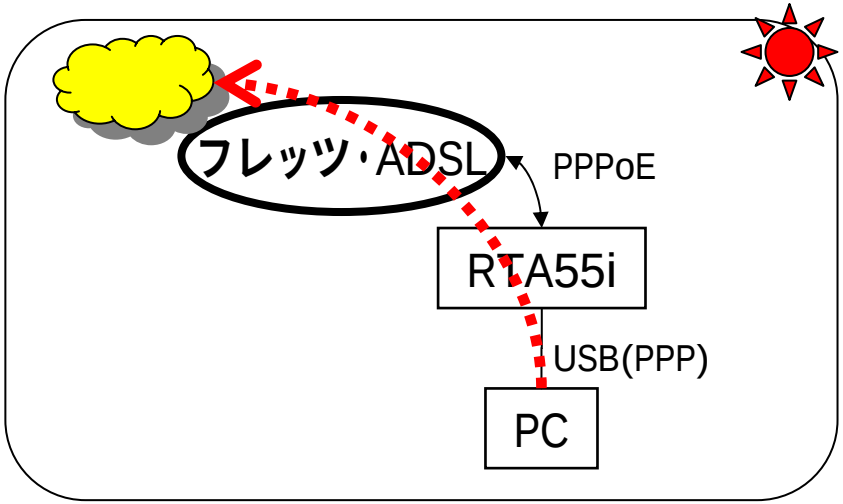
ブロードバンドのプロバイダ接続



ADSL/CATV**プロバイダ接続**(LAN)

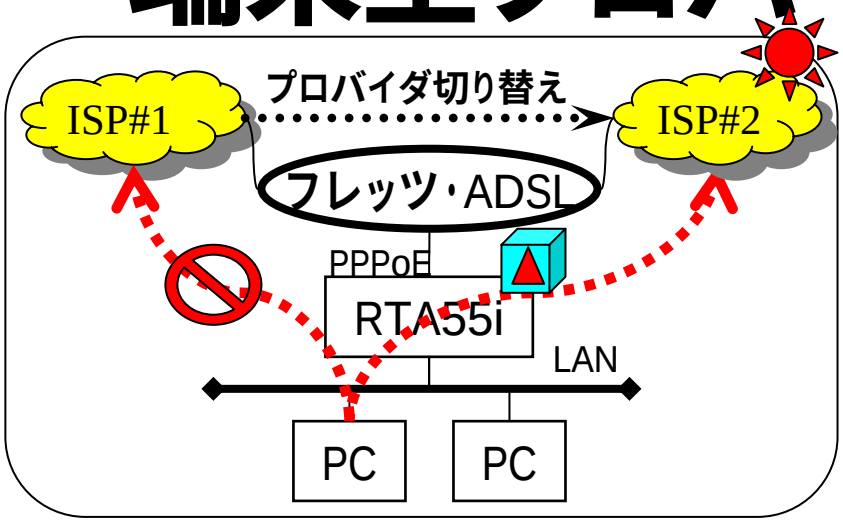


ADSL/CATV**プロバイダ接続**(USB**の擬似**LAN)

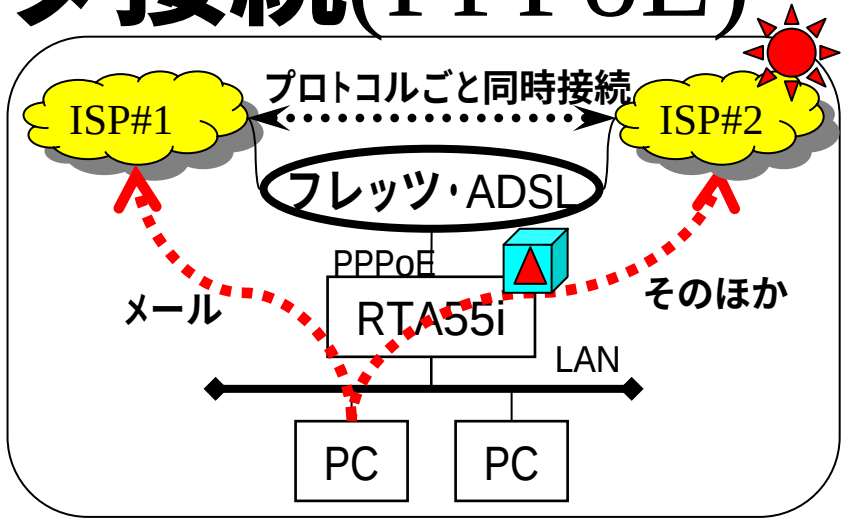


ブロードバンドTA(**フレッツ**・ADSL,USB)

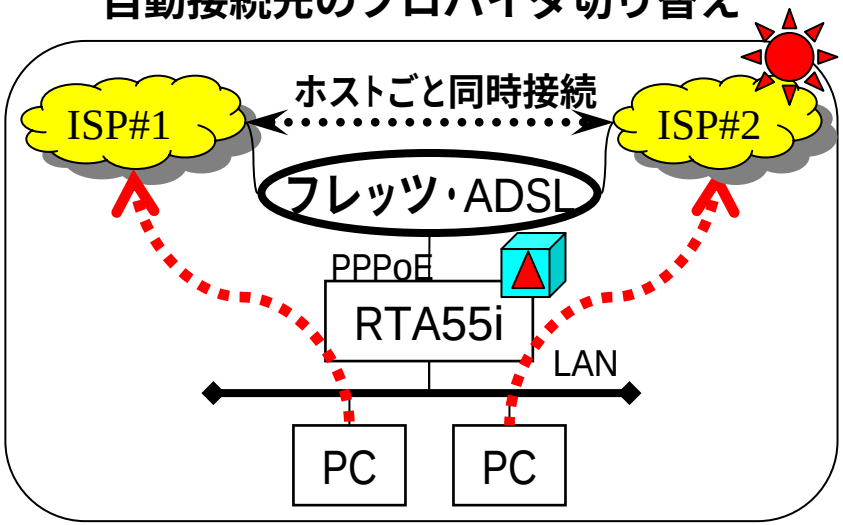
端末型プロバイダ接続(PPPoE)



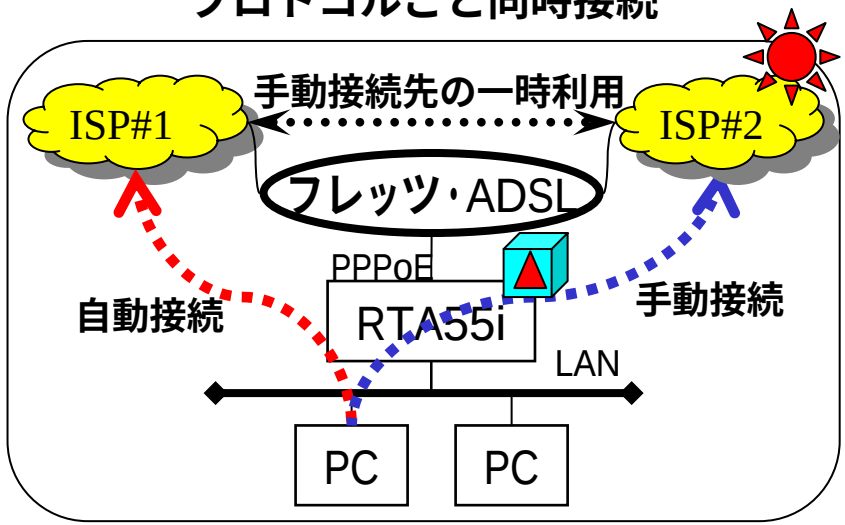
自動接続先のプロバイダ切り替え



プロトコルごと同時接続

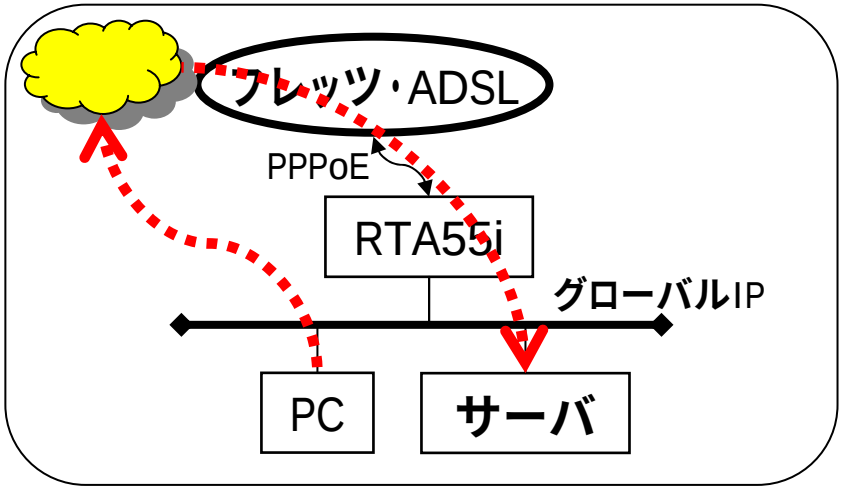


ホストごと同時接続

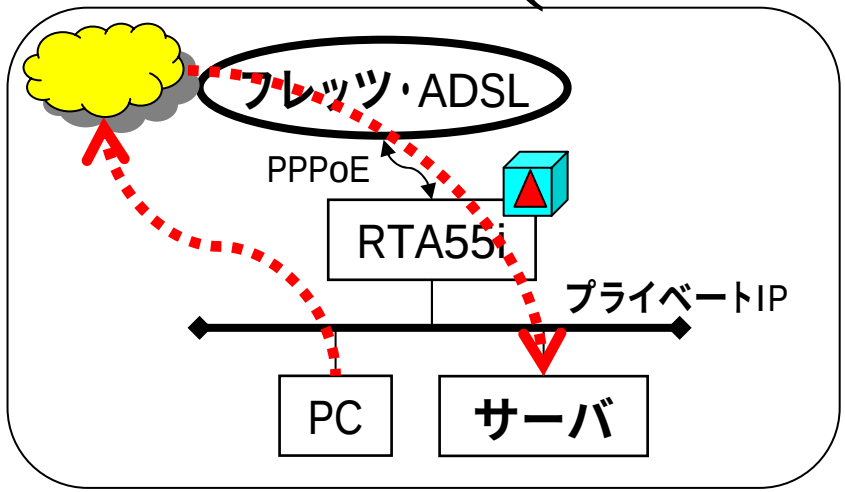


手動接続先の一時切り替え

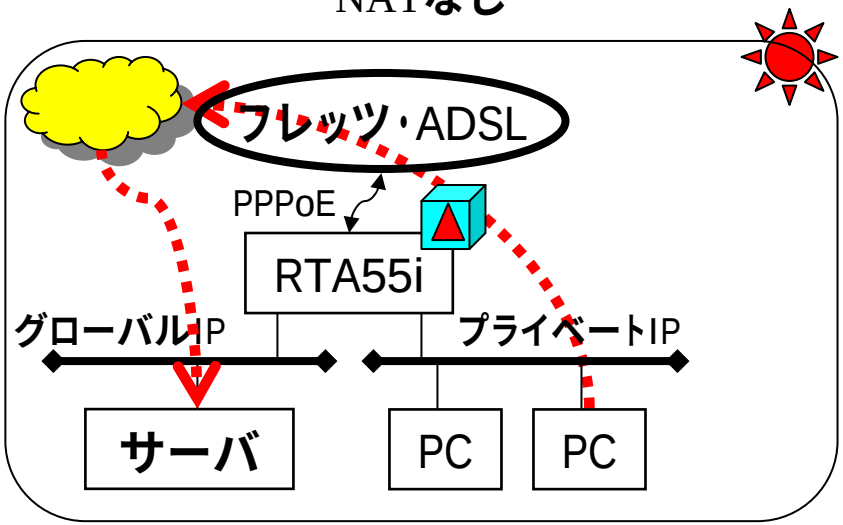
ネットワーク型プロバイダ接続(PPPoE)



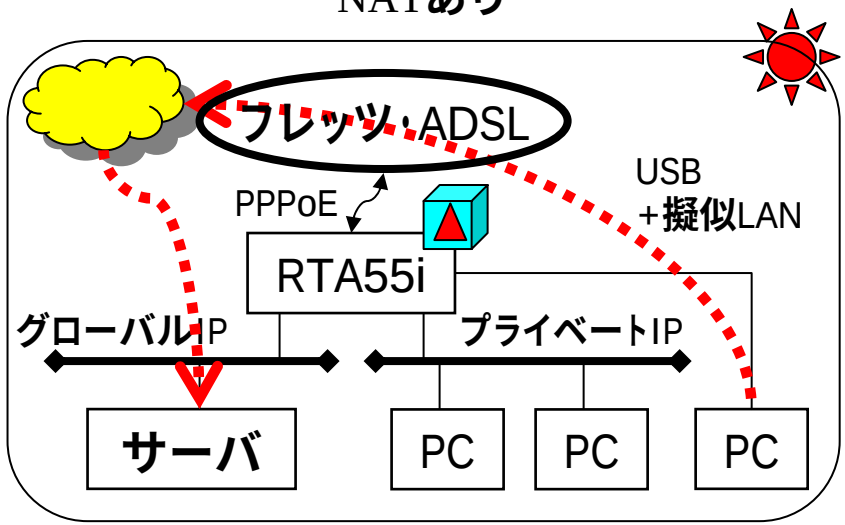
NATなし



NATあり

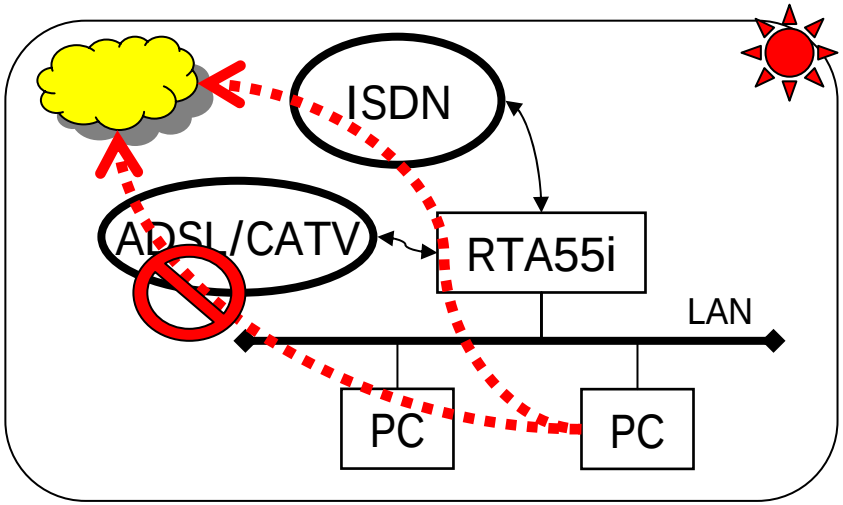


NATなし&あり(primary/secondary)

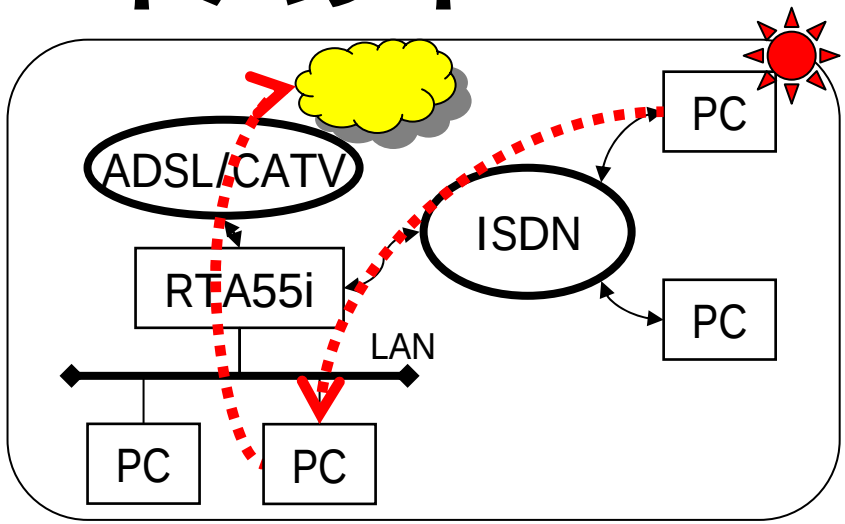


NATなし&あり(USB+擬似LAN)

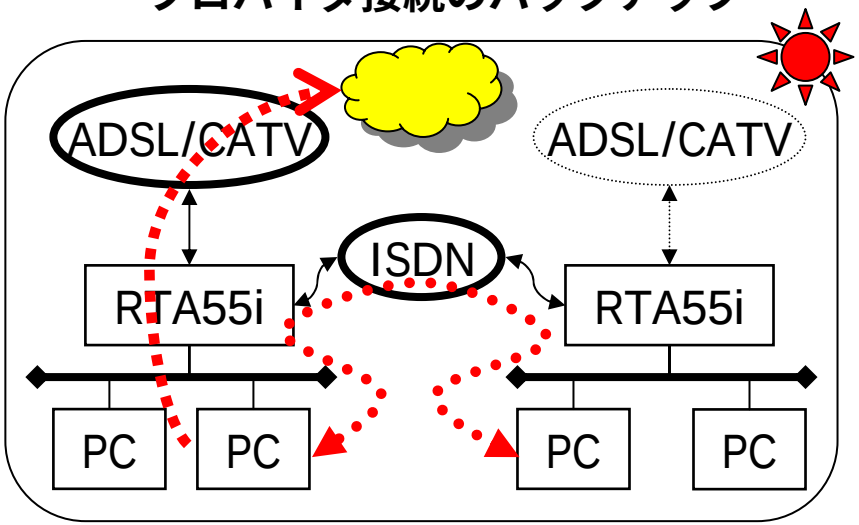
ISDN+ブロードバンド



プロバイダ接続のバックアップ

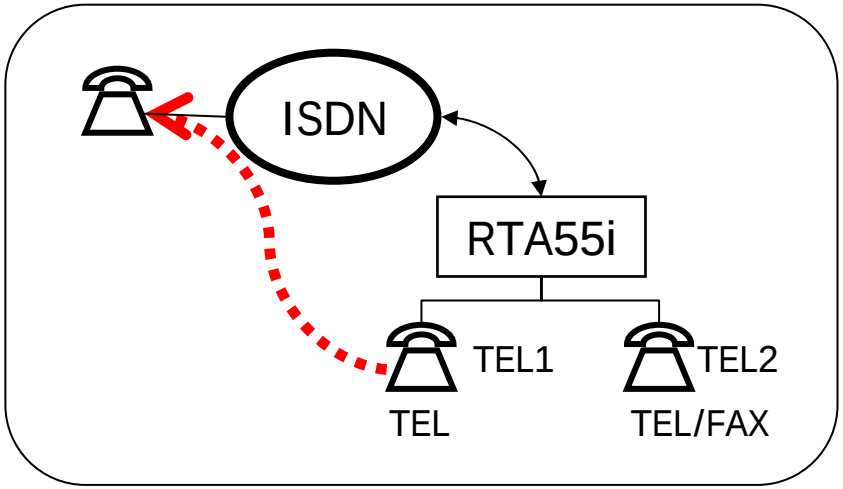


プロバイダ接続+リモートアクセスサーバ

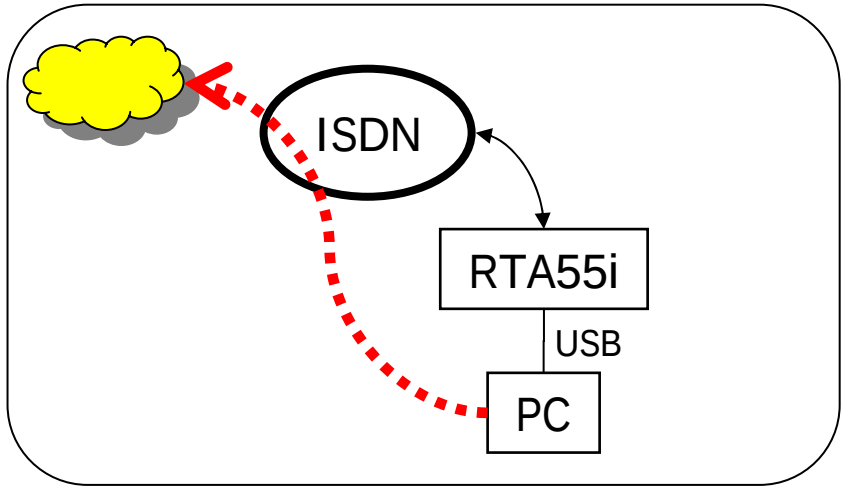


プロバイダ接続+LAN間接続

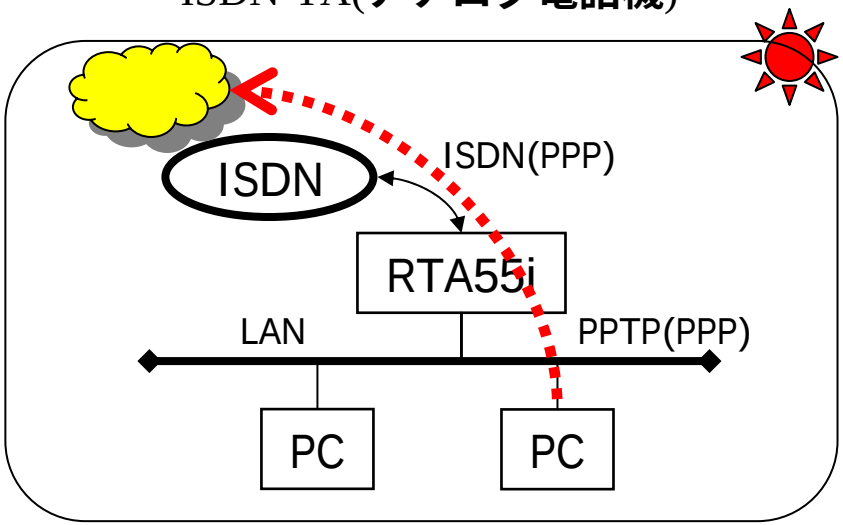
ISDN回線の基本



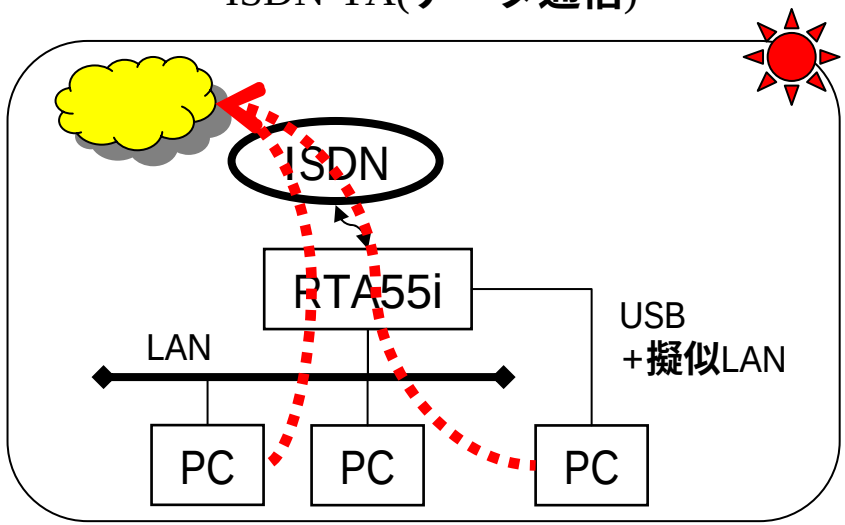
ISDN-TA(**アナログ電話機**)



ISDN-TA(**データ通信**)

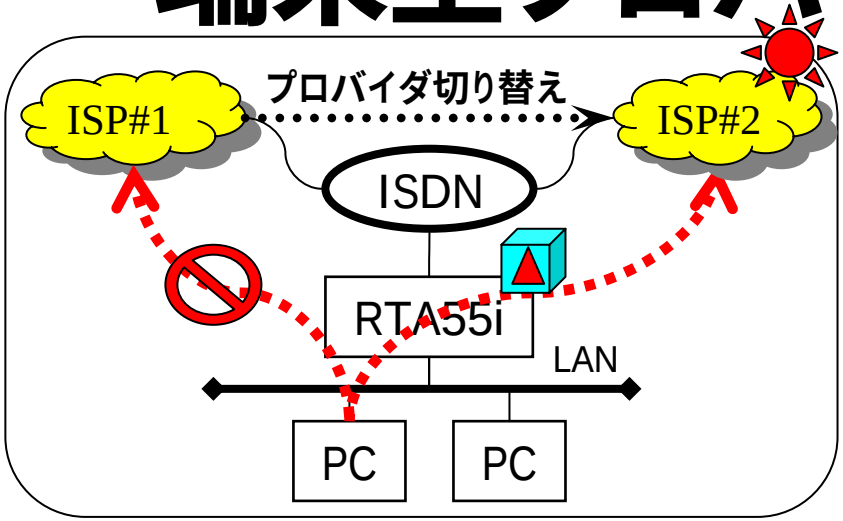


LAN-TA (PPTP client,MS VPN Adapter)

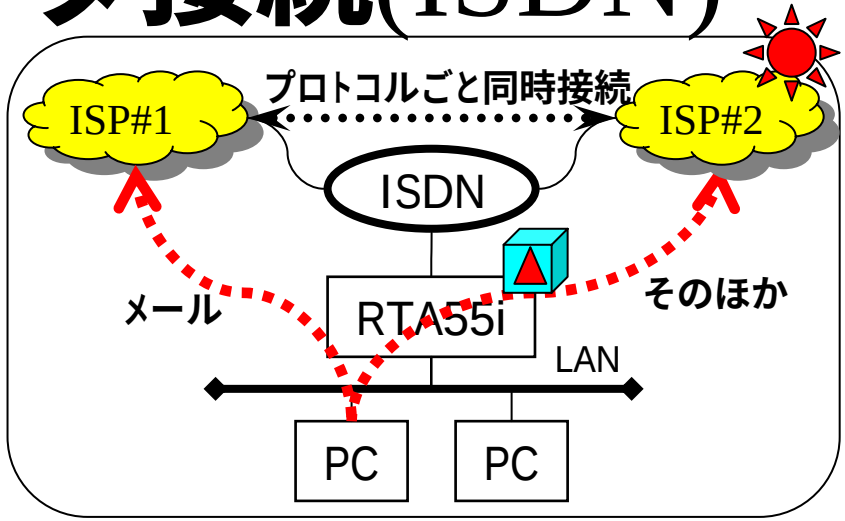


ダイヤルアップ・プロバイダ接続(LAN/USB)

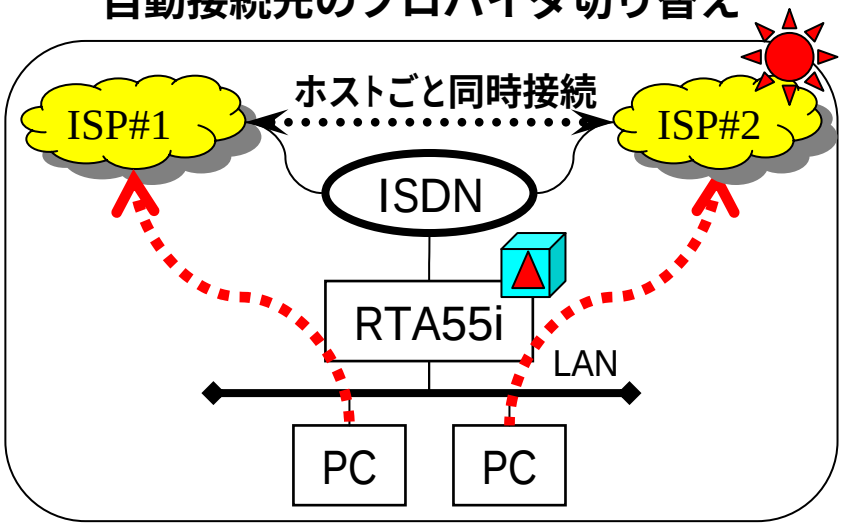
端末型プロバイダ接続(ISDN)



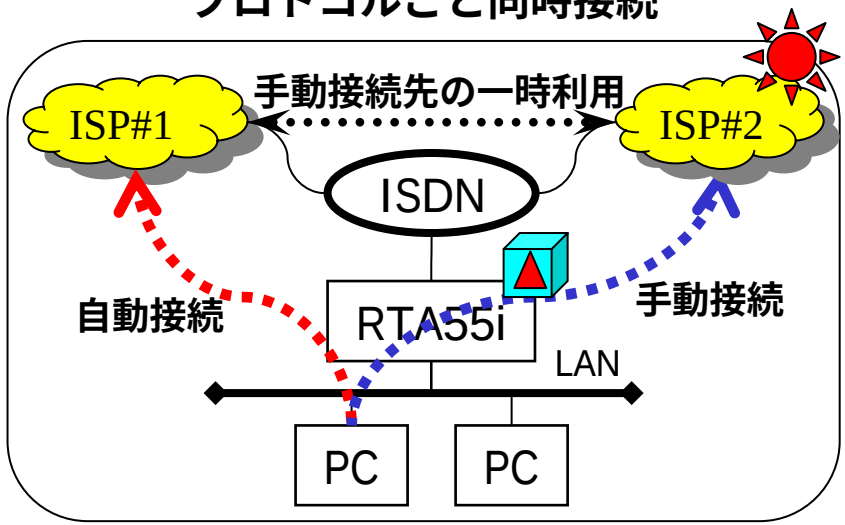
自動接続先のプロバイダ切り替え



プロトコルごと同時接続

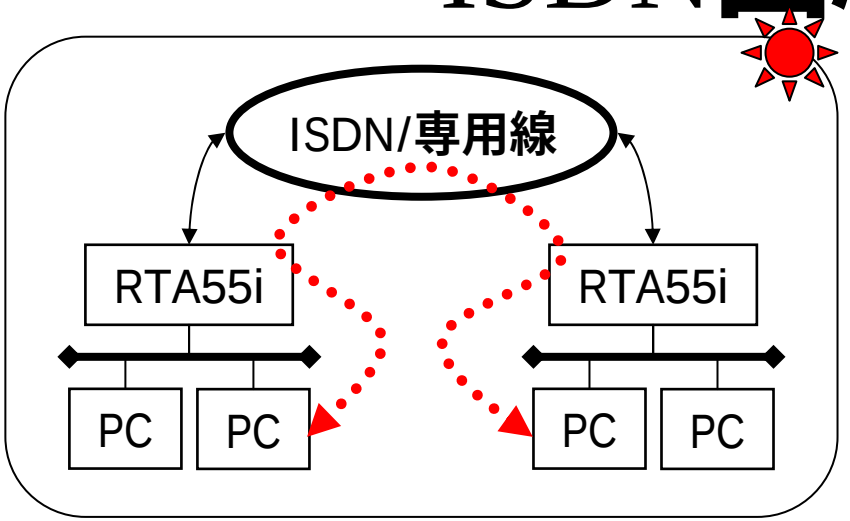


ホストごと同時接続

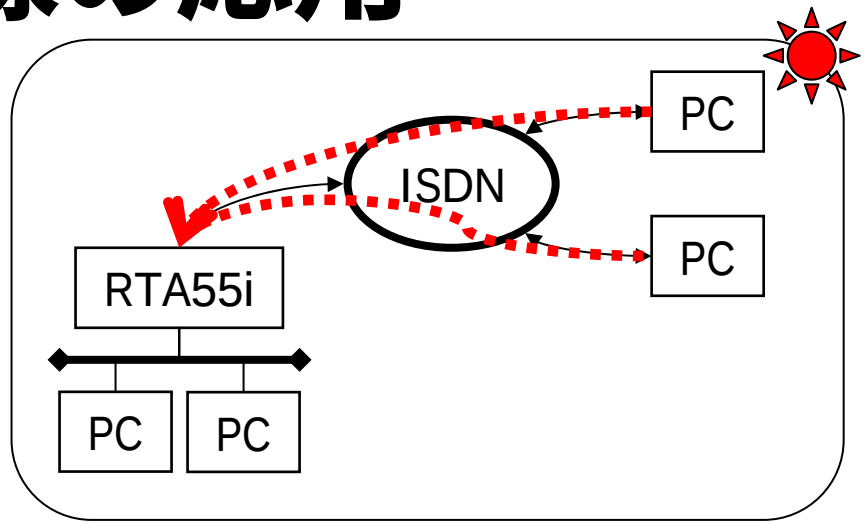


手動接続先の一時切り替え

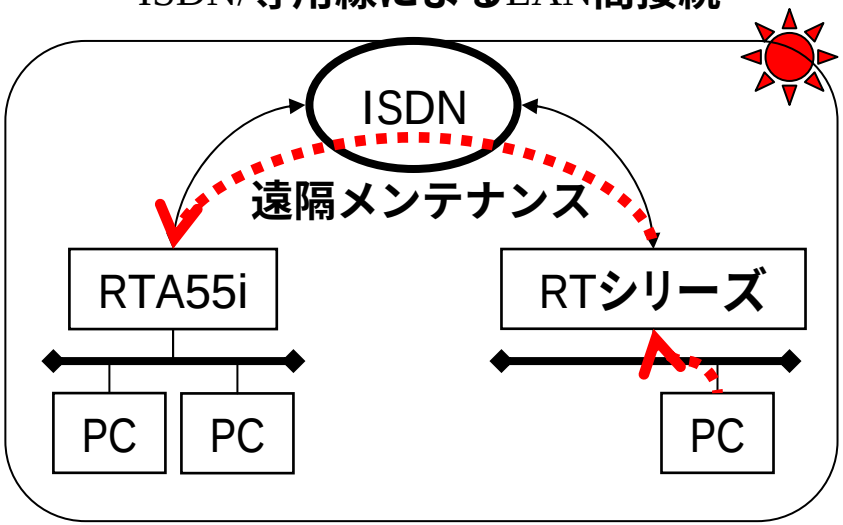
ISDN回線の応用



ISDN/専用線によるLAN間接続

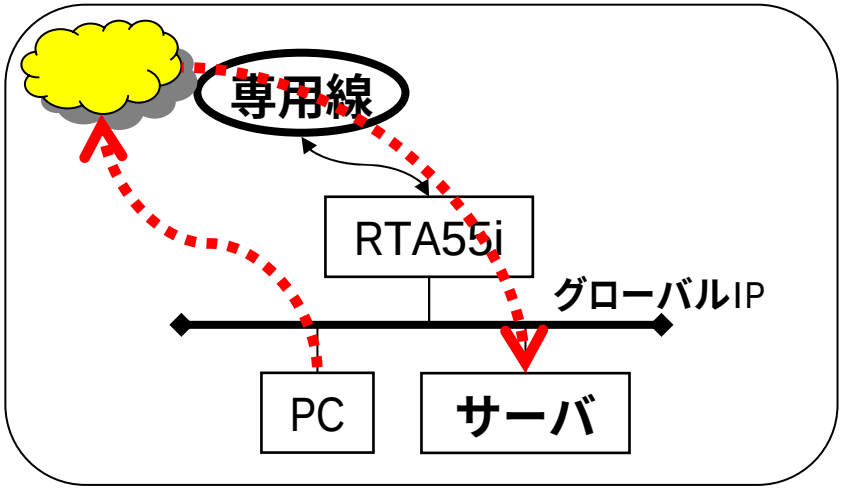


ダイヤルアップサーバ

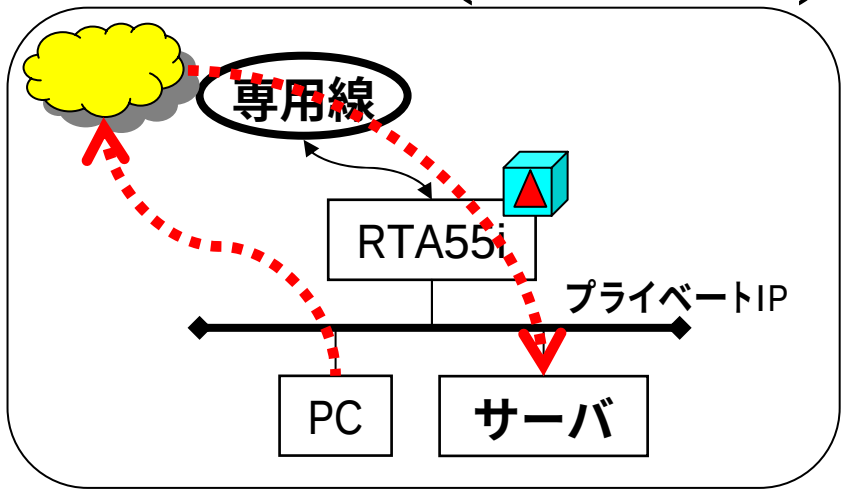


リモートセットアップ

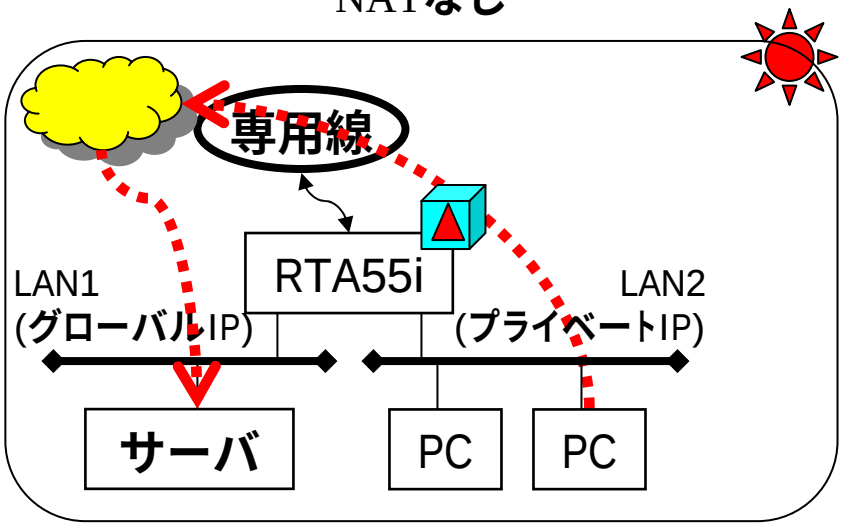
ネットワーク型プロバイダ接続(専用線)



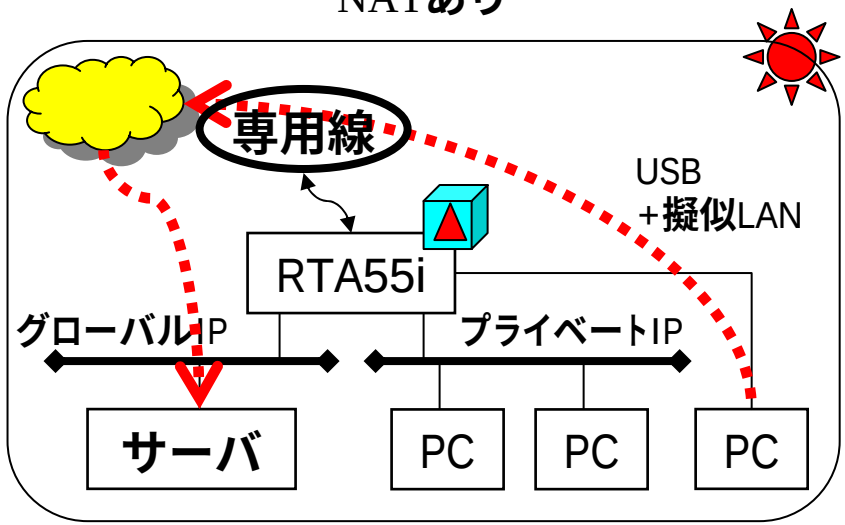
NATなし



NATあり



NATなし&あり(LAN1/LAN2)



NATなし&あり(USB+擬似LAN)

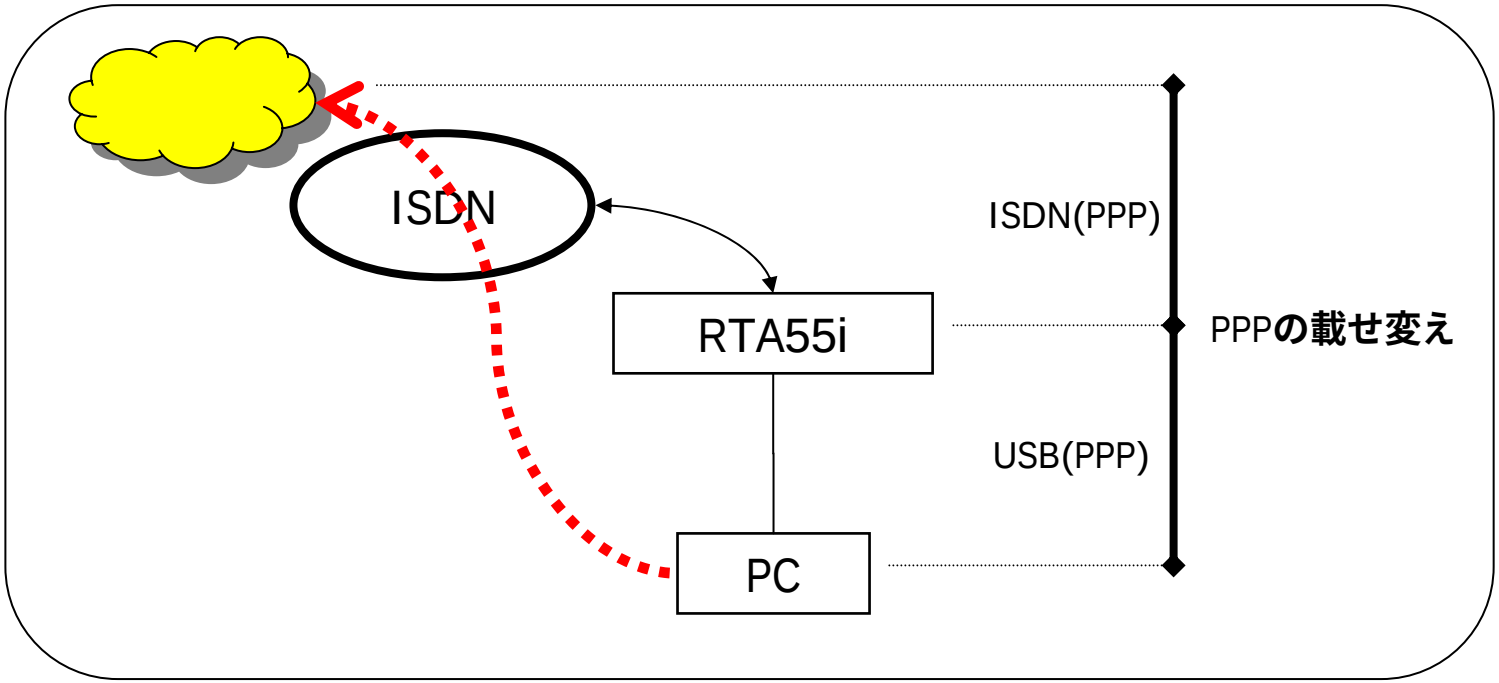
ネットボランチのネットアプリ対応

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)

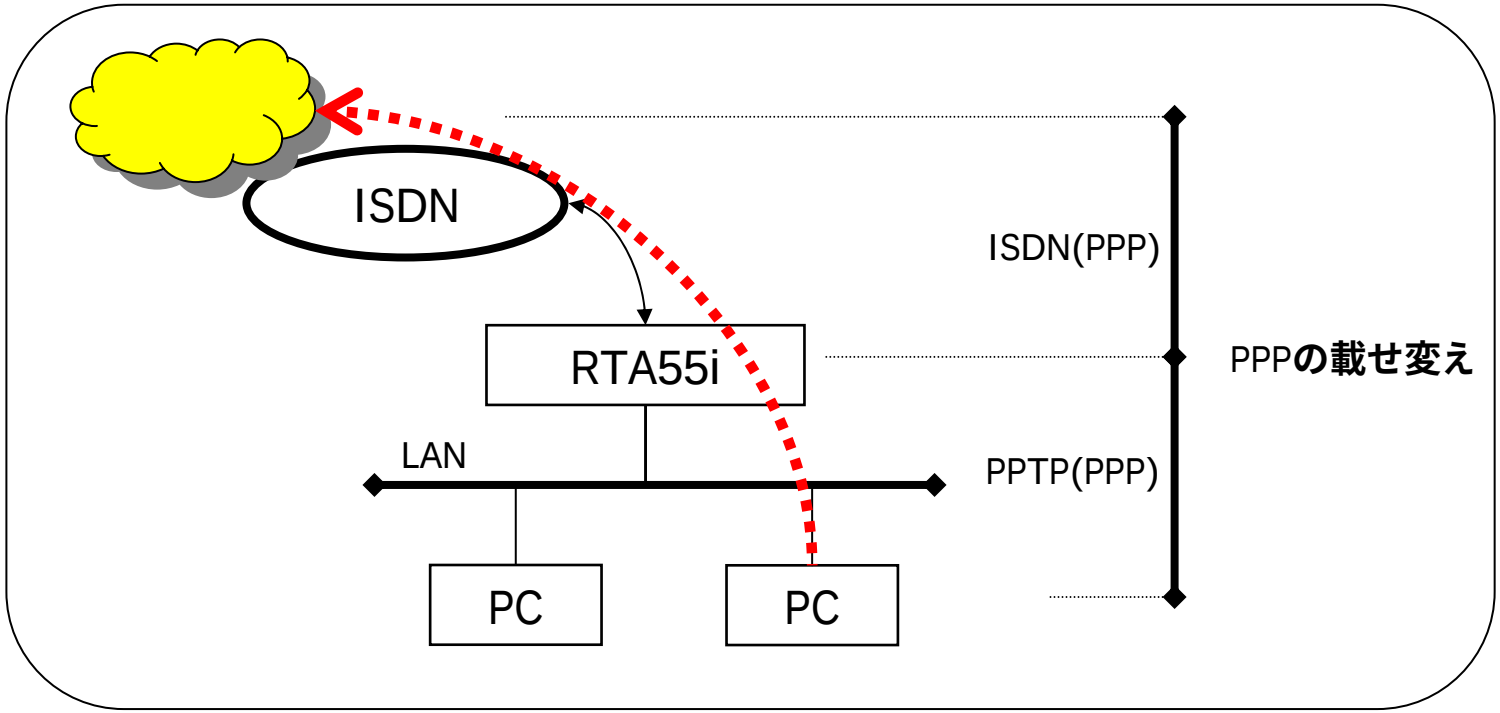
	RTA55i	RT56v
ISDNポート	OK	×
USBポート	OK	×



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

LAN-TA機能

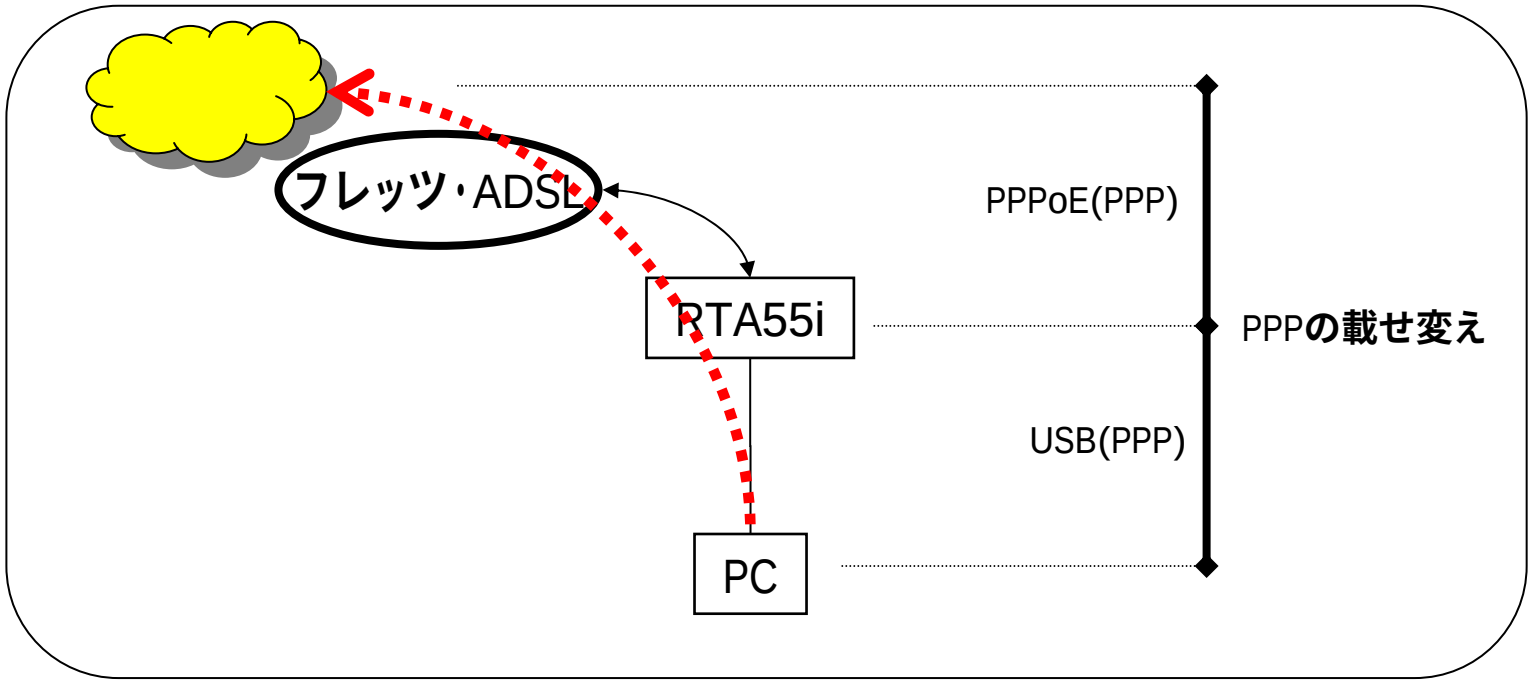
	RTA55i	RT56v
ISDNポート	OK	×



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

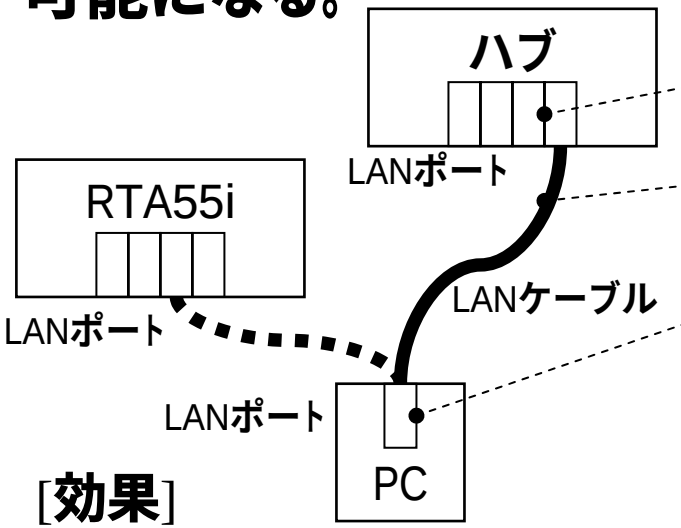
	RTA55i	RT56v
USBポート	OK	×



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

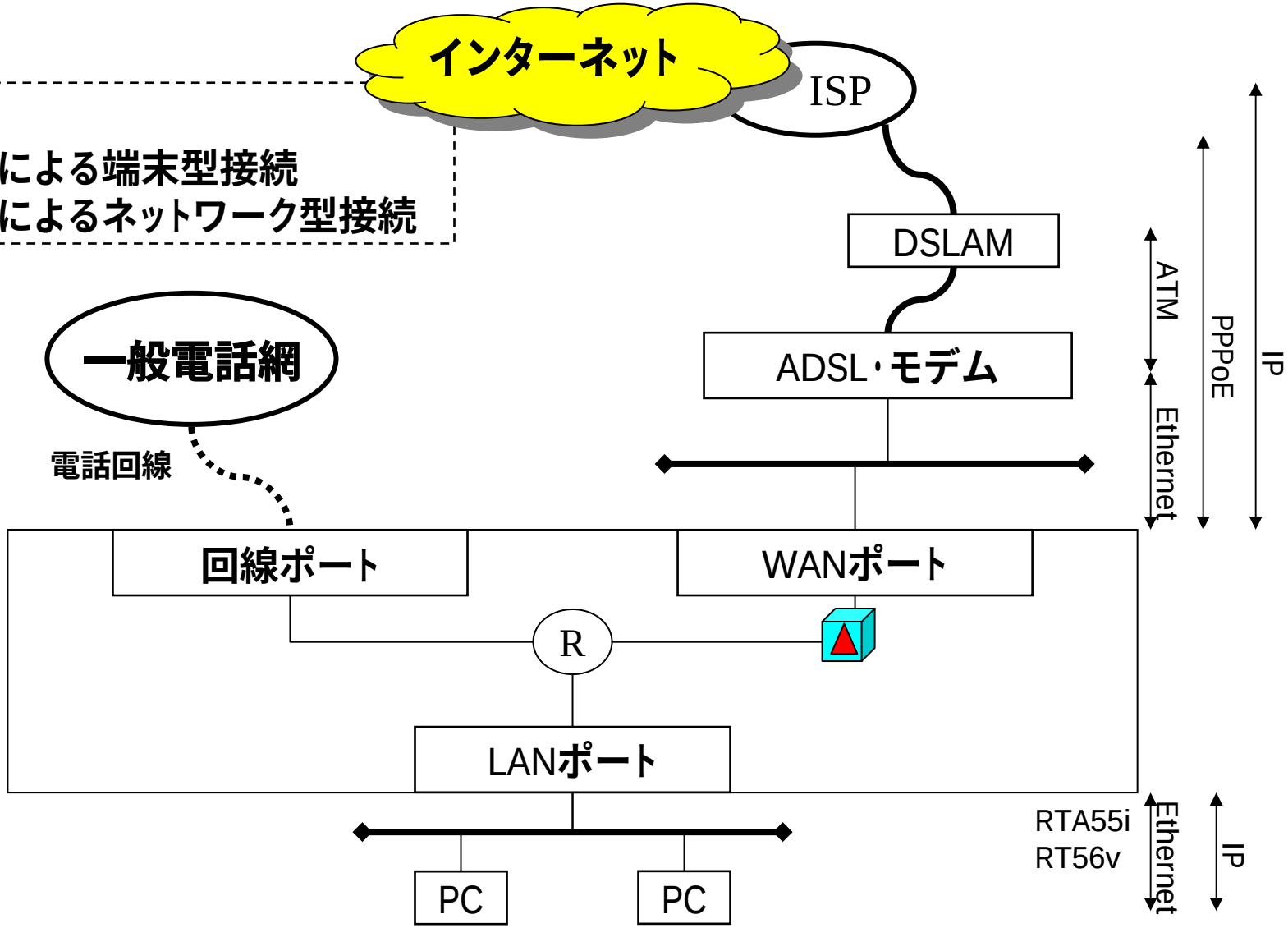
[ハブの記号の'='と'X']
- '=' : MDI　→端末に接続するポート
- 'X' : MDI-X→ハブに接続するポート(Uplink)

ネットボランチ RTA55i&RT56v の インターネット接続

		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	OK	×

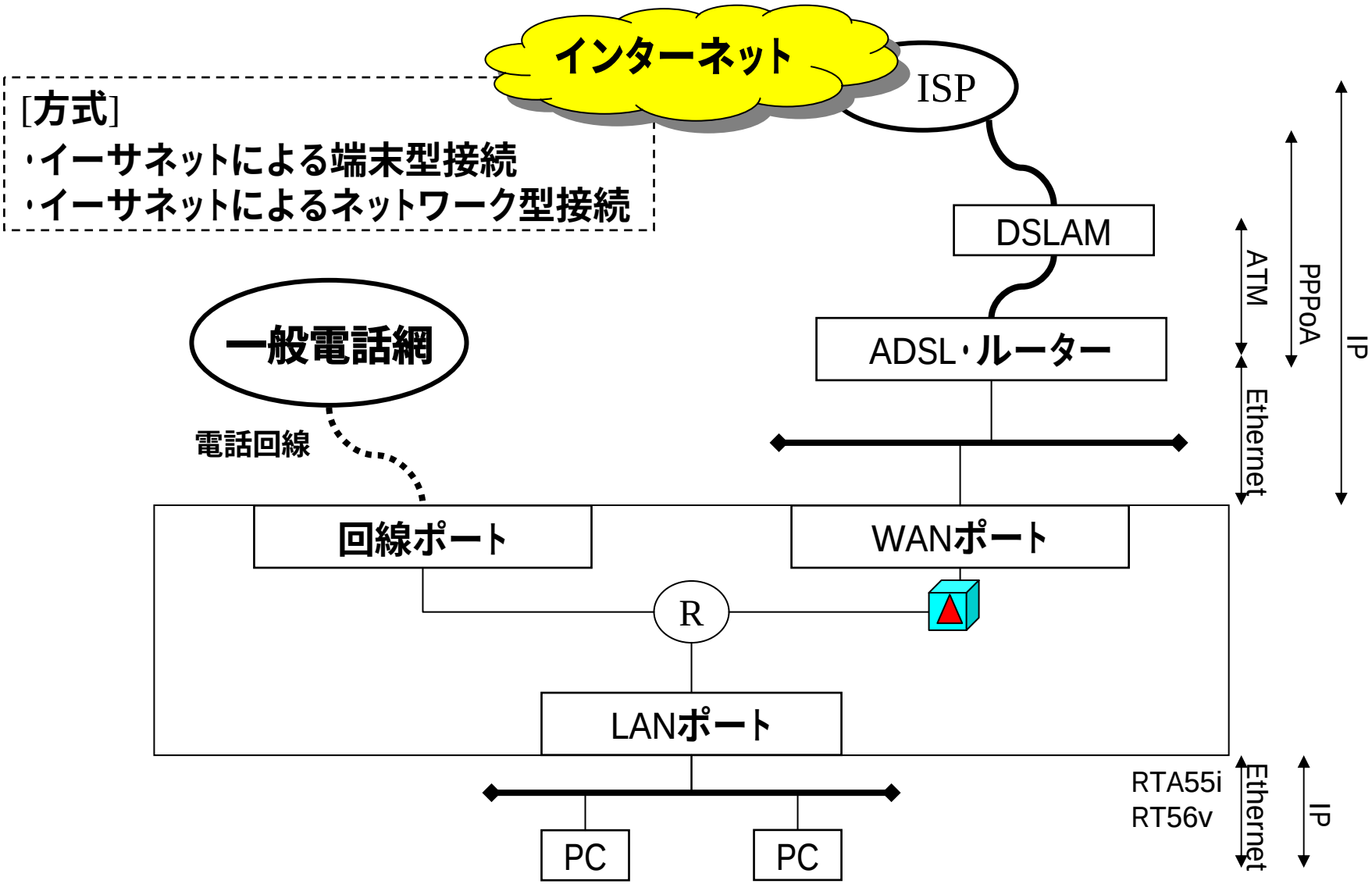
ADSLによるプロバイダ接続#1

[方式]
・PPPoEによる端末型接続
・PPPoEによるネットワーク型接続



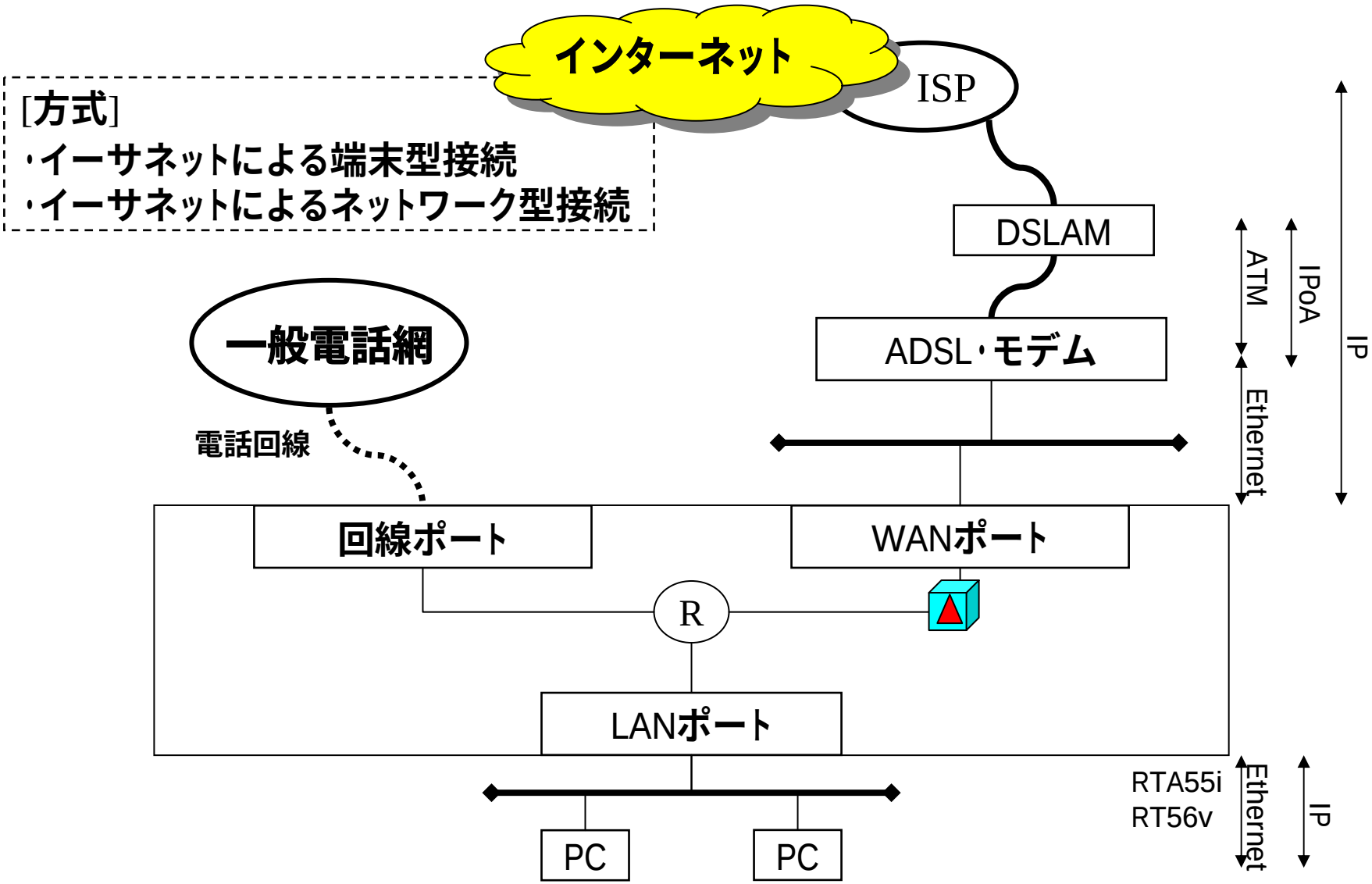
http://www.yamaha.co.jp/news/01121201.html

ADSLによるプロバイダ接続#2



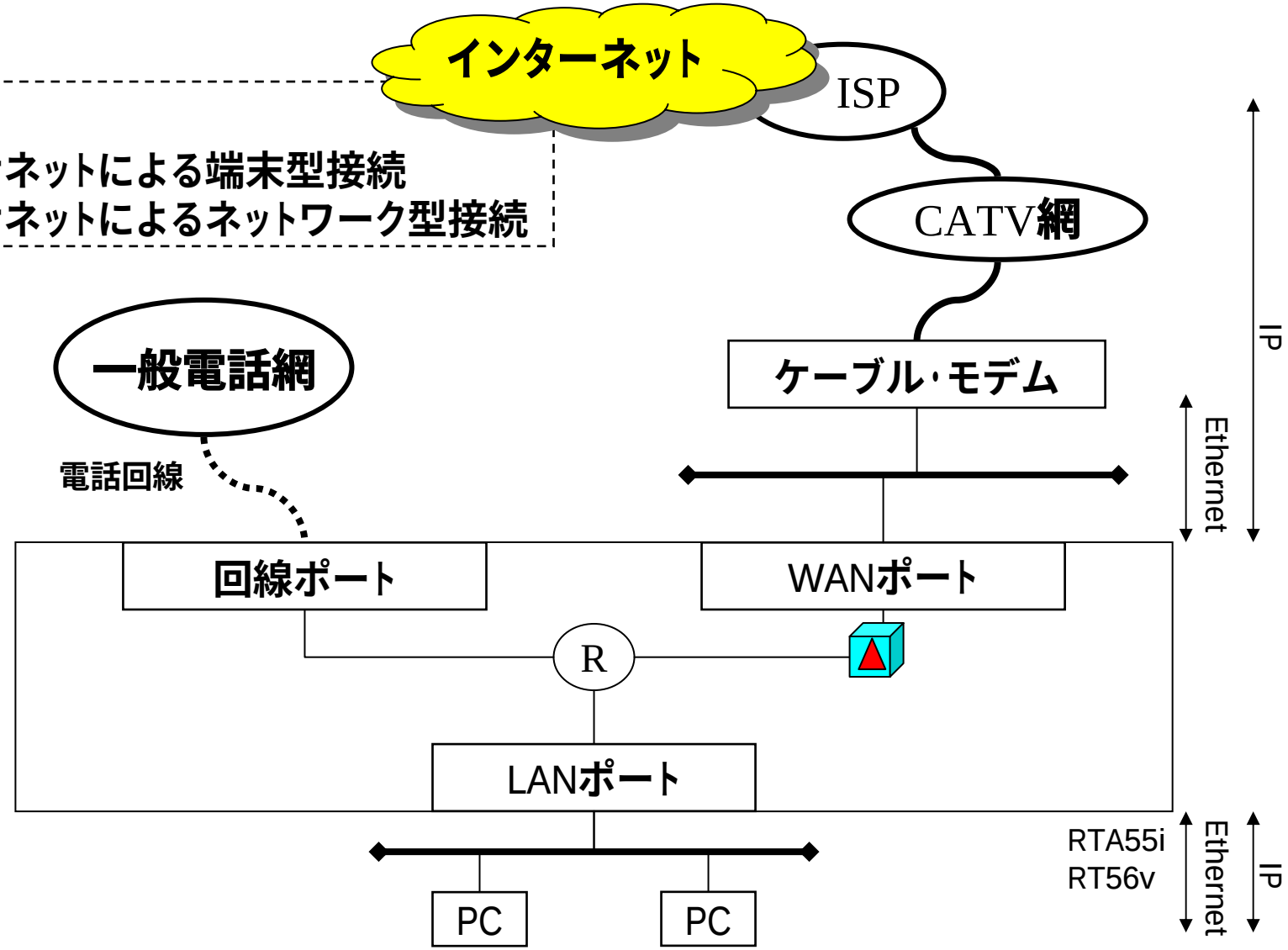
http://www.yamaha.co.jp/news/01121201.html

ADSLによるプロバイダ接続#3



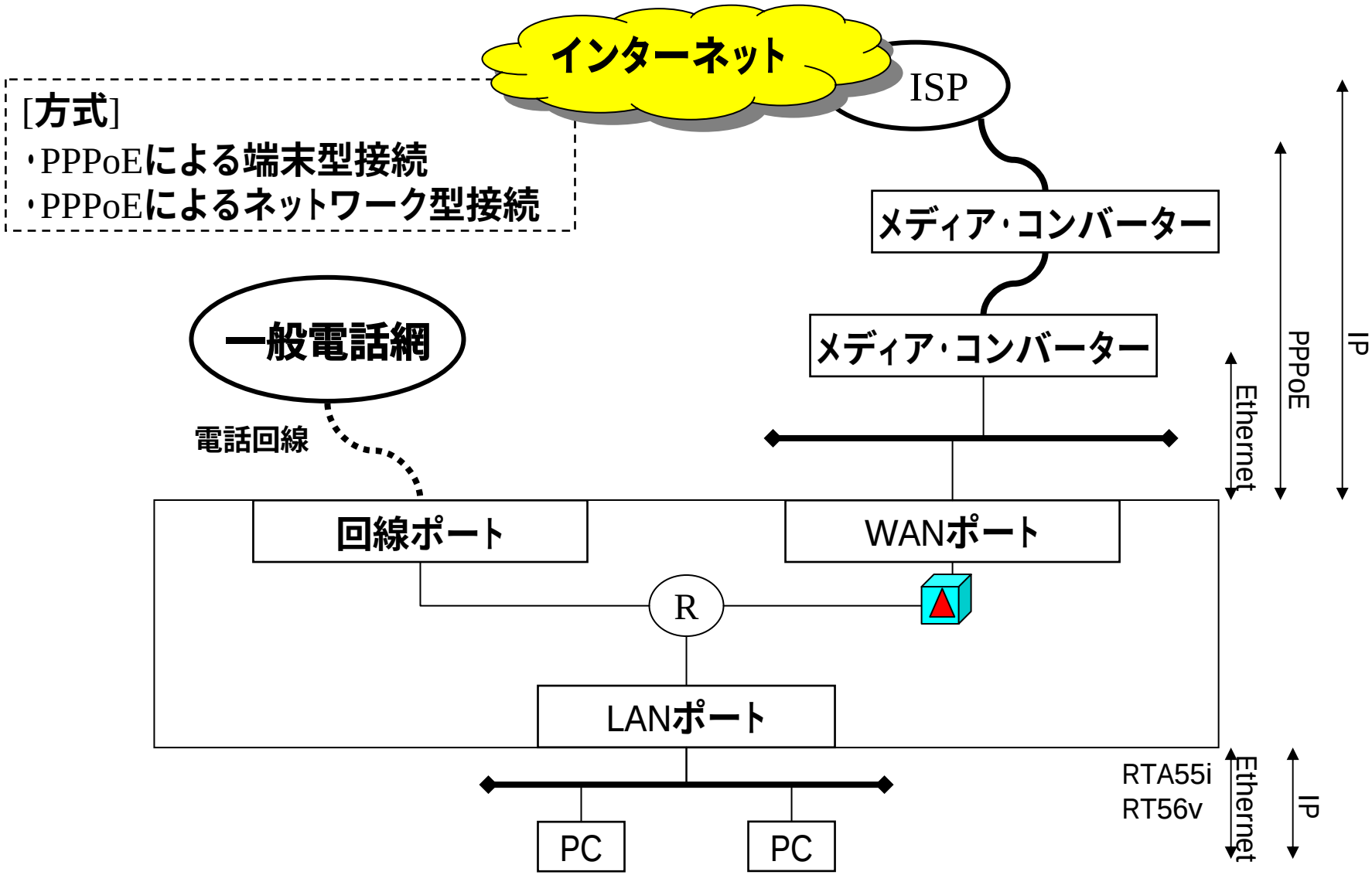
CATVによるプロバイダ接続

[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



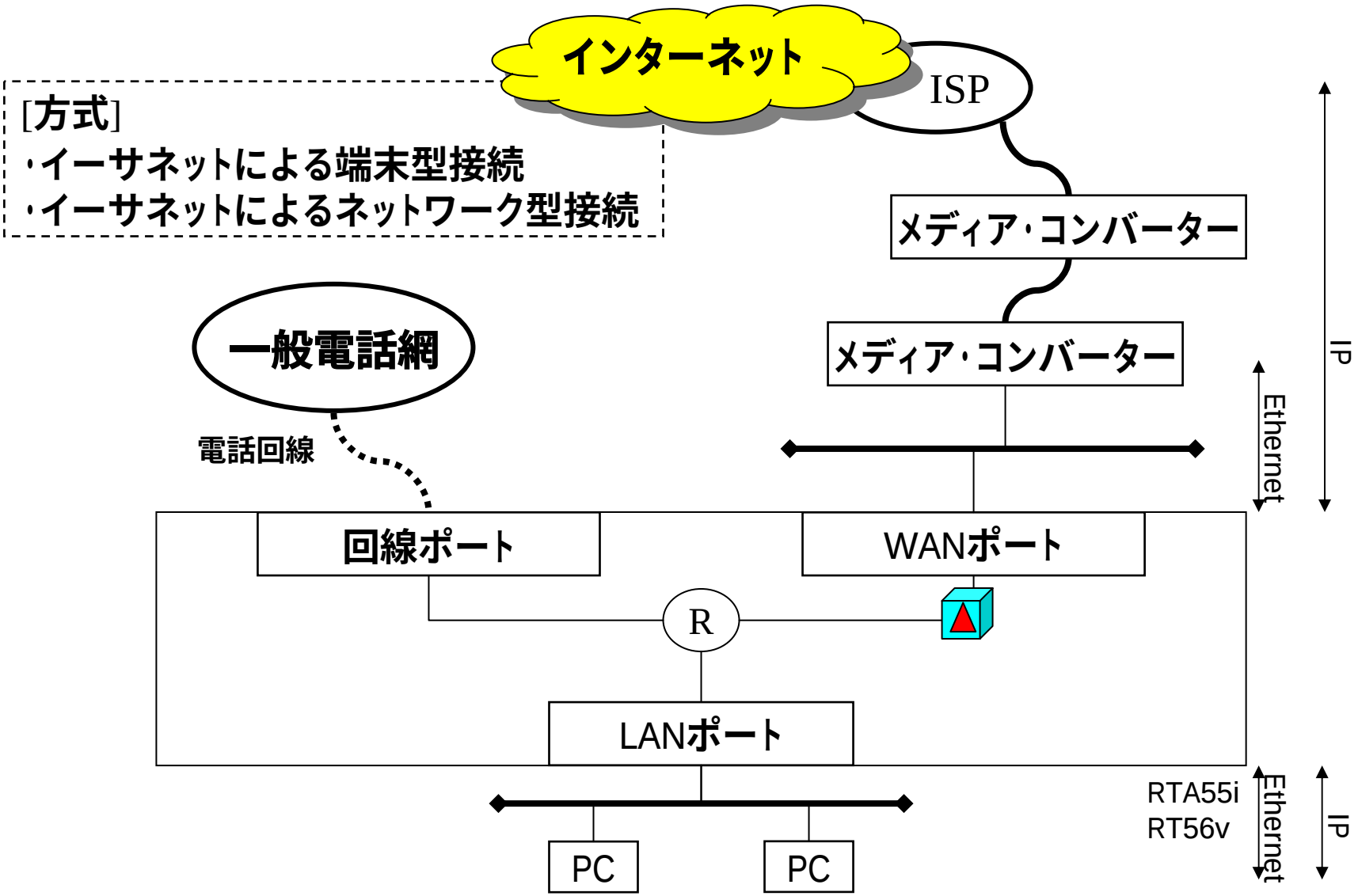
http://www.yamaha.co.jp/news/01121201.html

FTTHによるプロバイダ接続#1

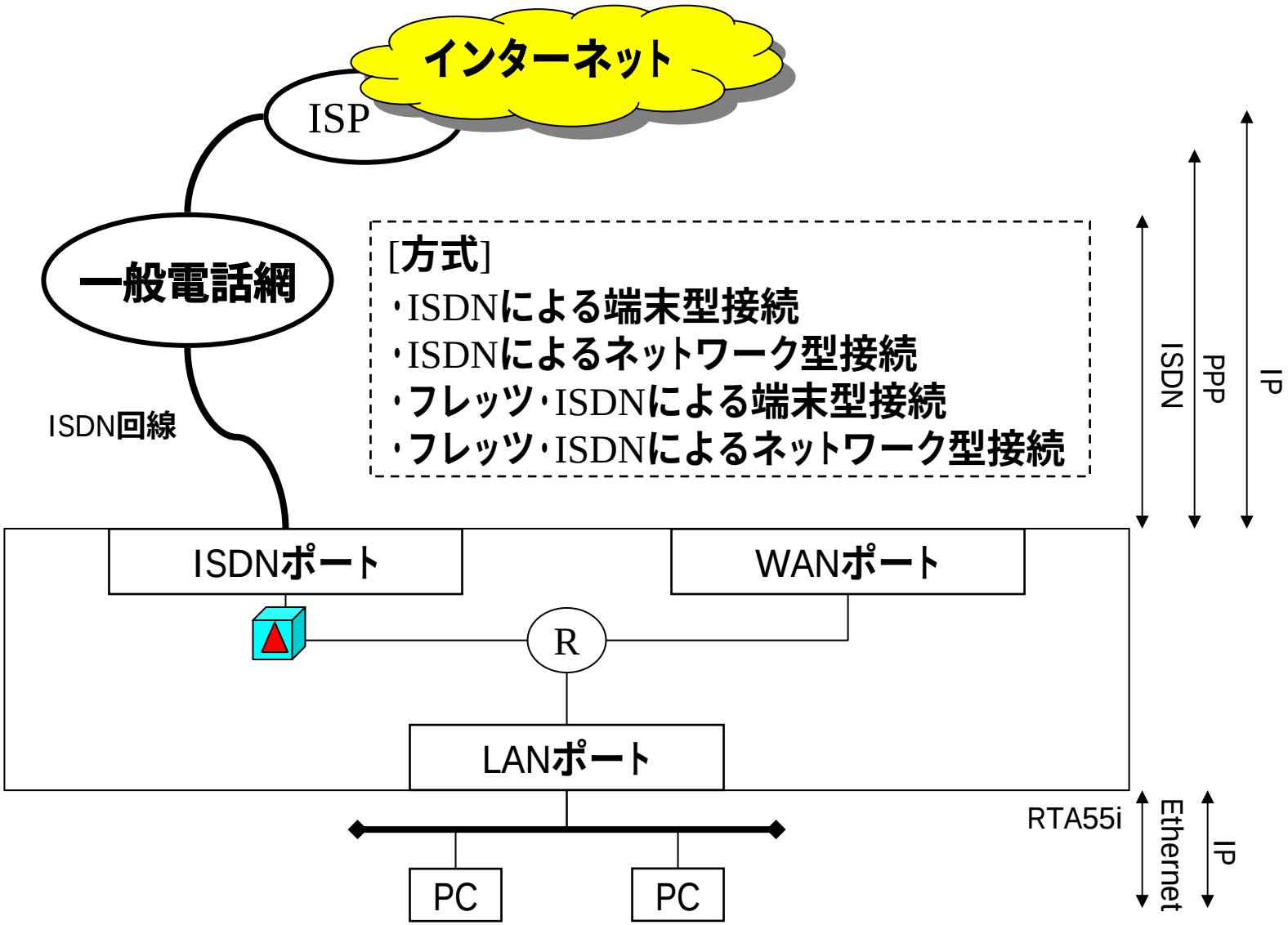


http://www.yamaha.co.jp/news/01121201.html

FTTHによるプロバイダ接続#1

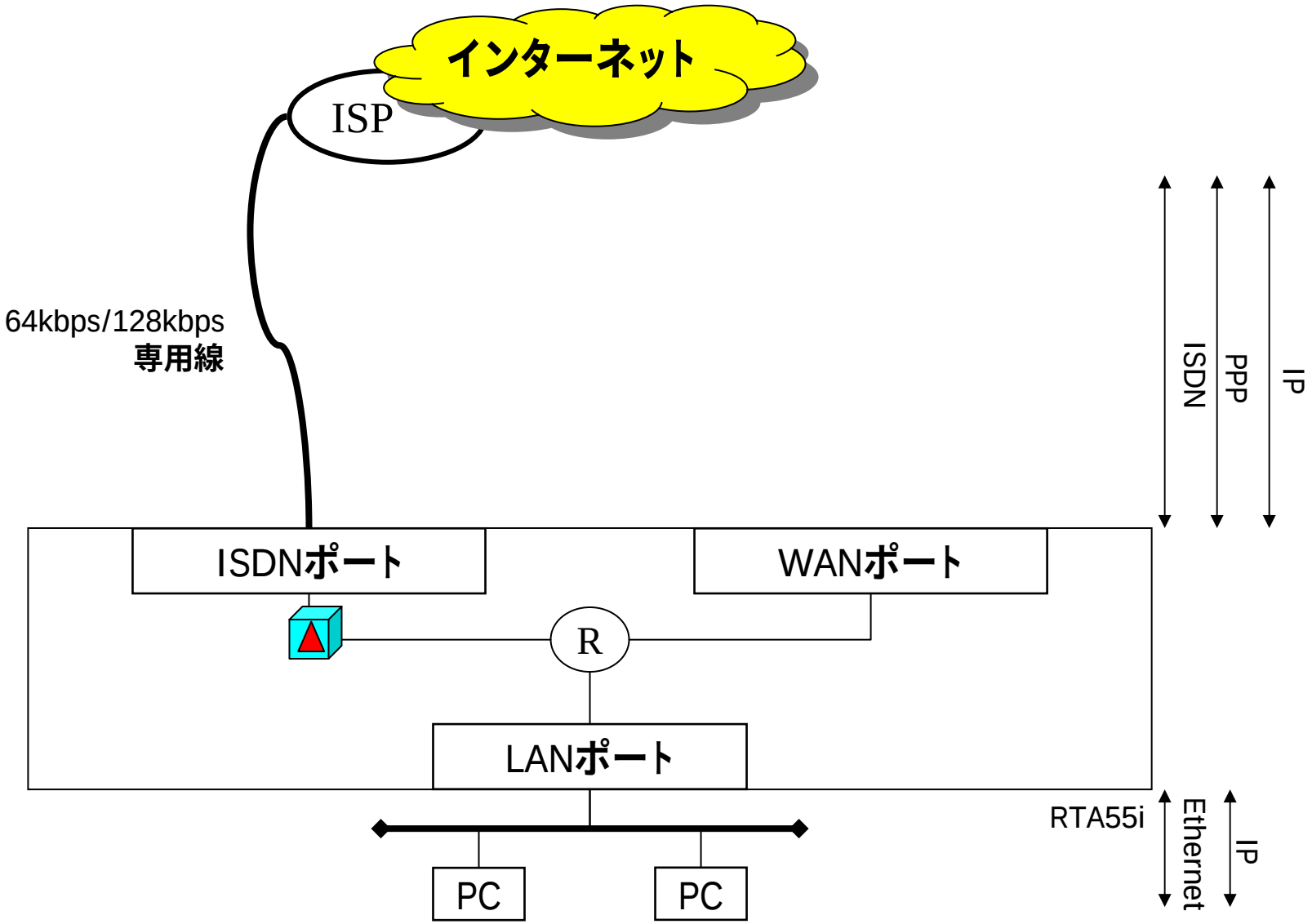


ISDN回線によるプロバイダ接続



http://www.yamaha.co.jp/news/01121201.html

専用線によるプロバイダ接続

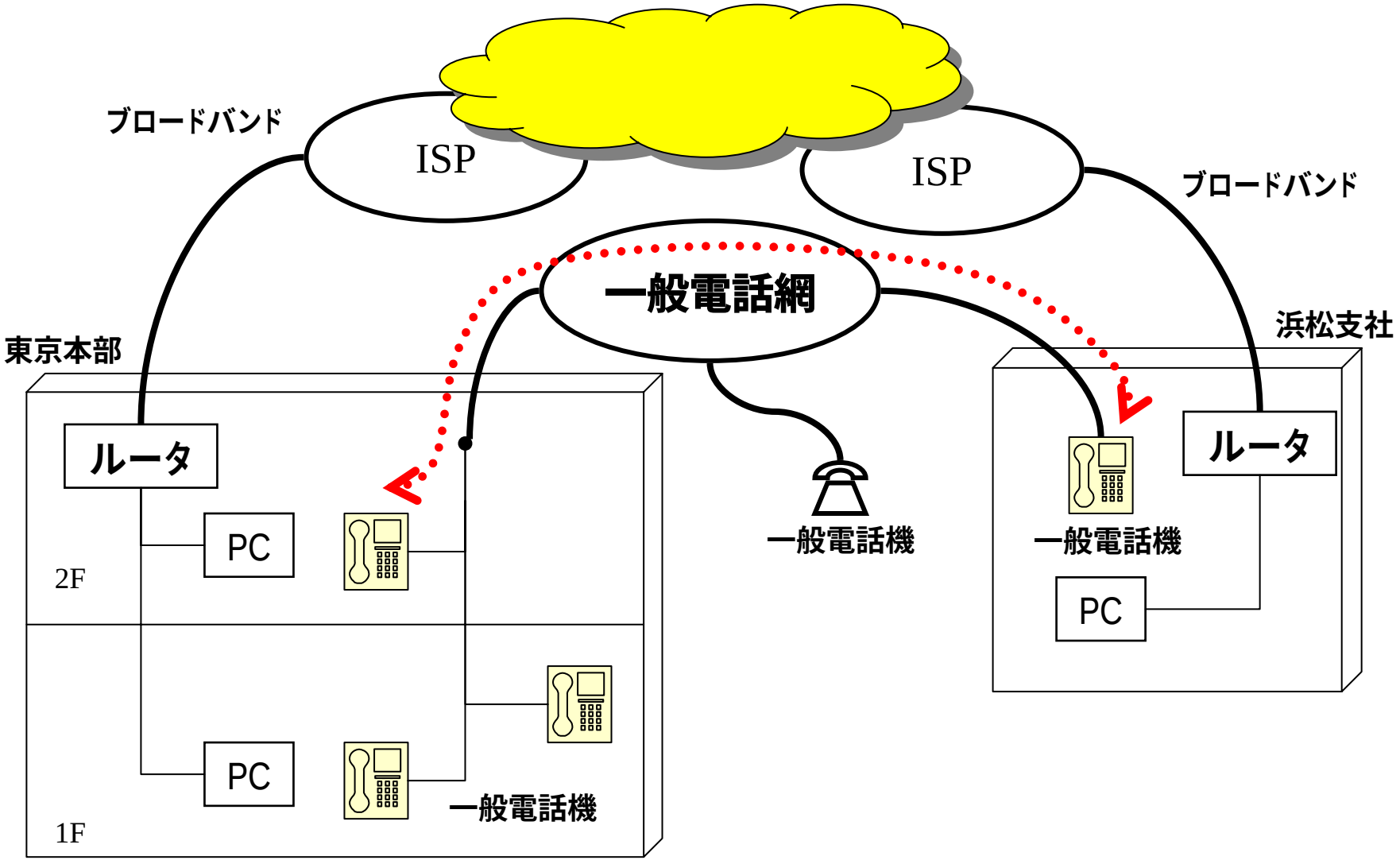


http://www.yamaha.co.jp/news/01121201.html

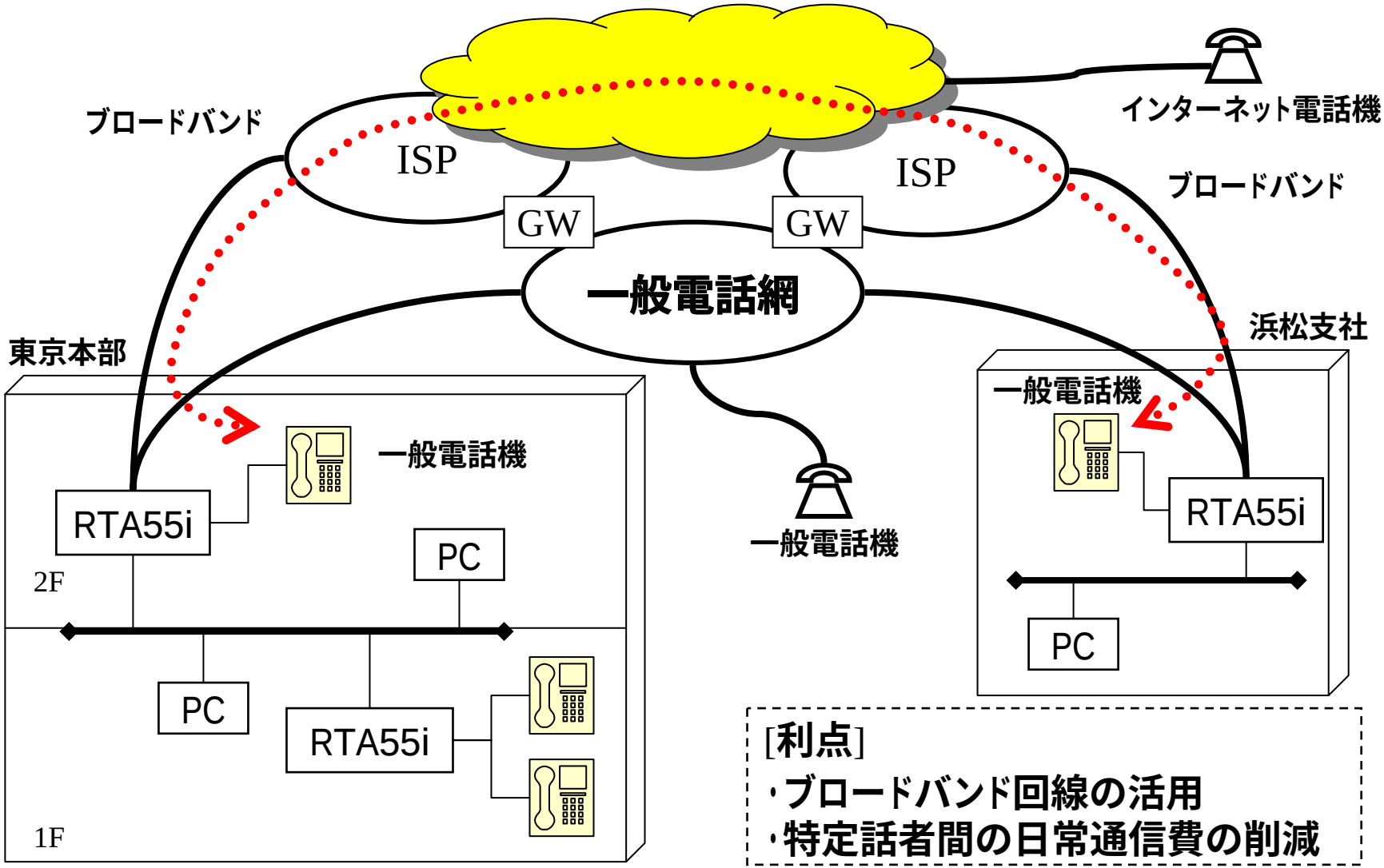
ネットボランチ RTA55i
の
ビジネス用途
(VoIPソリューション)

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

中小規模ブロードバンド・ネットワーク

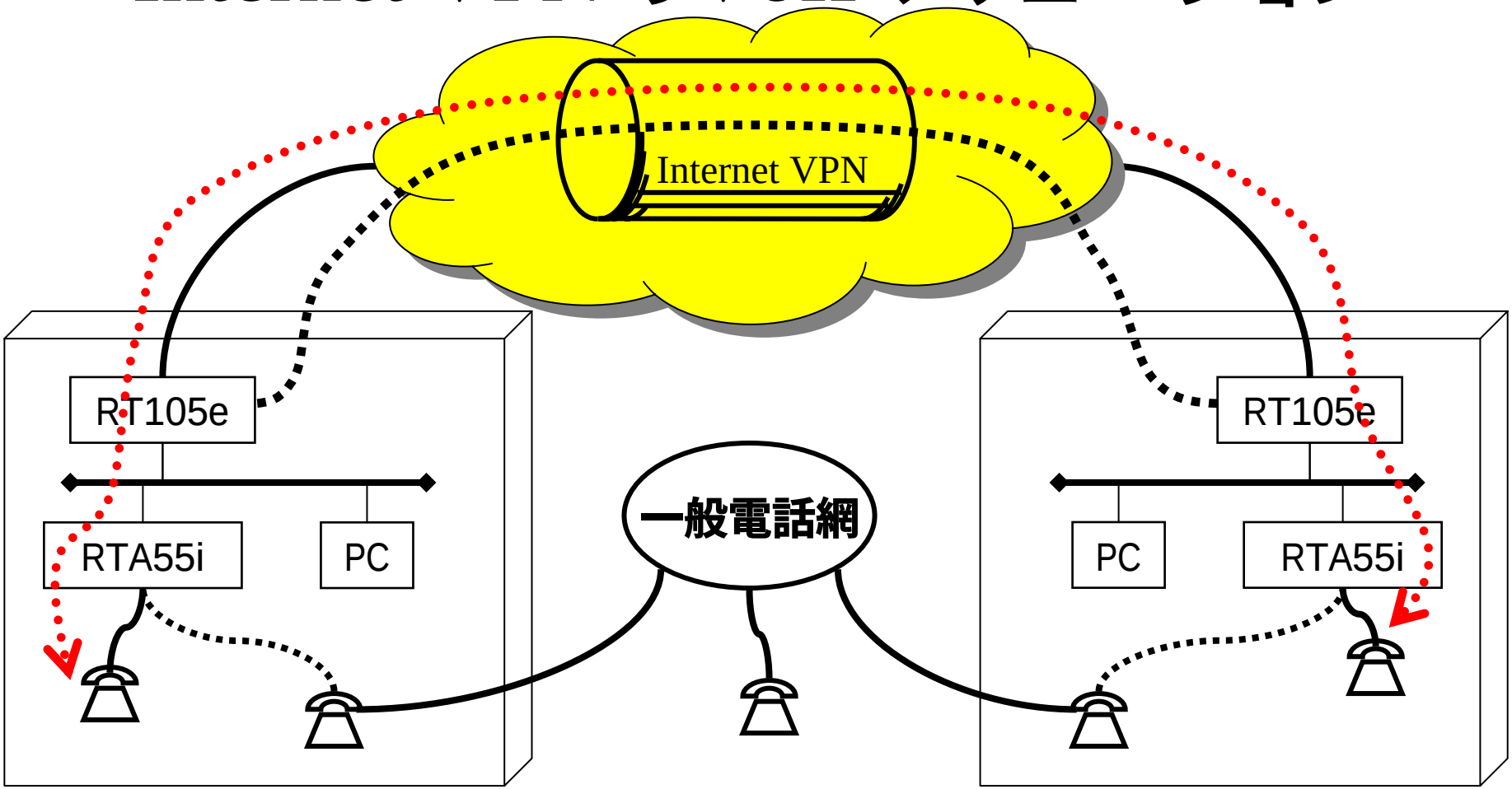


中小規模ネットワークのVoIP化



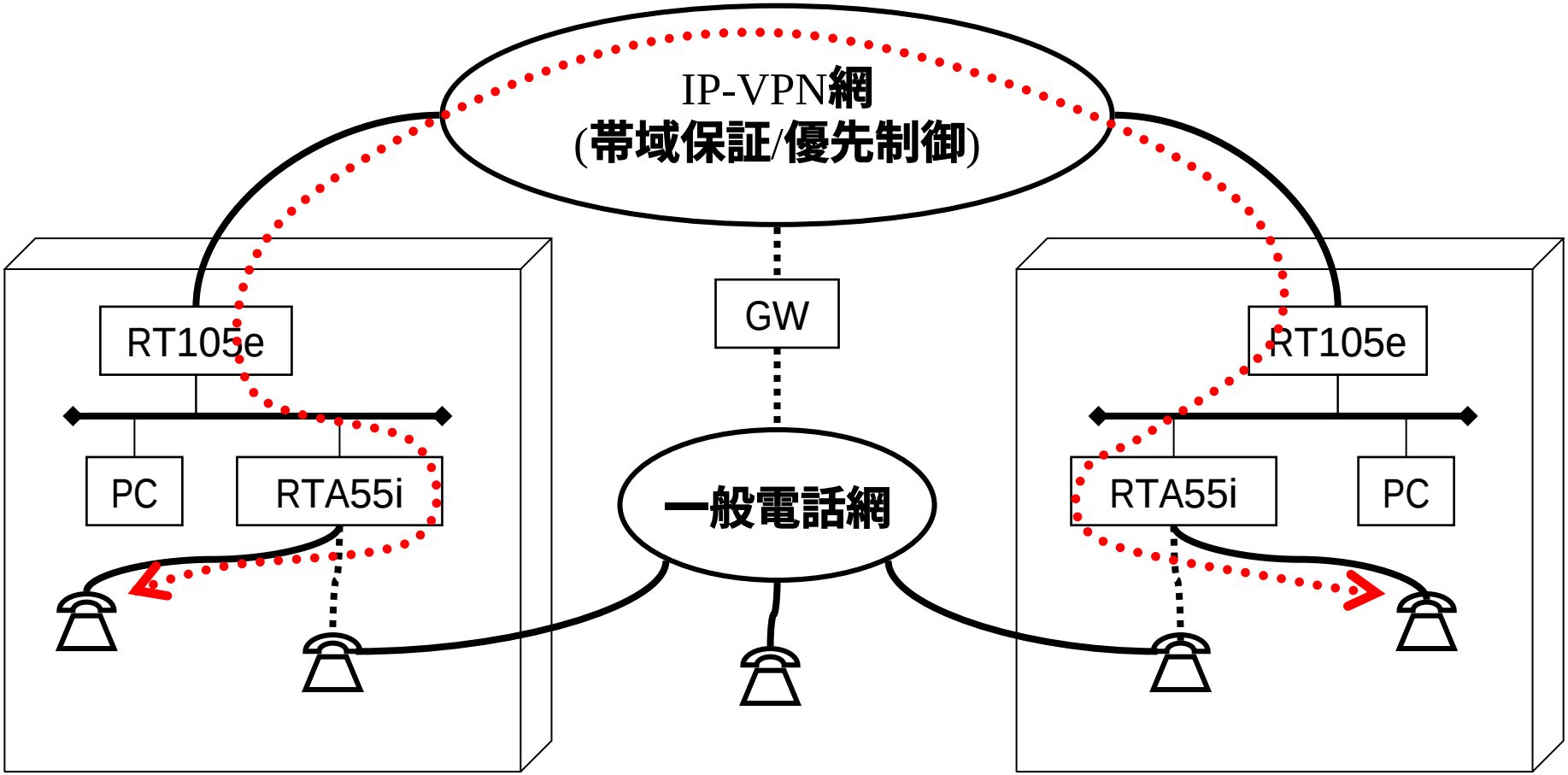
[利点]
・ブロードバンド回線の活用
・特定話者間の日常通信費の削減

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

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 (ftpなどのtcpアプリケーション利用を想定した測定)
　b-1) ローカルルータとして設定/動作させたときのtcp(ftpなど)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
RTA55i	Rev.4.06.xx	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)

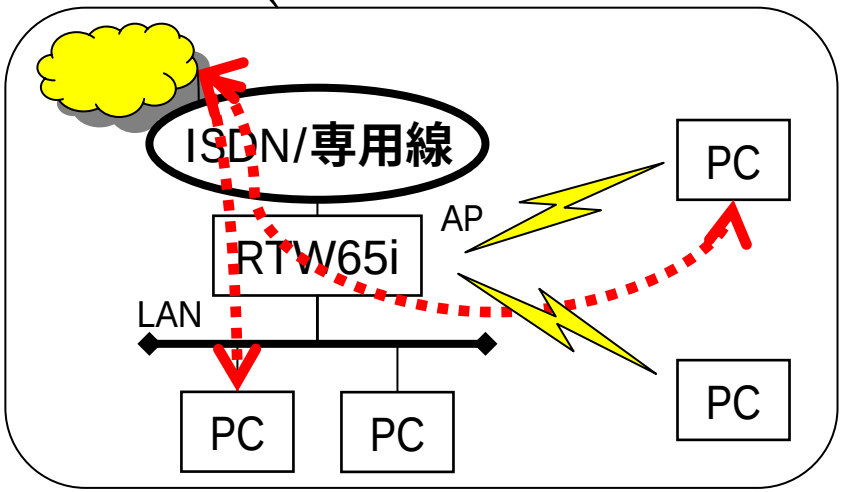
実効: アドレス変換あり、フィルタ設定あり(CATV型セキュリティレベル4)

※スループットは使用環境によって異なる場合がある。

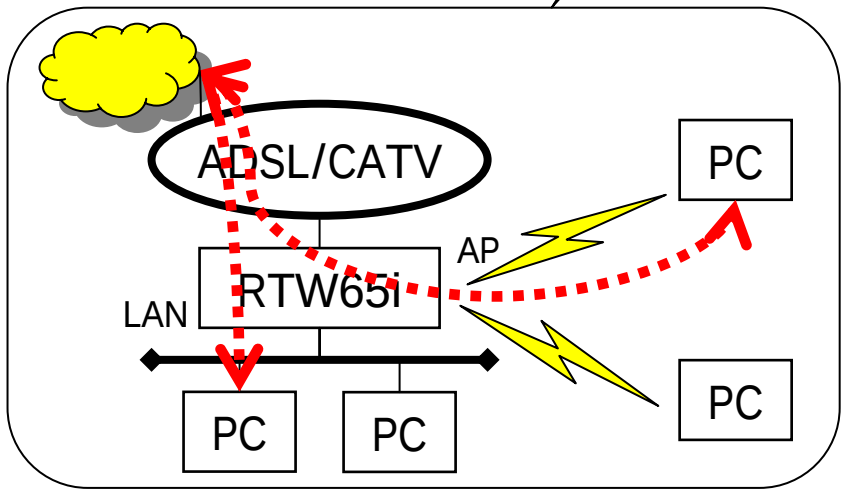
セキュリティレベル6/7の実効スループットは、レベル4より高い。

ネットボランチ
の
いろいろな機能や使い方
「無線LAN編」

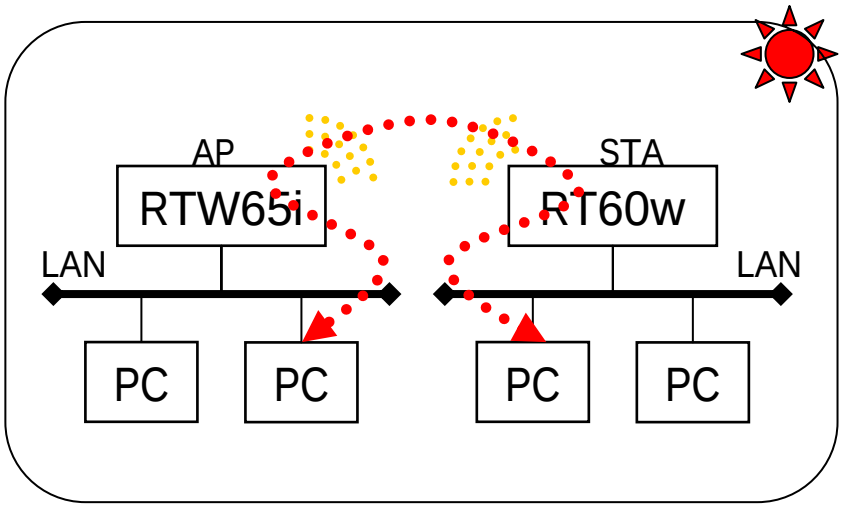
RTW65iの無線LAN機能



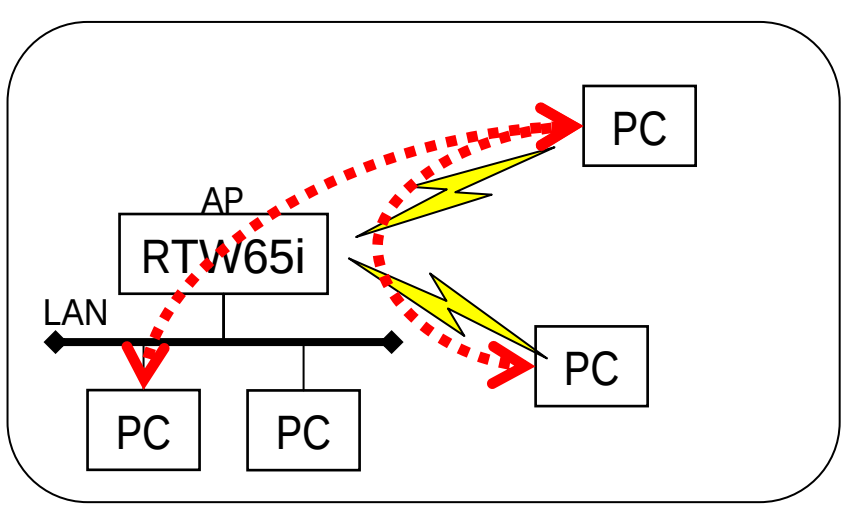
ISDN/専用線によるプロバイダ接続



ADSL/CATVによるプロバイダ接続

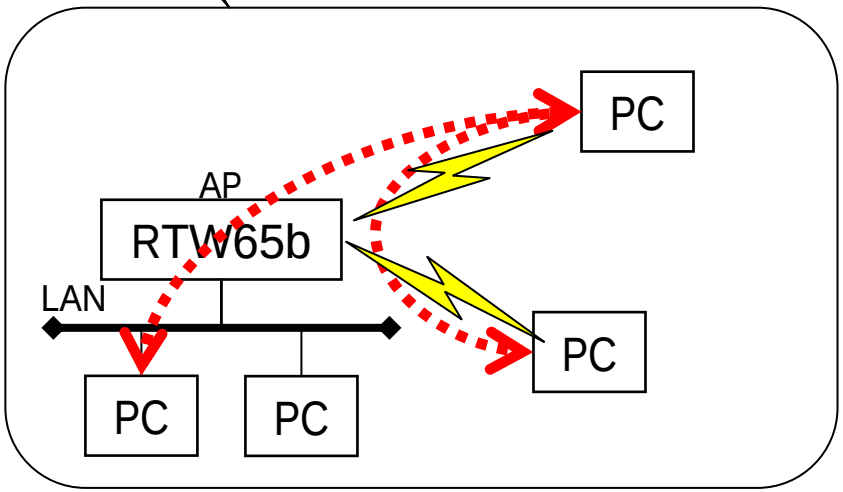


無線ブリッジ機能(離れた有線LAN間を接続)

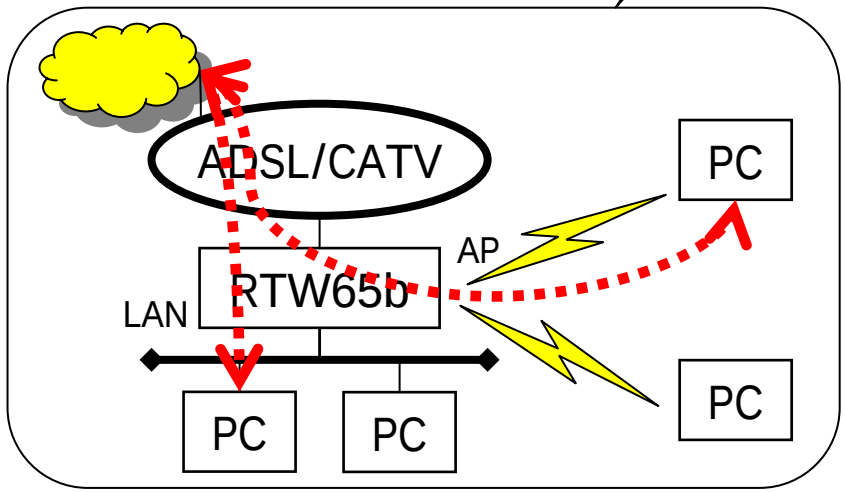


有線LANと無線LANのブリッジ機能

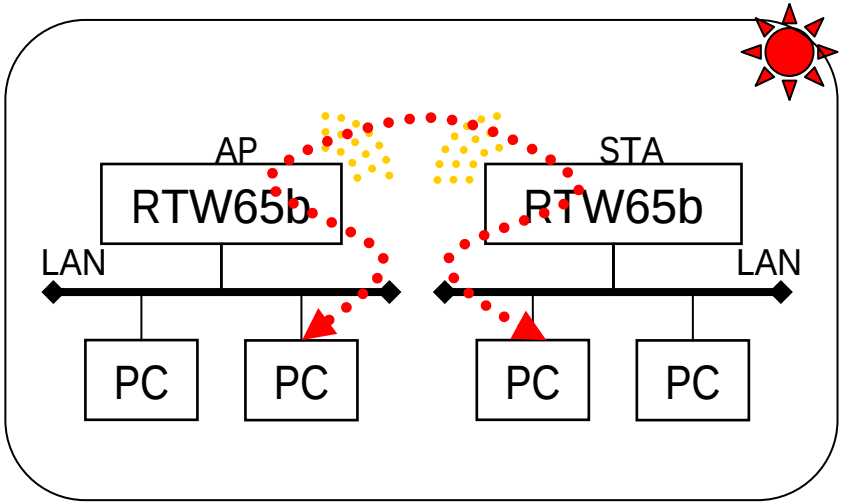
RTW65bの無線LAN機能



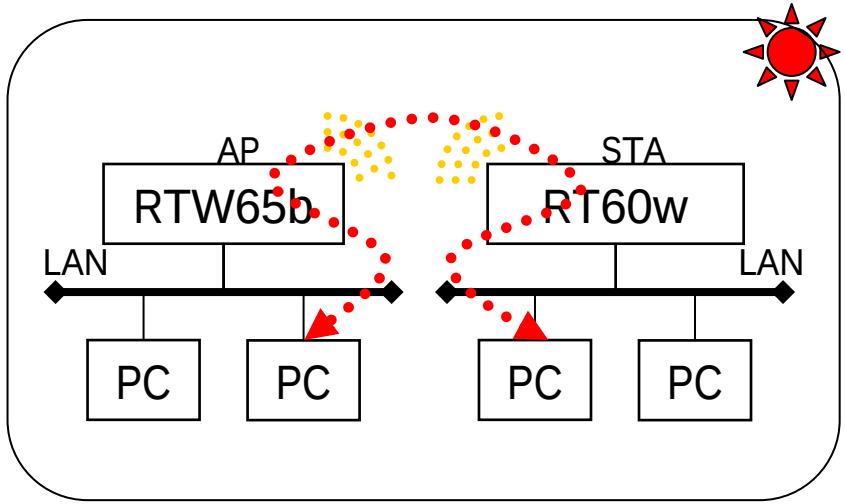
有線LANと無線LANのブリッジ機能



ADSL/CATVによるプロバイダ接続



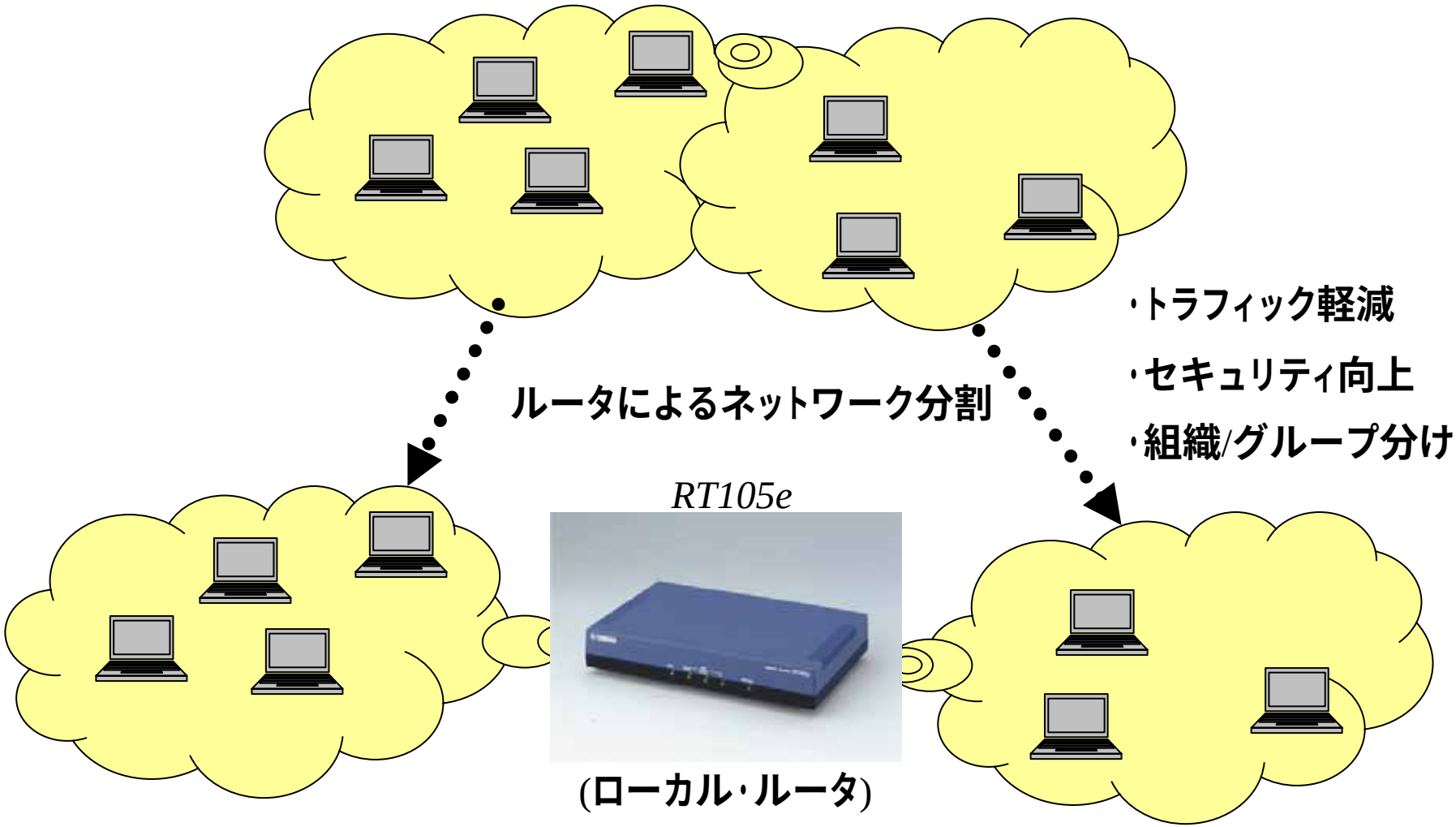
無線ブリッジ機能(離れた有線LAN間を接続)



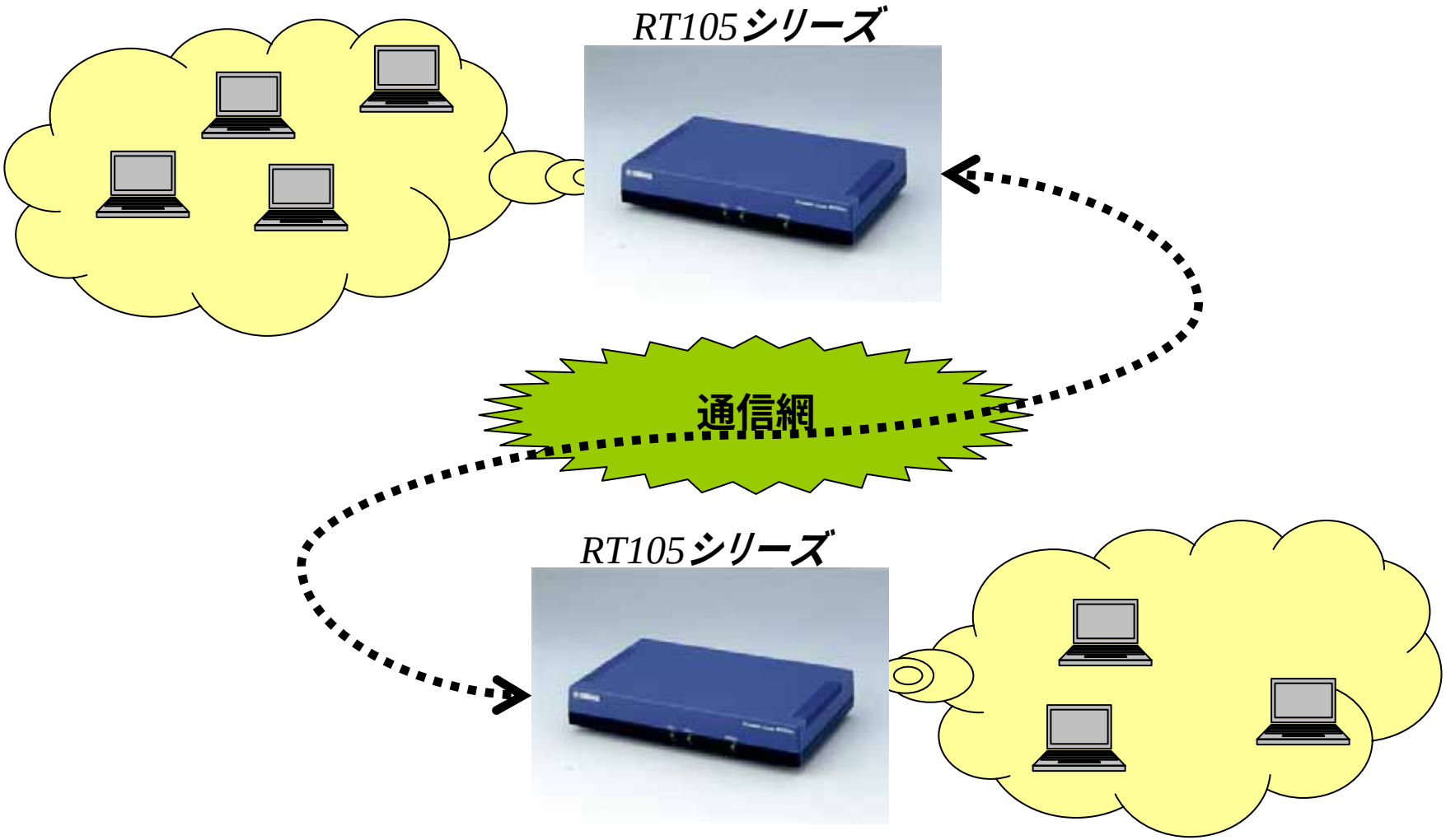
RT60wとの相互接続

ヤマハルータ
の
いろいろな機能や使い方
「RTシリーズ」

ネットワーク分割

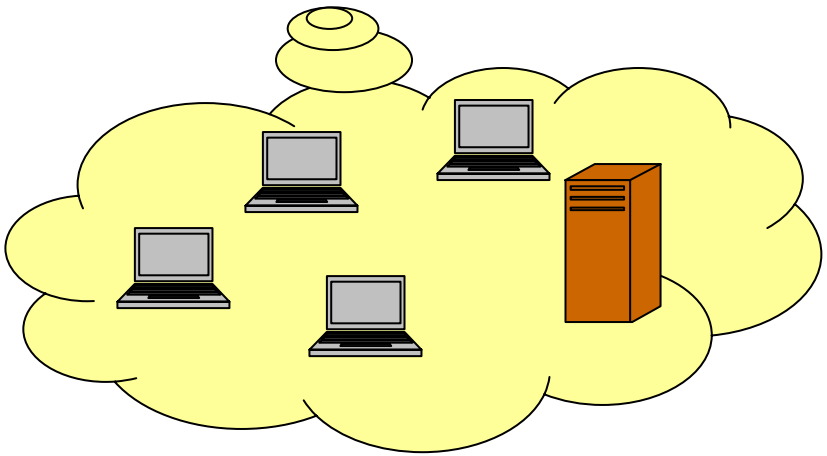


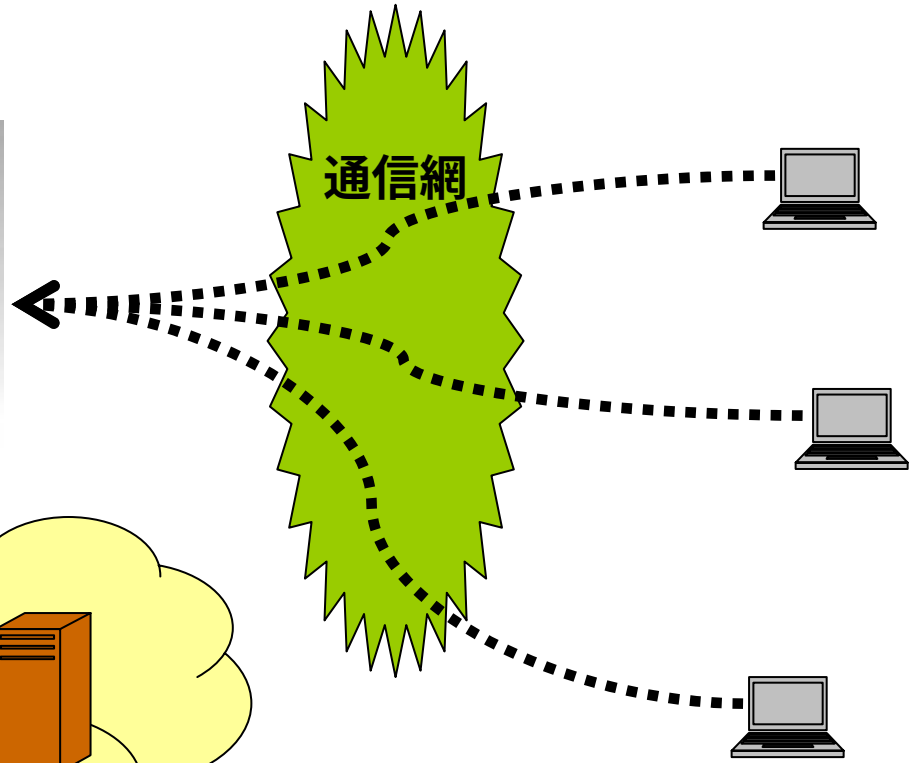
遠隔地とのLAN間接続



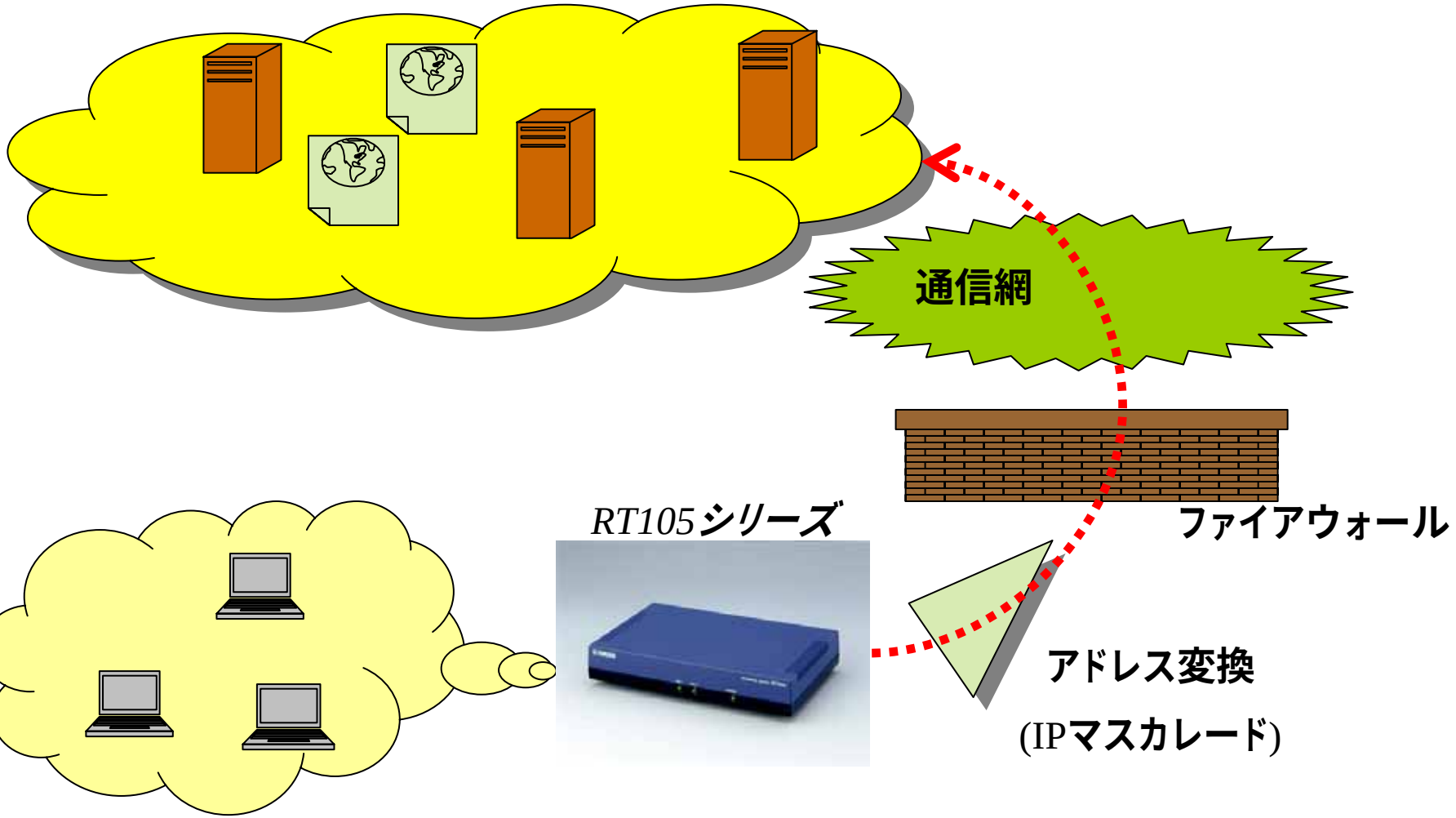
ダイヤルアップサーバ

*RT300i + **オプションモジュール***

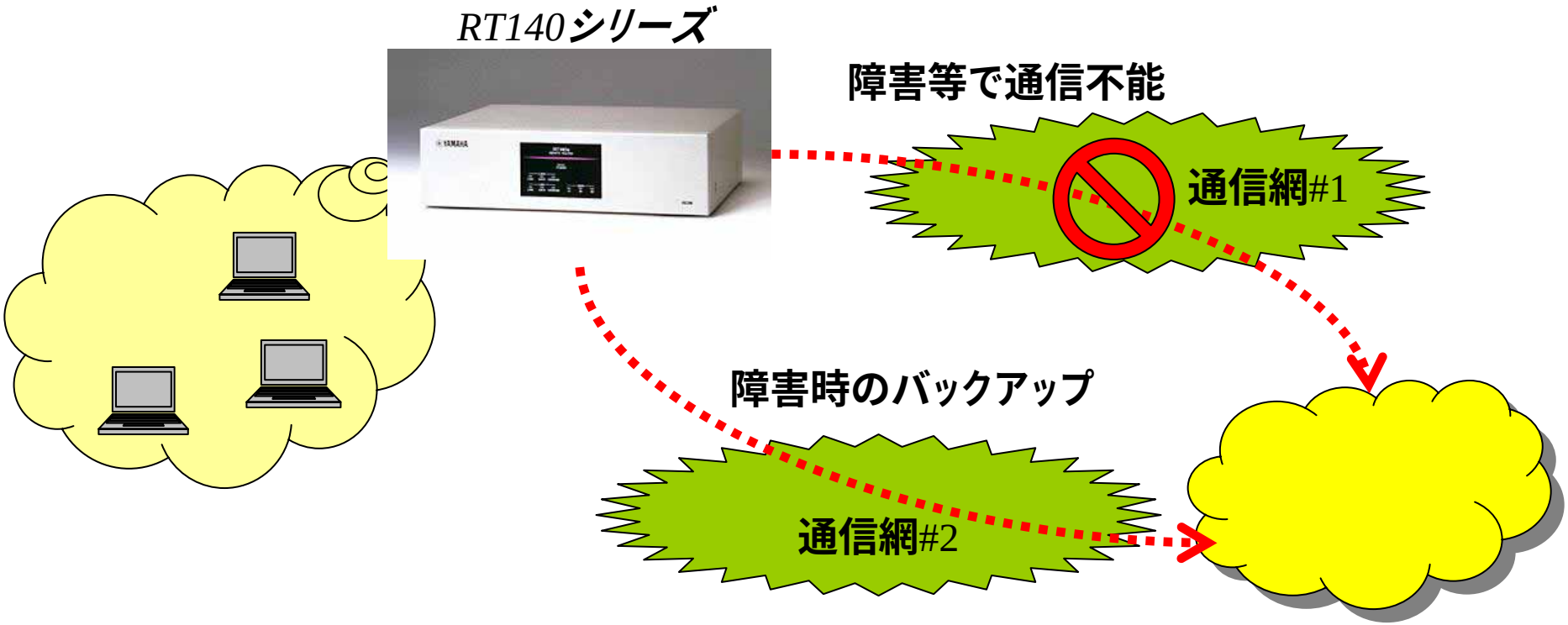




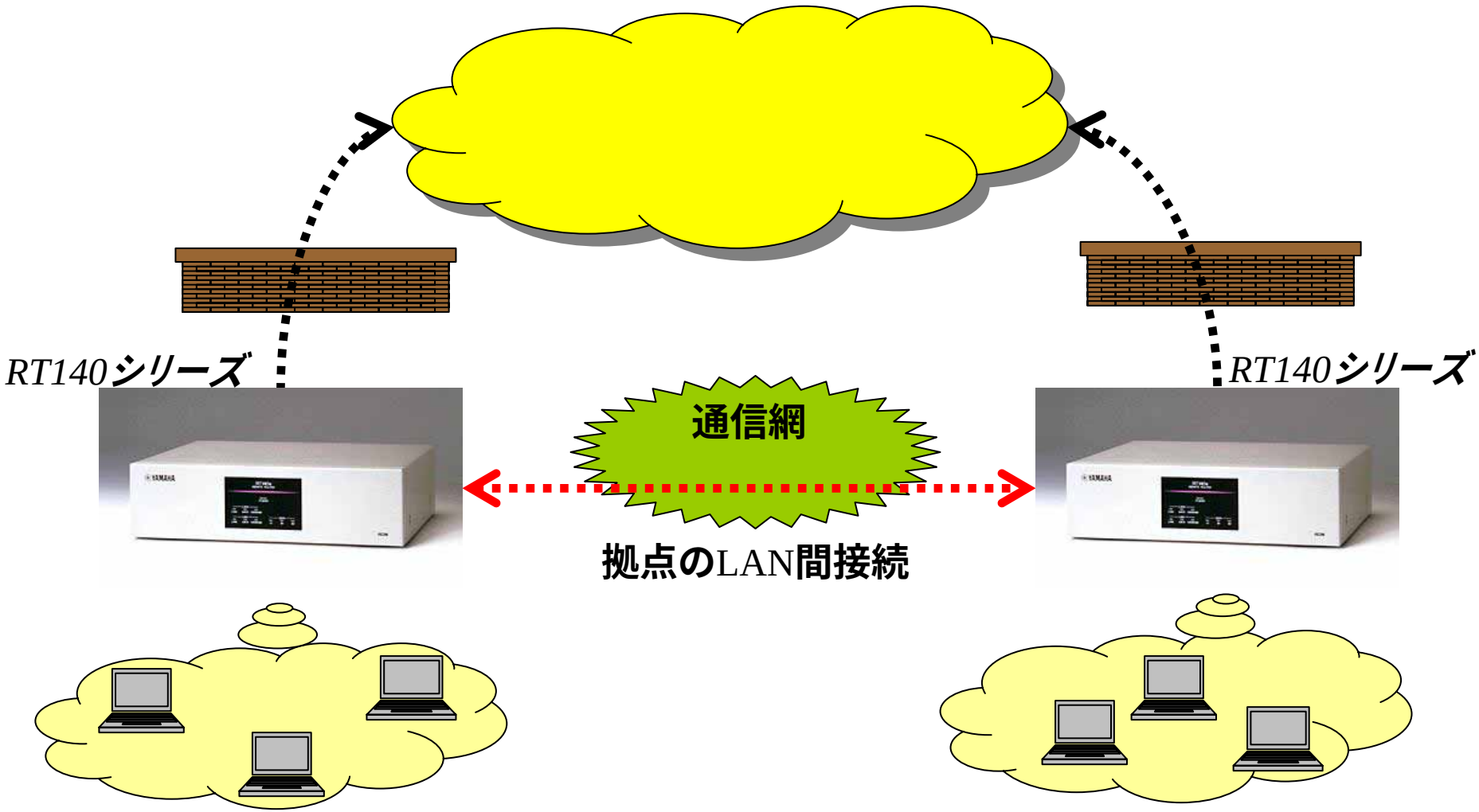
プロバイダ接続



プロバイダ接続のバックアップ

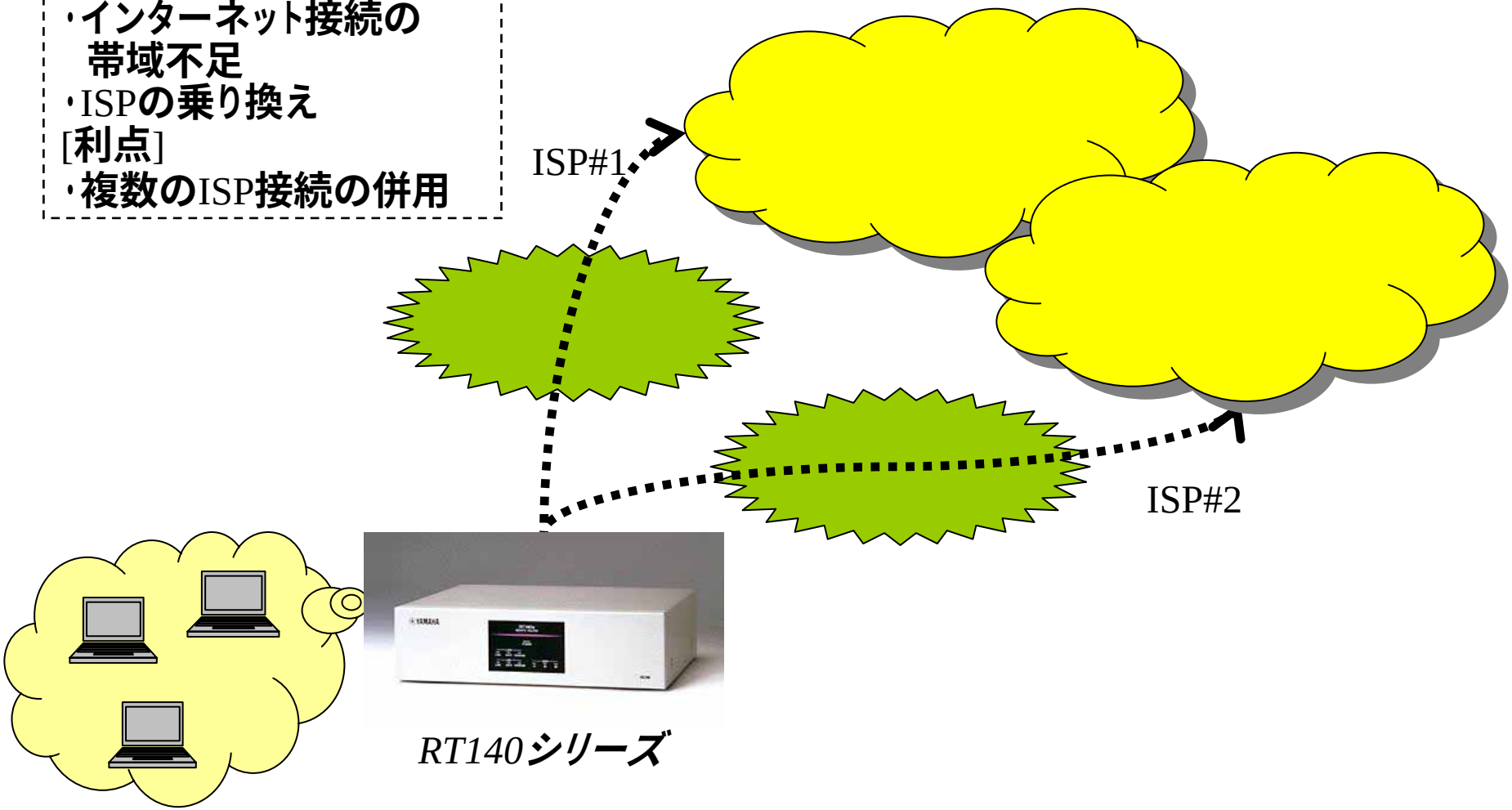


プロバイダ接続+LAN間接続



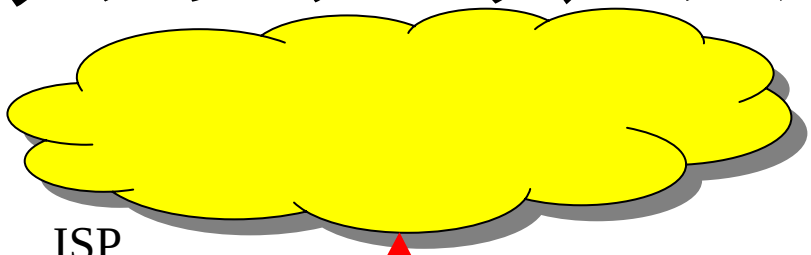
マルチホーミング

[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接続の併用

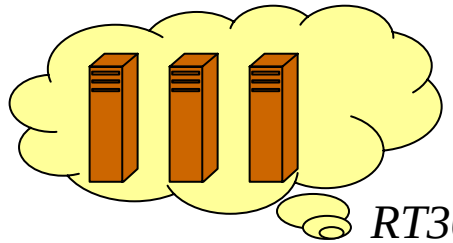


RT140シリーズ

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

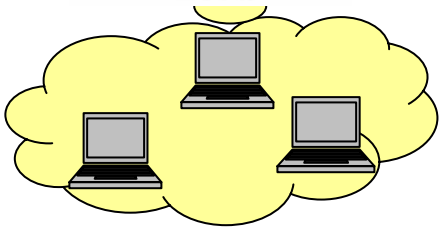
・接続先切り替え
・同時接続

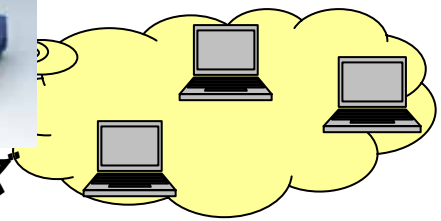
フレッツ・ADSL
Bフレッツ

RTA55i

[悩み]
・インターネット接続と
IP-VPNの併用
[利点]
・フレッツシリーズの活用

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
[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

RT105シリーズ

IP-VPN網

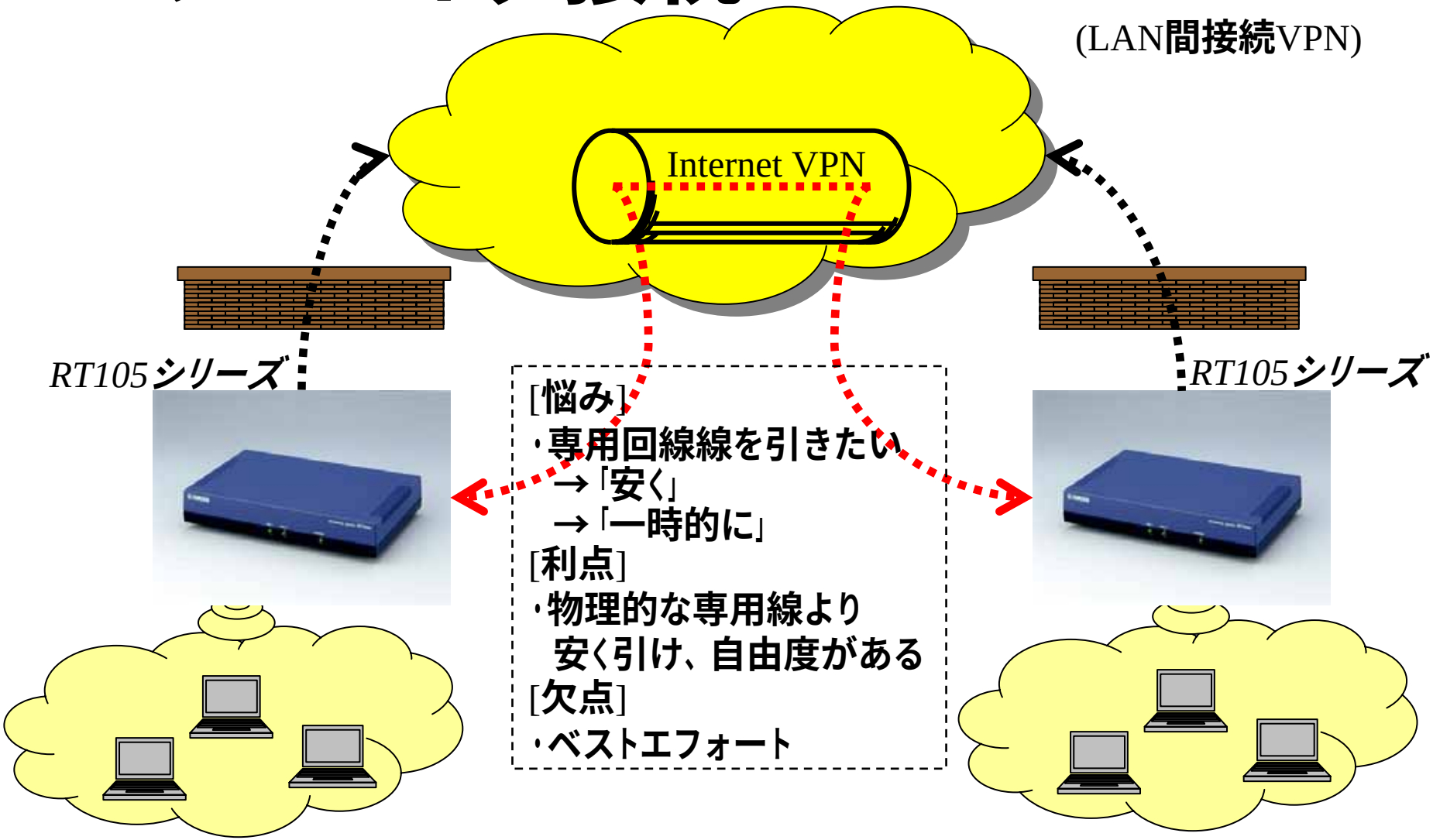
RT105シリーズ

RT105シリーズ

RT105シリーズ

プロバイダ接続+Internet VPN

(LAN間接続VPN)



ダイヤルアップVPN

(リモートアクセスVPN)

[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

IP固定

RT300i

VPN

VPN

VPN

IP不定

RT105シリーズ

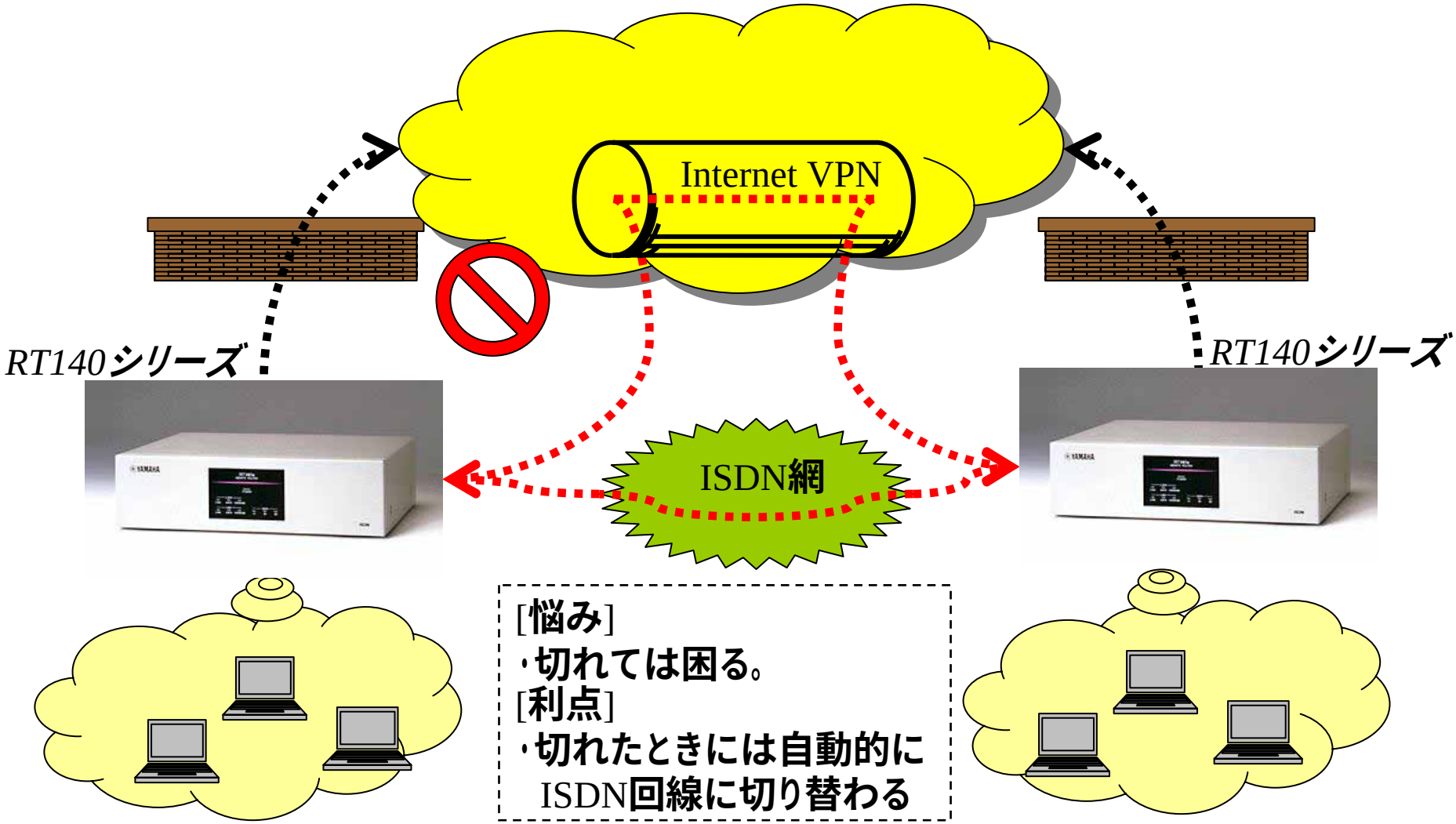
IP不定

RT105シリーズ

IP不定

RT105シリーズ

Internet 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

ヤマハルータの構造

柔軟性と多機能のために

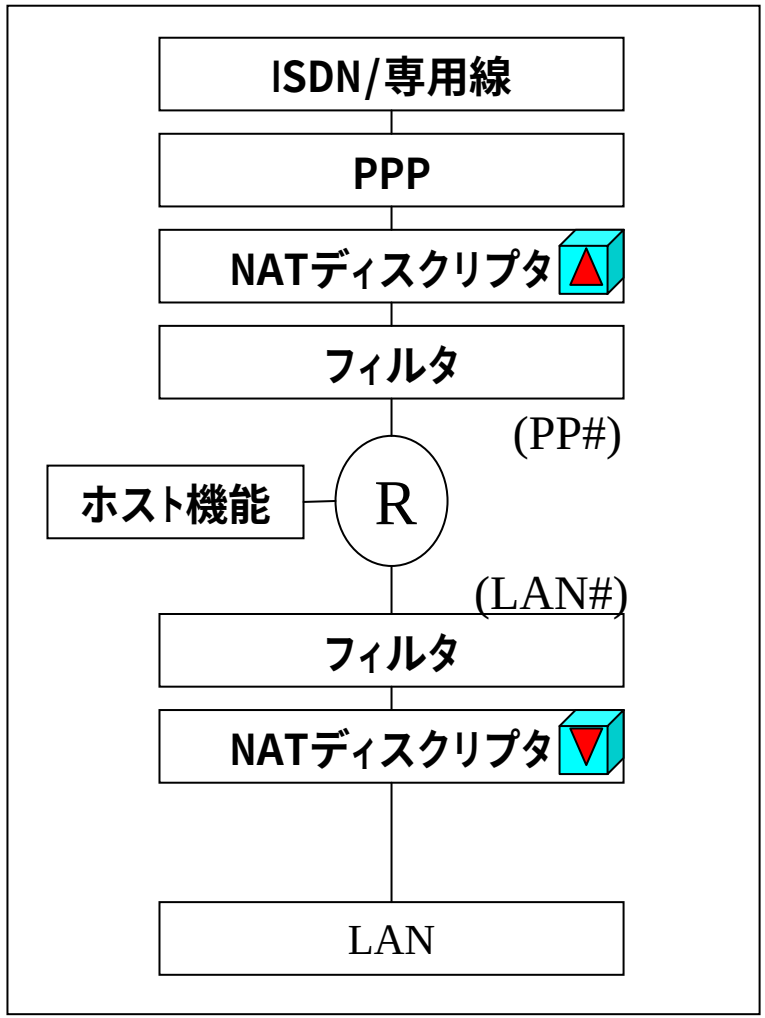
多機能で信頼性のある
モジュール構成

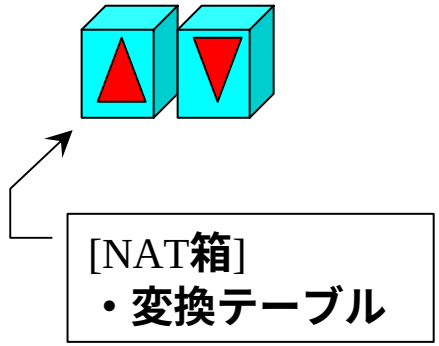
構造#1(PPP)

RT140i

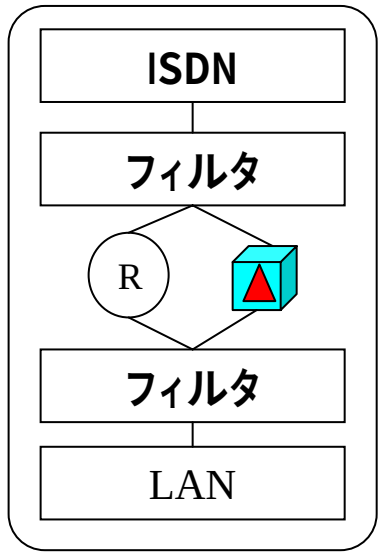
RT105i

RTA52i





比較構成例

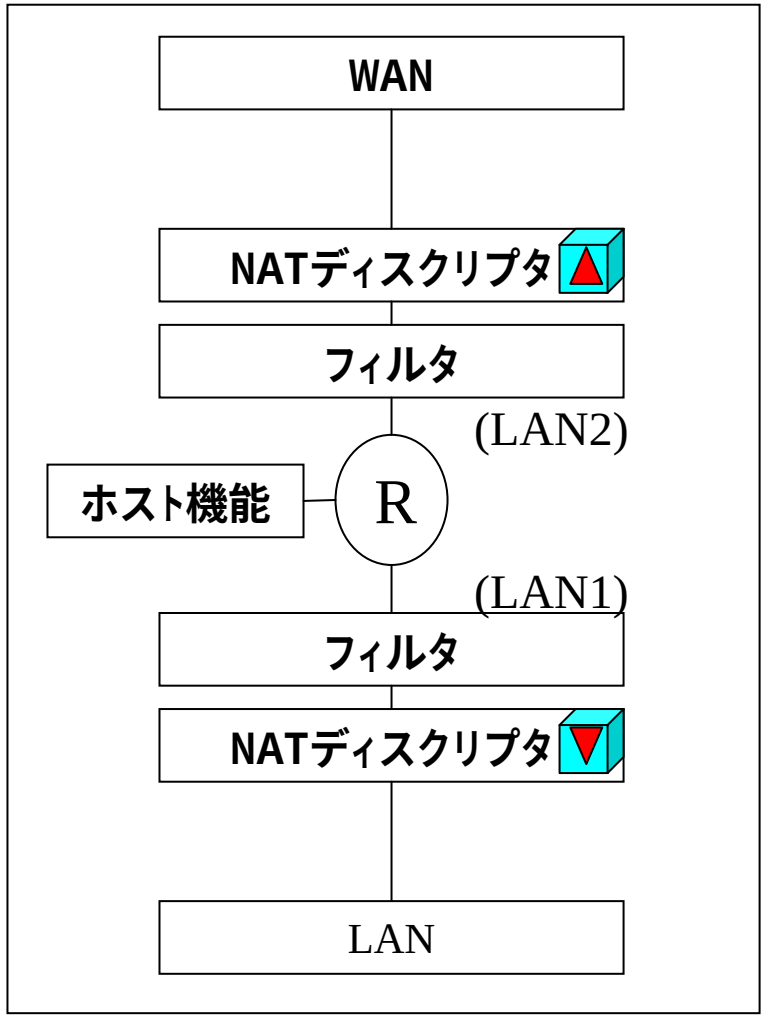


構造#2(ローカルルータ)

RT300i

RT140e

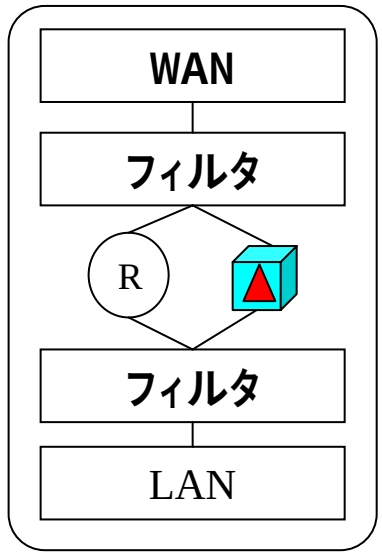
RT105e



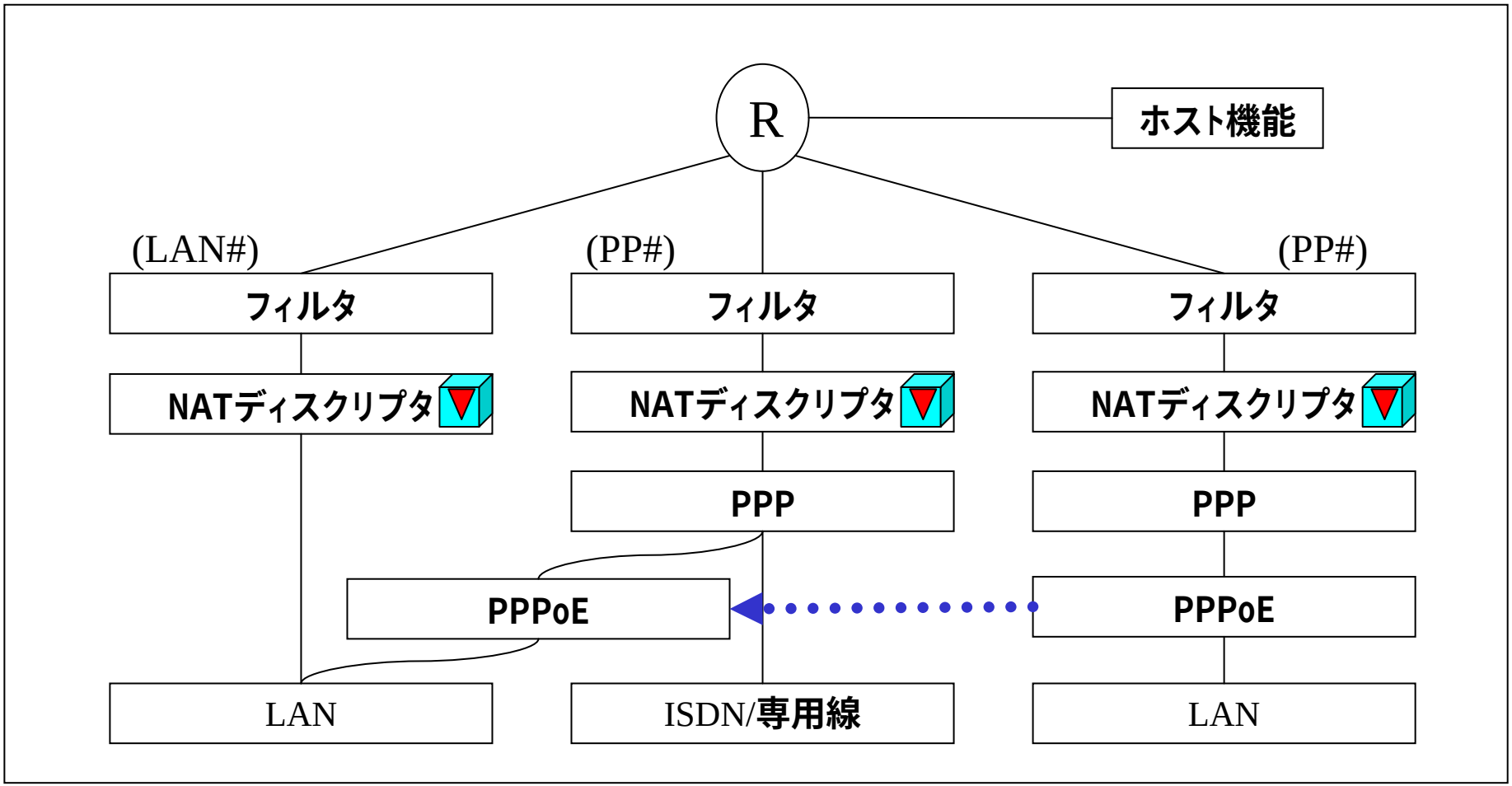
RTW65b

RTA55i

比較構成例



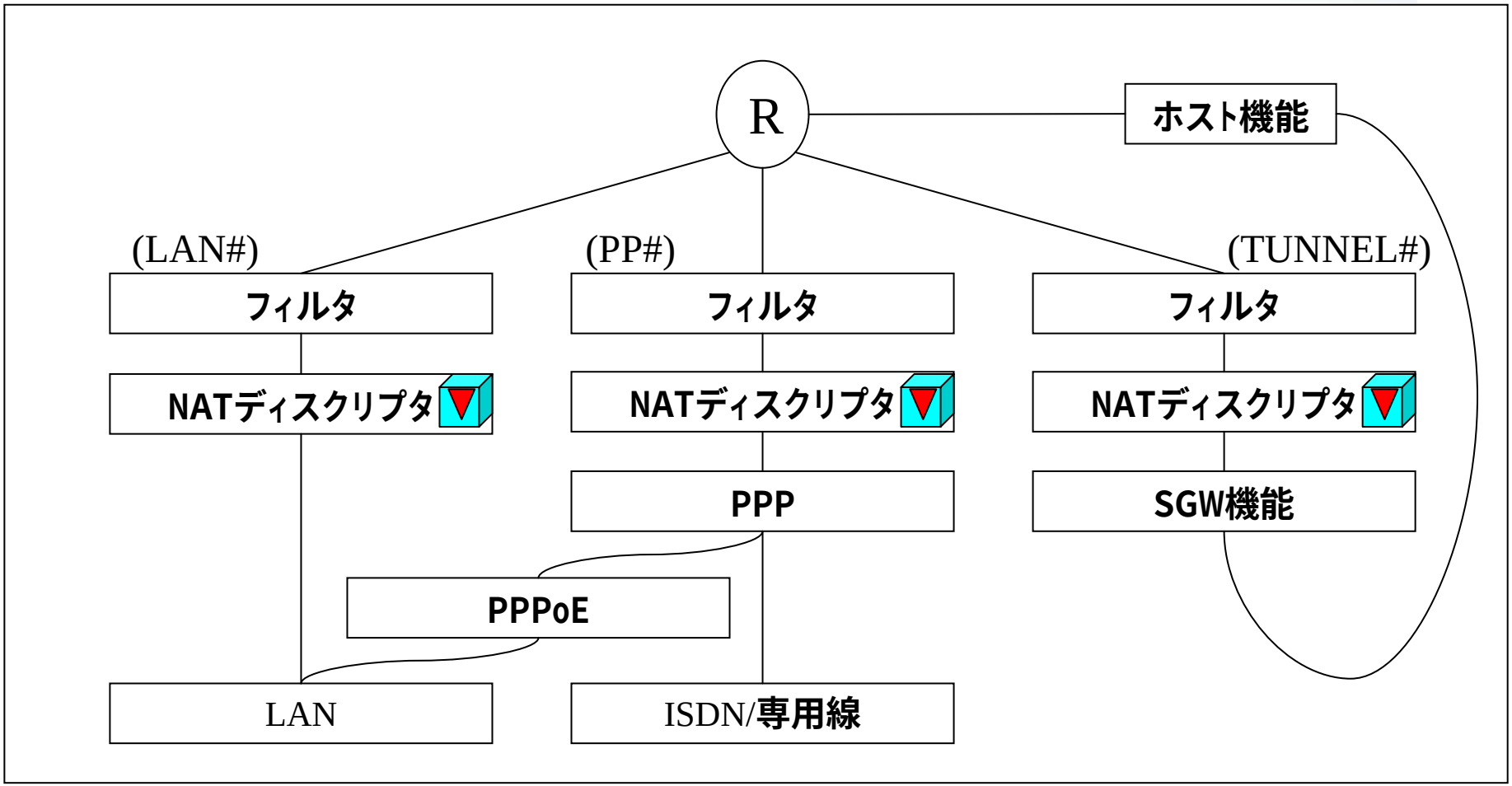
構造#3(PPPoE)



RT300i

構造#4(VPN)

RT105シリーズ



アドレス変換

- 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。

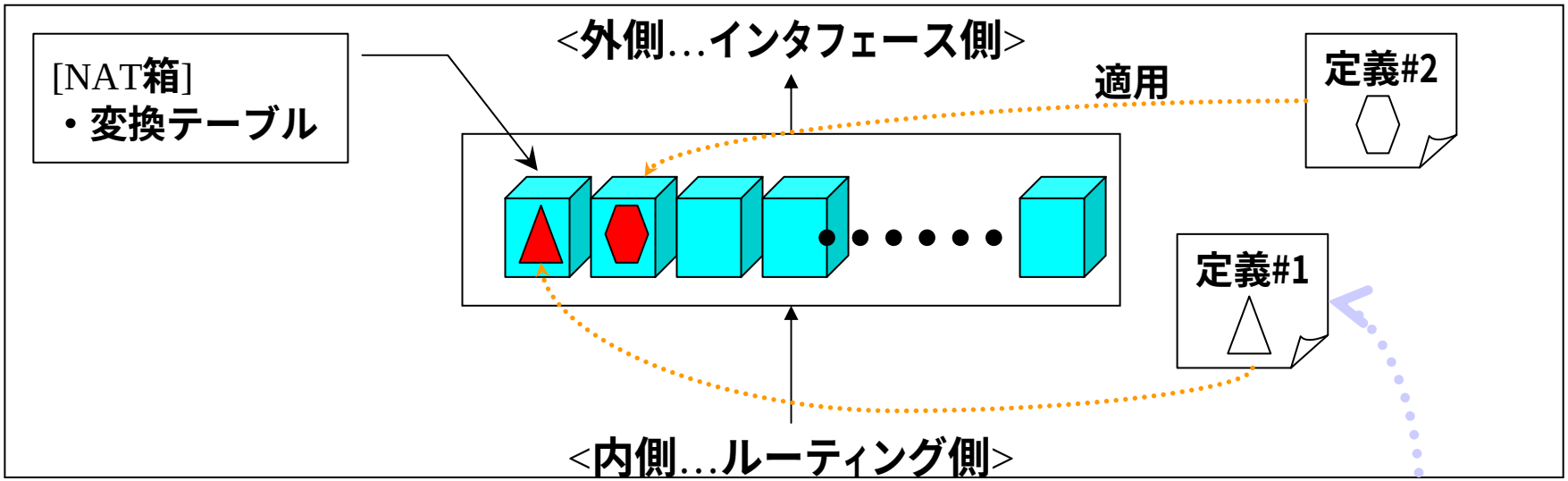
アドレス変換機能(NAT)への取り組み

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

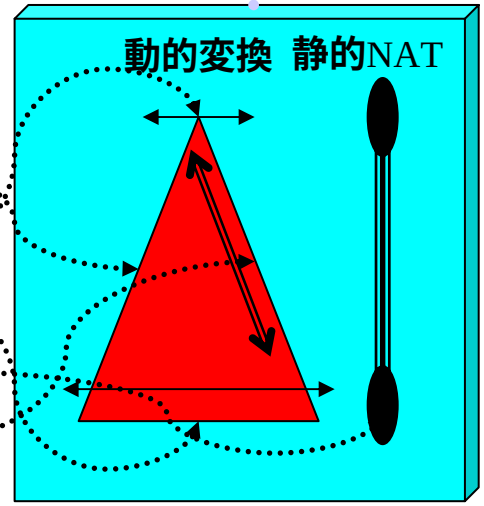
- LANインタフェースに対応
  - LANのprimary⇔secondaryの変換が可能
- TUNNELインタフェースに対応
  - VPNで変換が可能
- 3つの変換タイプ
  - NAT形式
  - IPマスカレード形式
  - NAT + IPマスカレード形式
- 機能統合、制限の緩和
  - 複数の変換規則を並列的に適用可能
    (ひとつのインタフェースに16組)

NATディスクリプタの構造



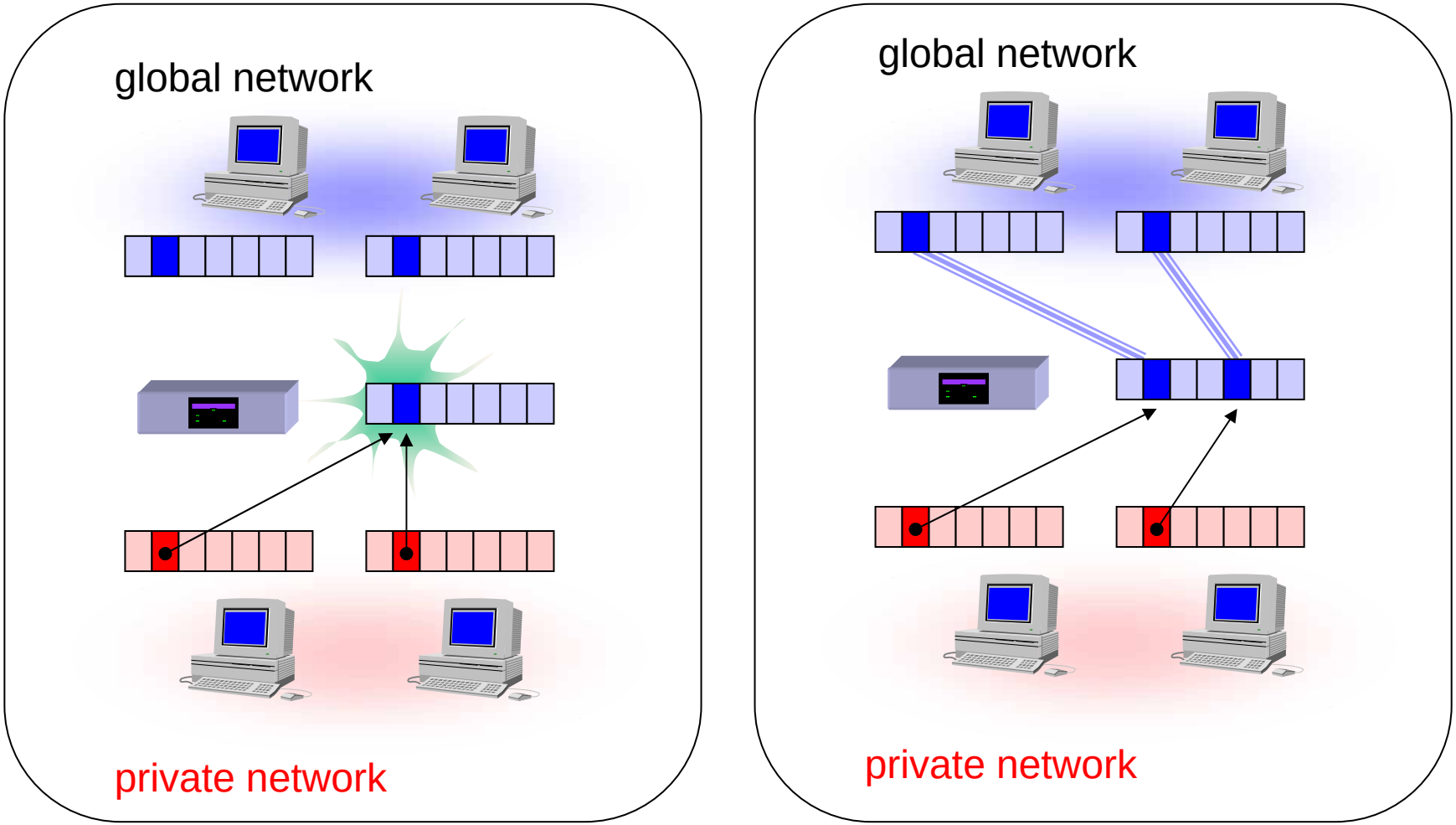
[定義→アドレス変換の設計図]

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



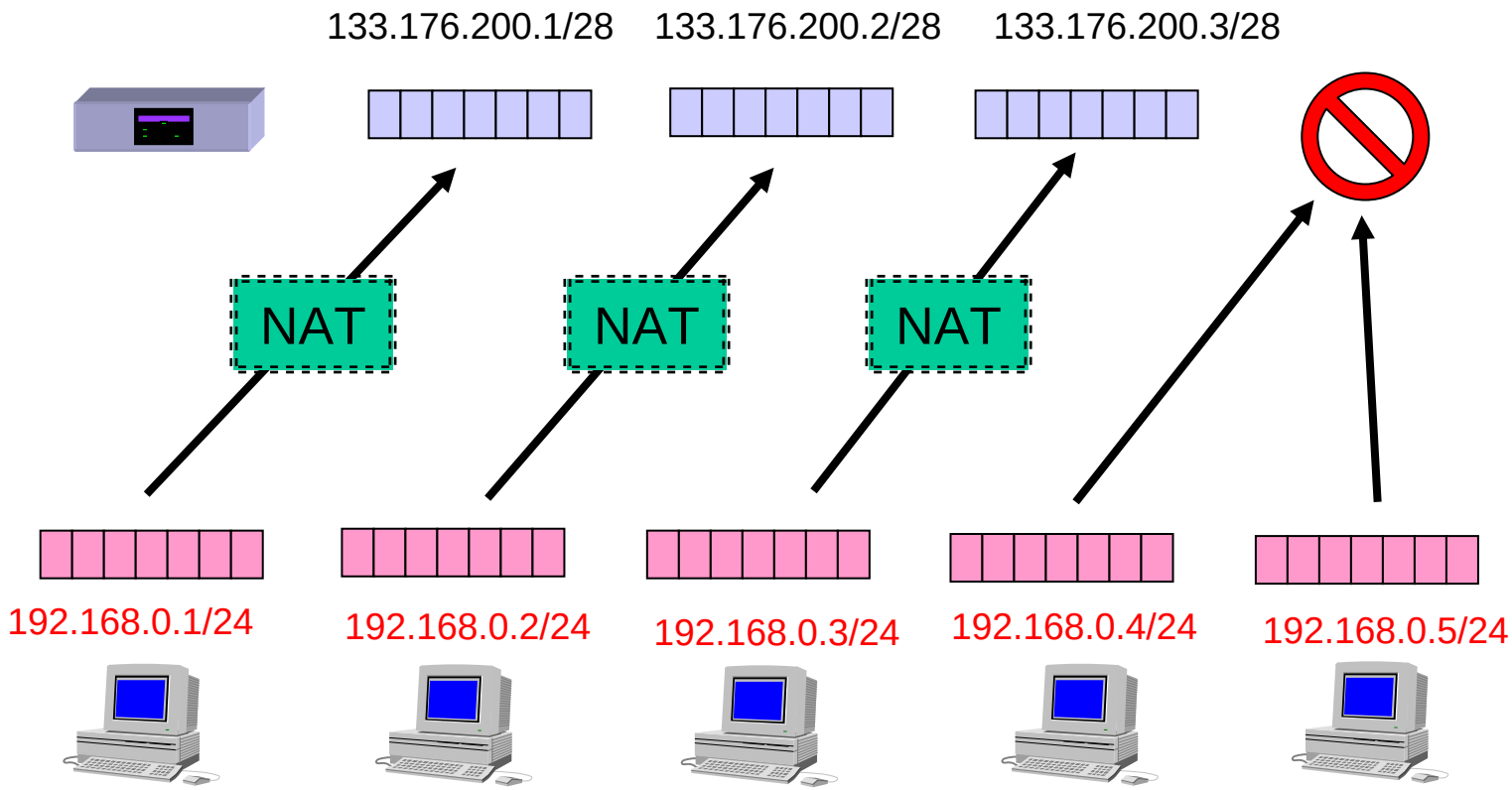
IPマスカレード(IP Masquerade)

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



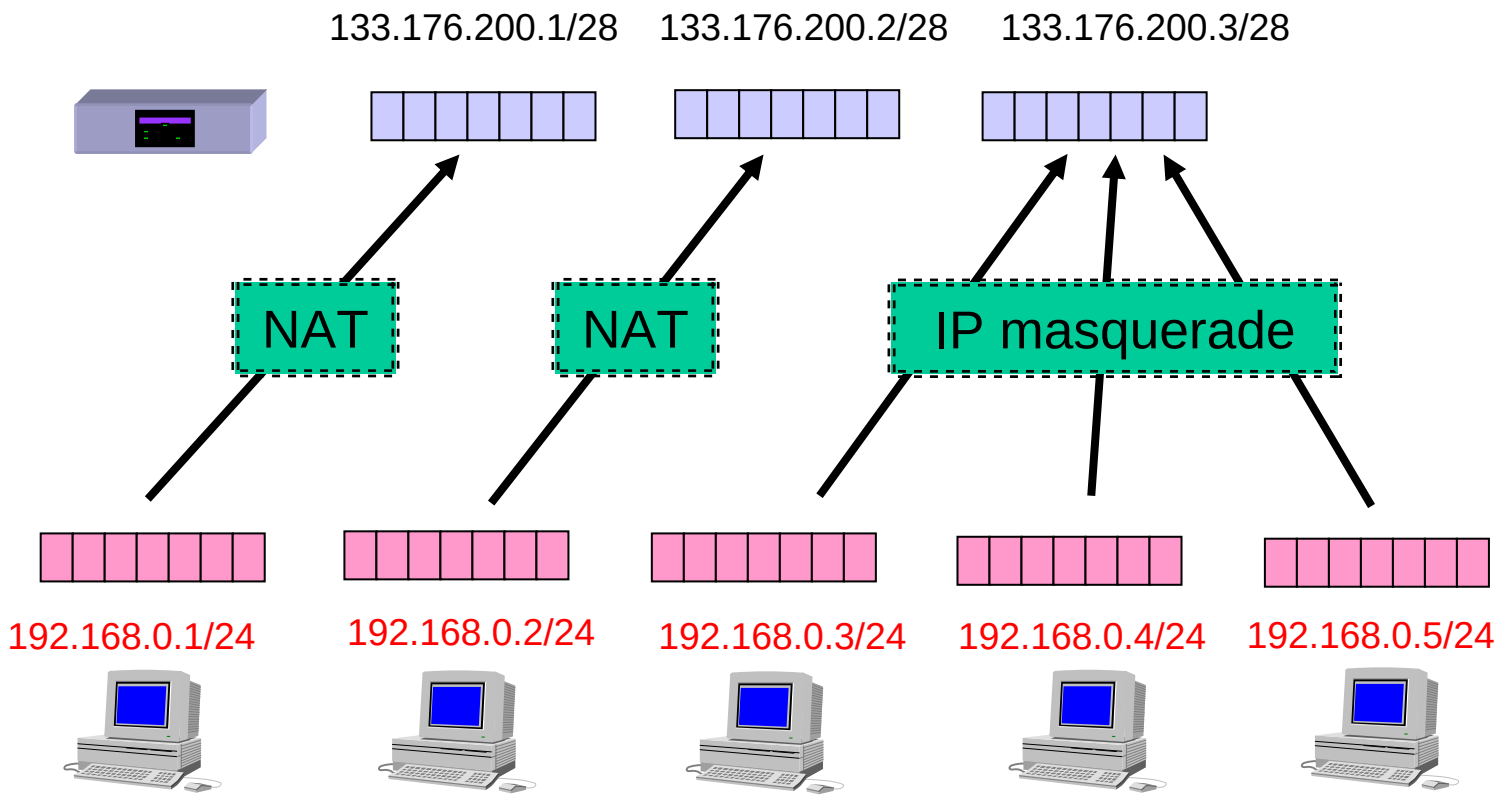
NAT (Network Address Translation)

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

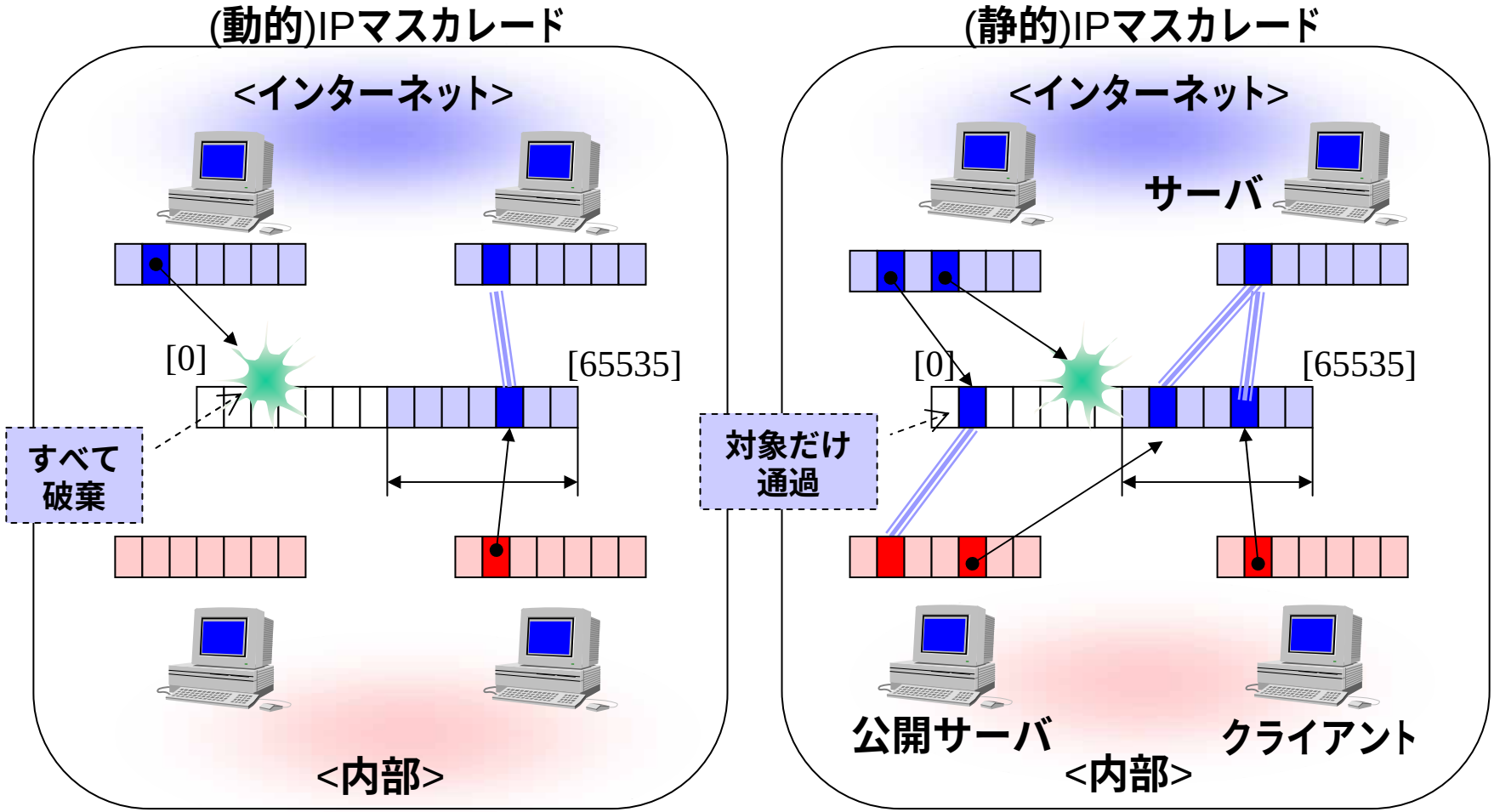


NAT + IPマスカレード形式

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



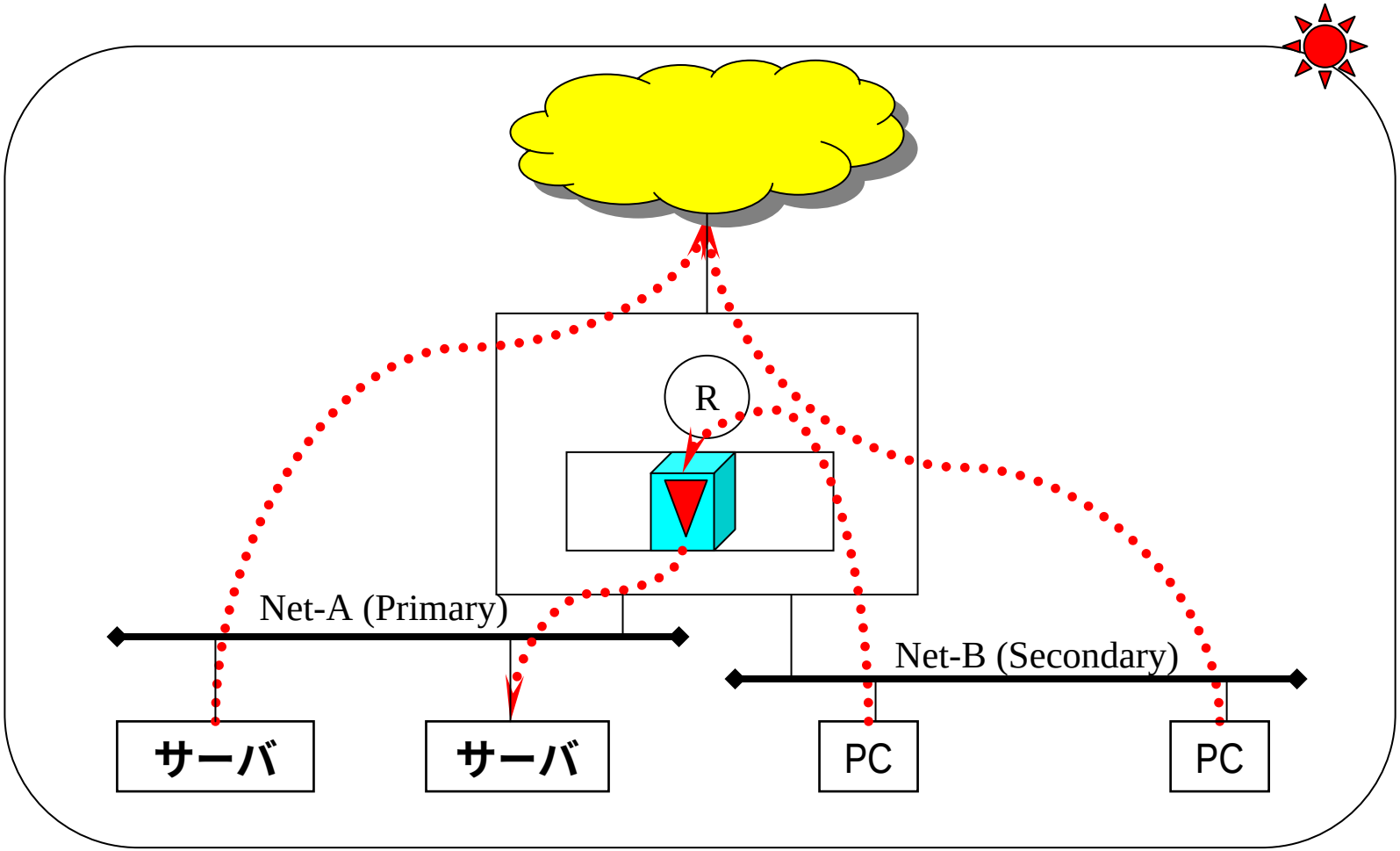
静的IPマスカレード



(静的IPマスカレード)

特定の通信だけ固定して、公開する。

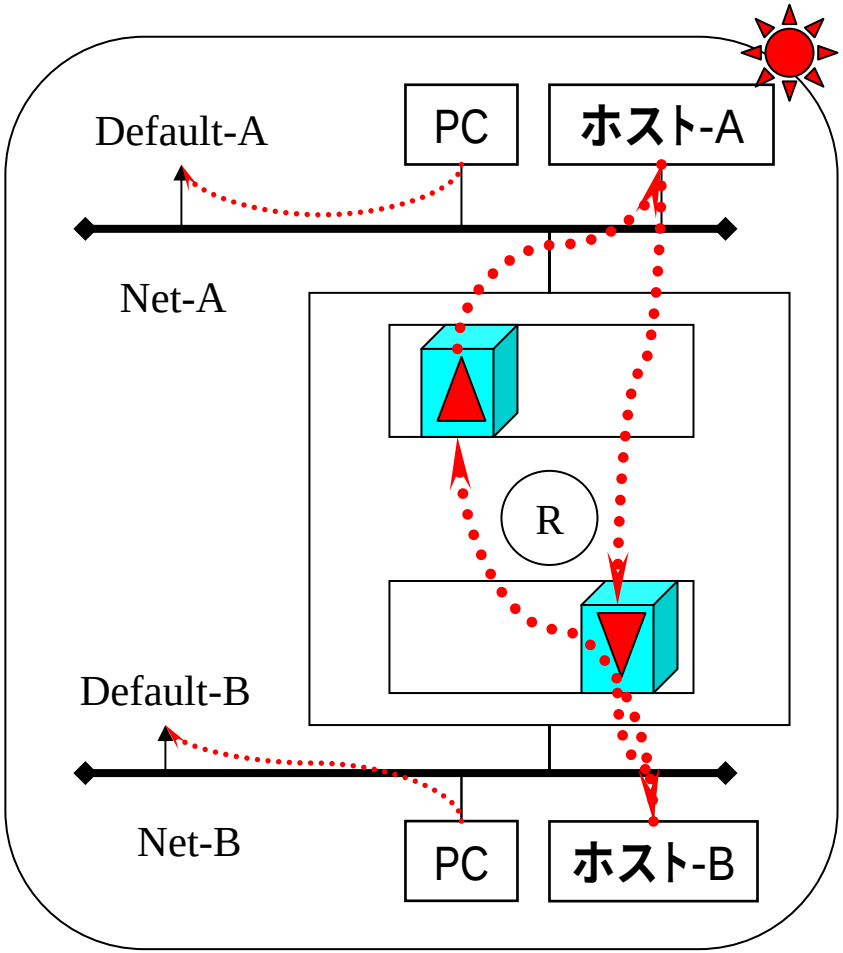
NATディスクリプタの応用例#1



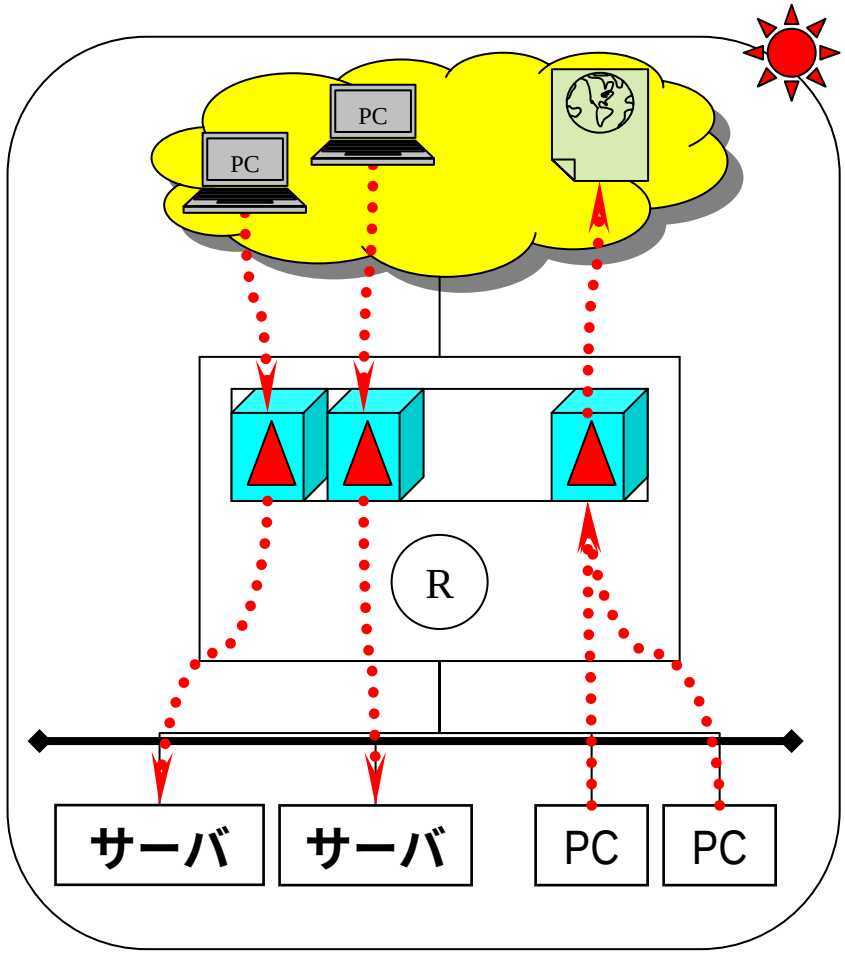
primary⇔secondary**間のIPマスカレード (逆マスカレード)**

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)

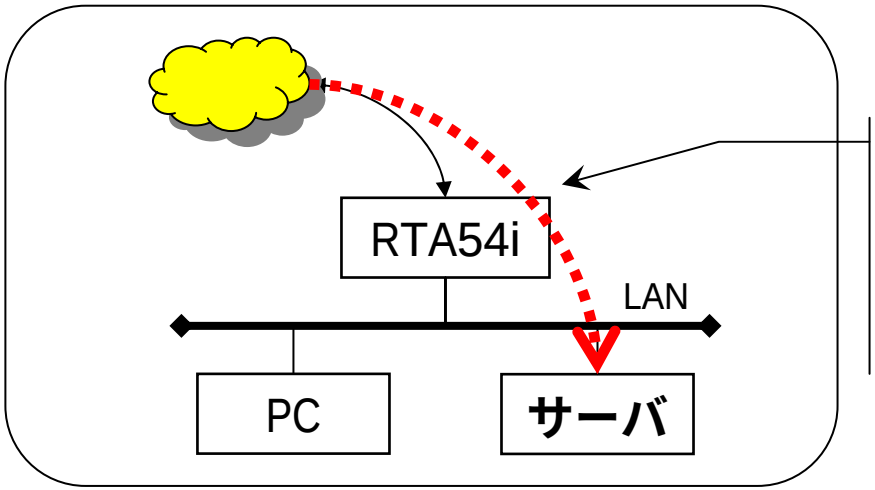


公開サーバにIPマスカレード適用

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

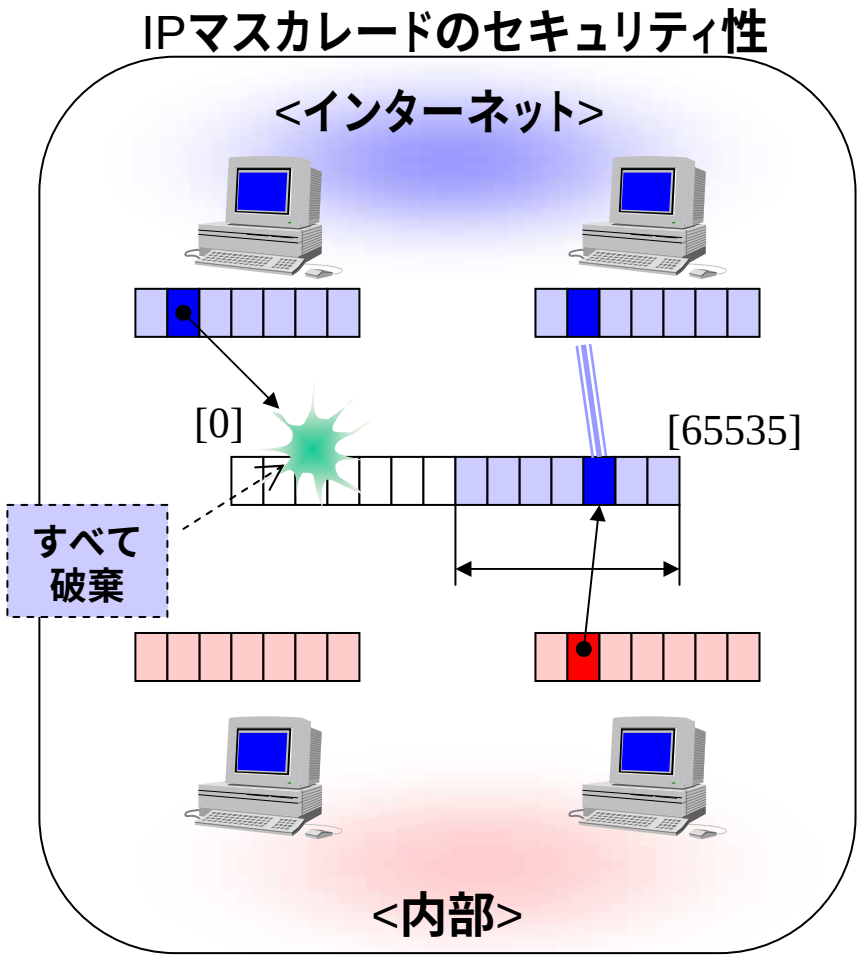
[入力形式] nat descriptor masquerade incoming DESC_ID ACTION [IP_ADDRESS]

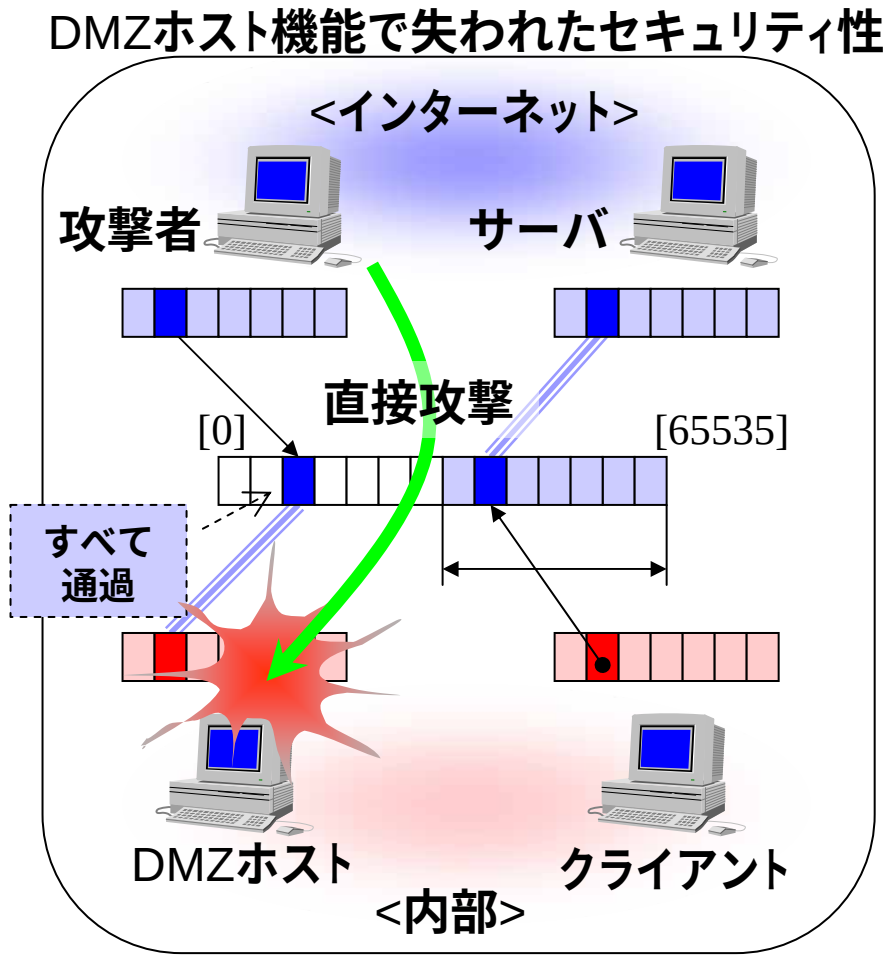
[パラメータ] - DESC_ID ..... NATディスクリプタ番号
- ACTION ..... 動作
  - through ... 変換せずに通す
  - reject .... 破棄して、TCPの場合はRSTを返す
  - discard ... 破棄して、何も返さない
  - forward ... 指定されたホストに転送する
- IP_ADDRESS ... 転送先のIPアドレス

[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



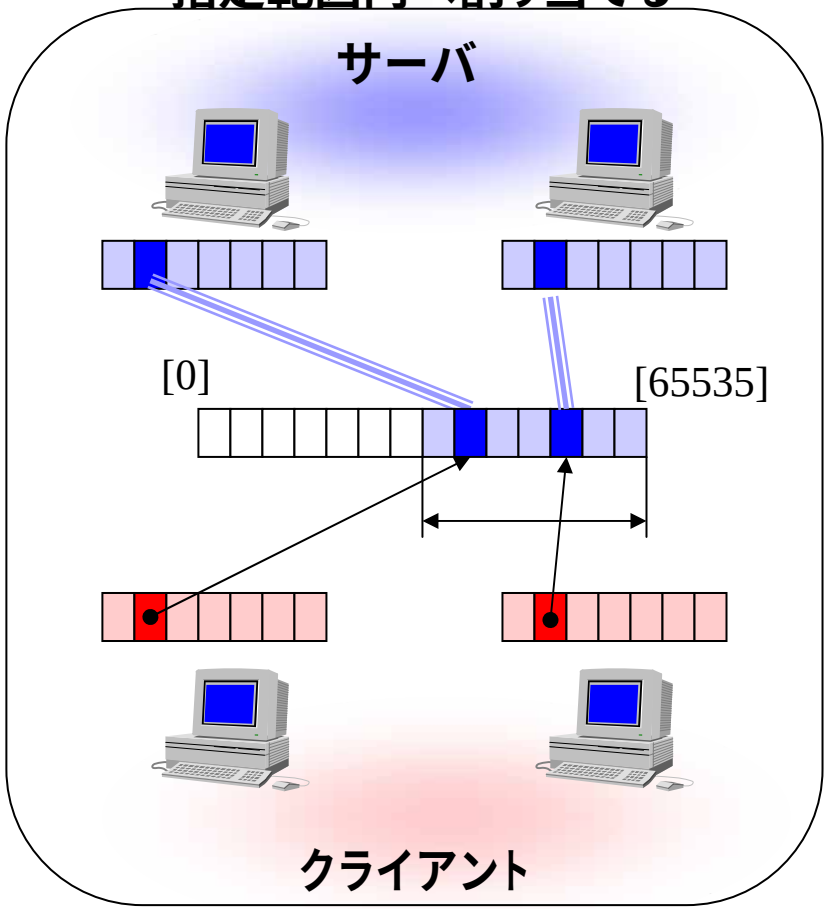


(利便性とセキュリティ性のトレードオフ)

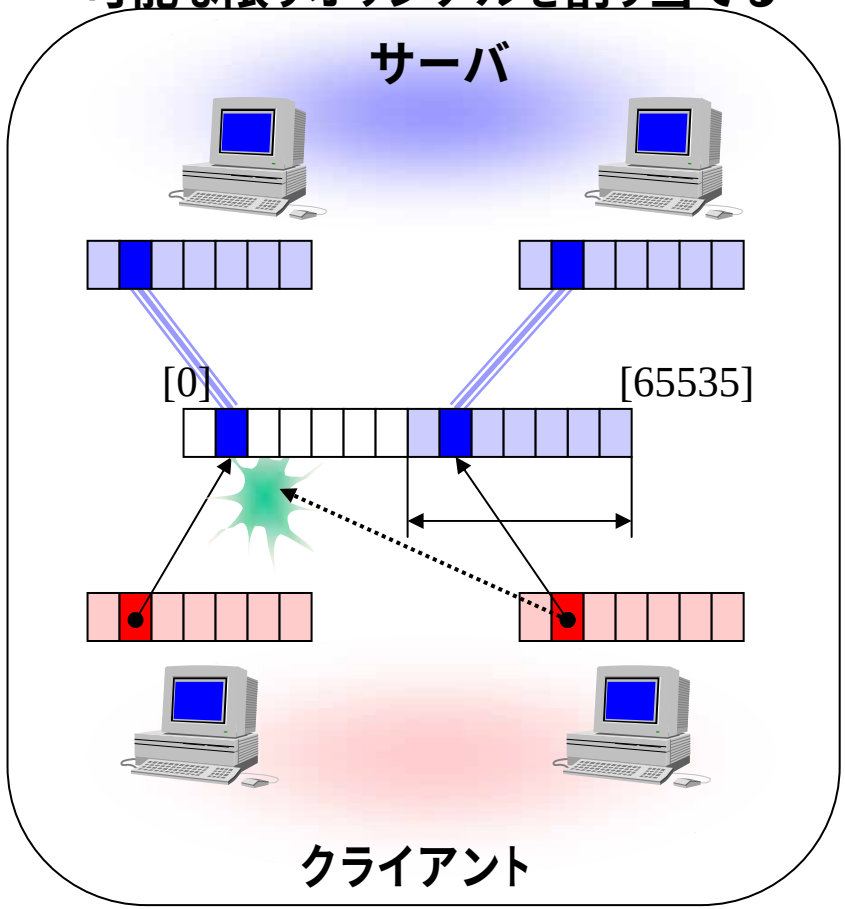
アドレス変換の苦手なアプリケーションが便利になるが、セキュリティ性は低下する。

ポート割当方式指定機能

指定範囲内へ割り当てる



可能な限りオリジナルを割り当てる



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]

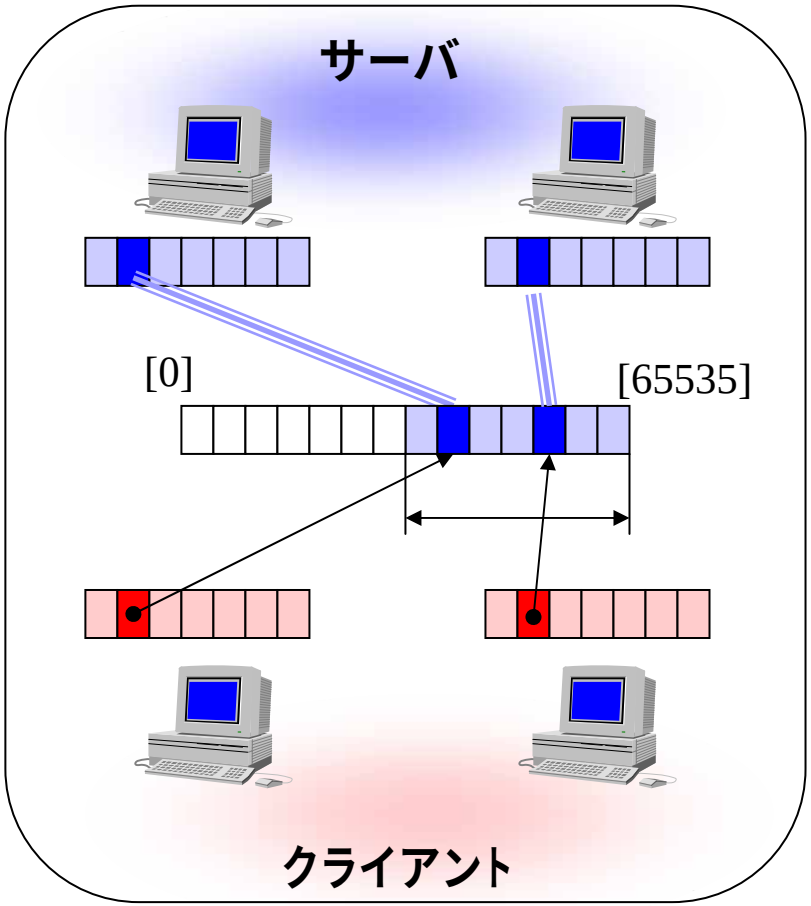
DESC ... ディスクリプタ番号
PROTOCOL ... プロトコル、'tcp'もしくは'udp'
PORT ... ポート番号の範囲

[説明]

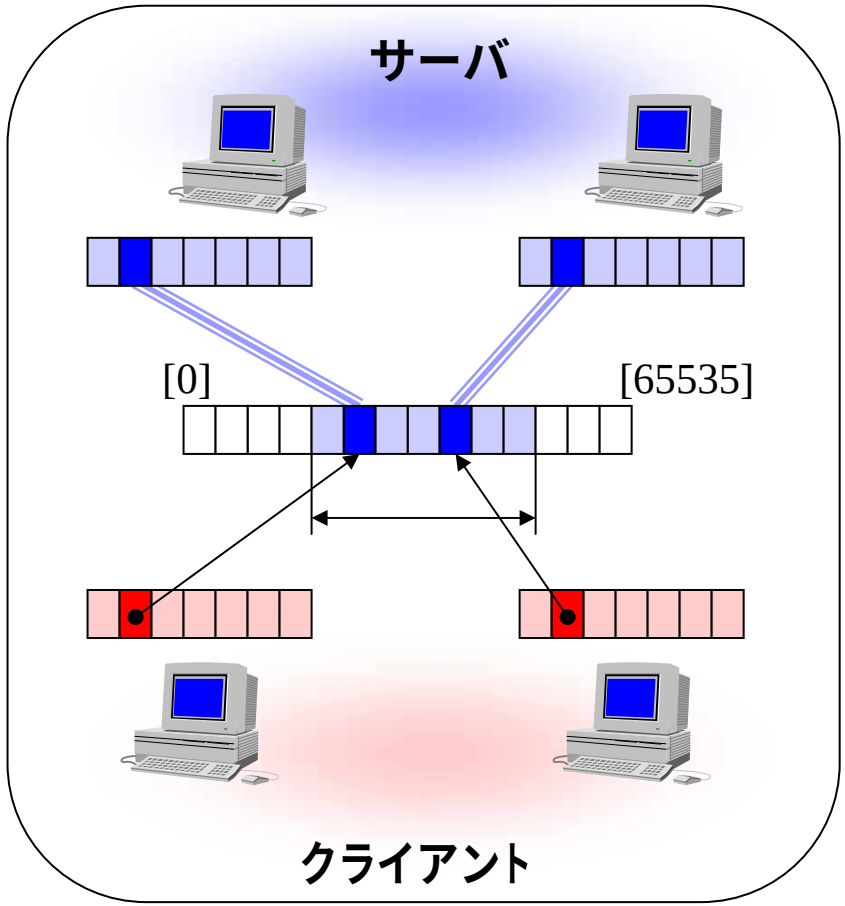
IPマスカレードで変換しないポート番号の範囲を設定する。
if-possibleが指定されている時には、処理しようとするポート番号が他の通信で使われていない場合には値を変換せずそのまま利用する。

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

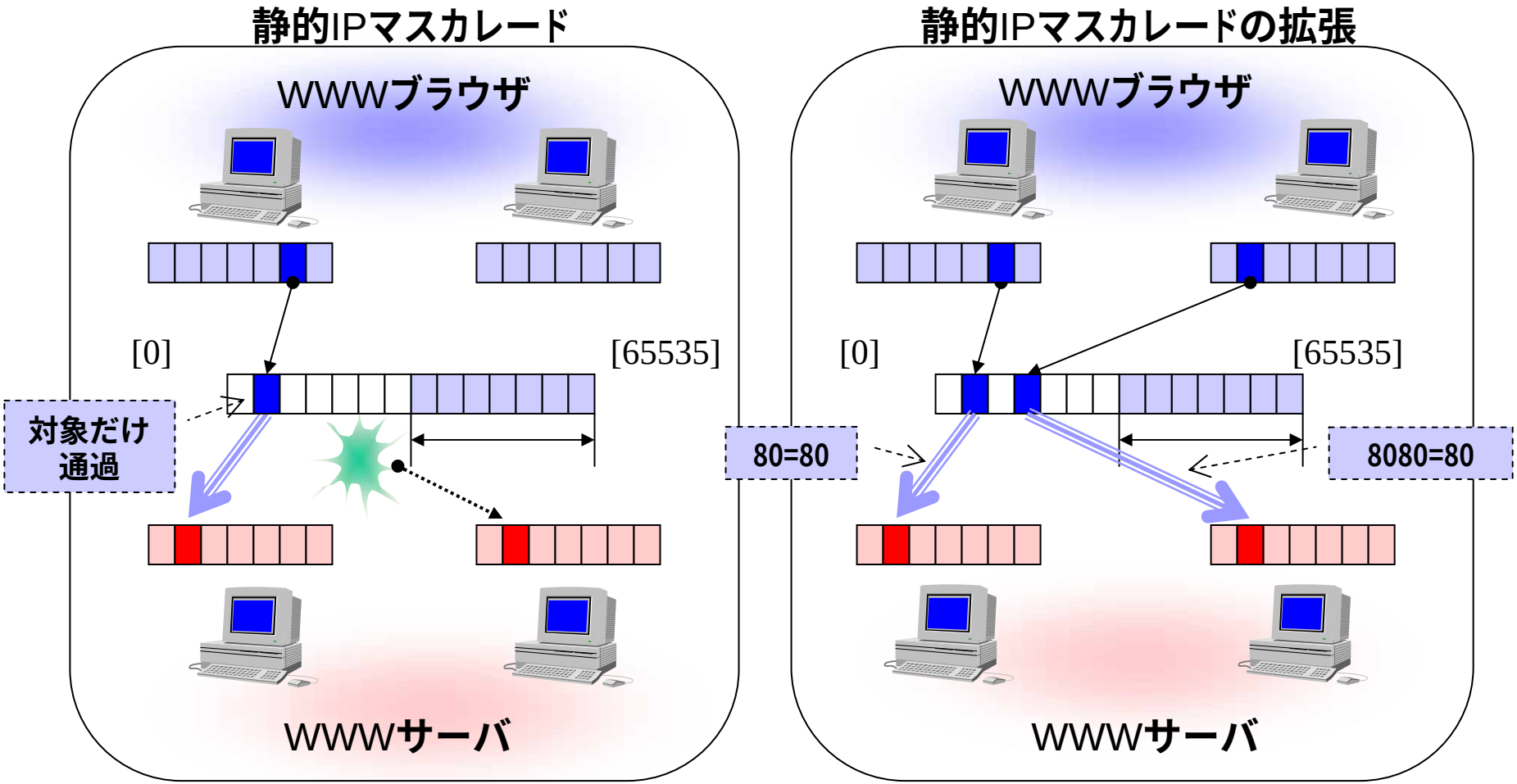
[説明]

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]

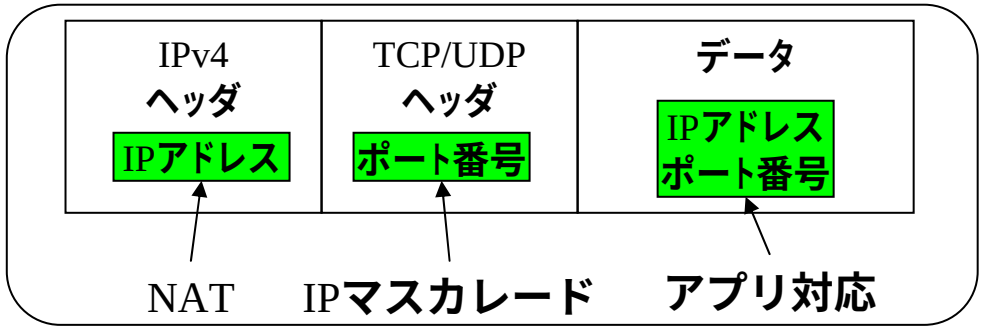
IPマスカレードによる通信でポート番号変換をしないように固定する。
また、外側ポートと内側ポートの関連付けも可能。

IPマスカレードのアプリケーション対応

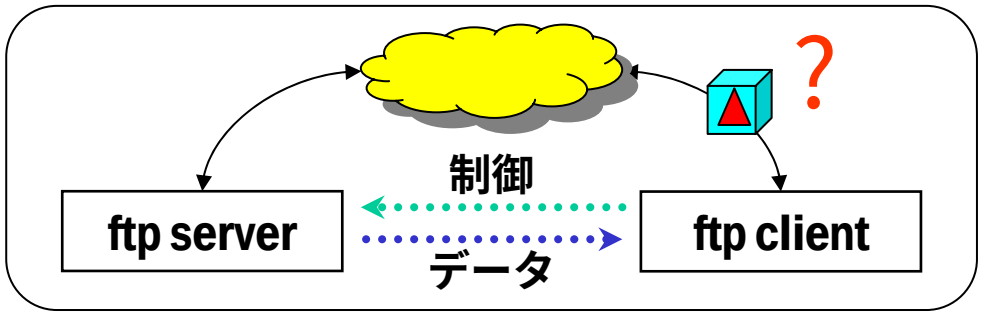
- FTP対応
  - FTP/アプリケーション対応の必要性
  - FTPセッション保持機能
  - FTP監視ポート指定機能
- NetMeeting 3.0対応
  - 可能な限りポート番号変換しない処理
- VPNパススルー機能
  - 同時1セッション、静的IPマスカレードの制限緩和
- PPTPのマルチセッション対応

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

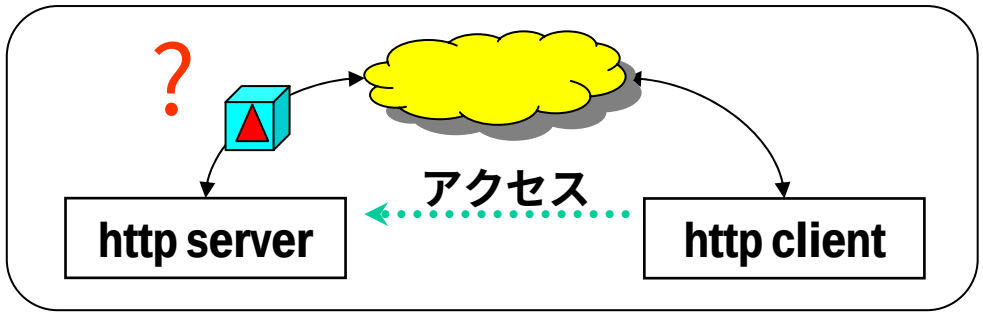


②複数のコネクションが利用される(異なる方向)



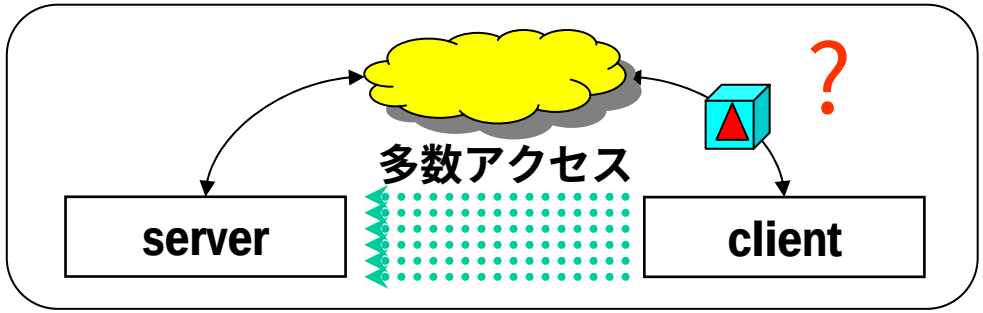
ftpのアクティブ転送(PORTコマンド)

③サーバ公開(サービス公開)

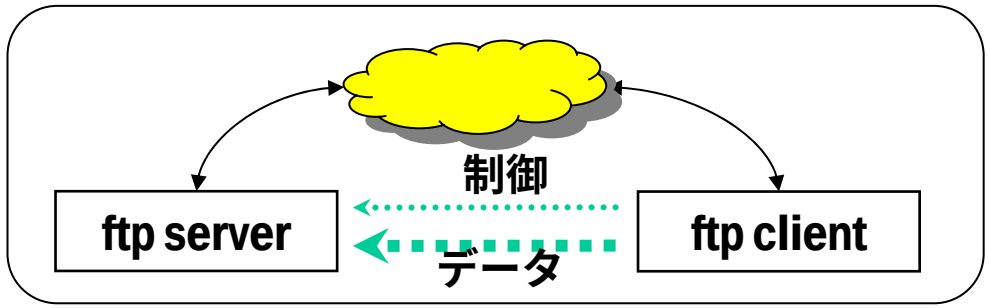


アプリケーション対応の概要#2

④同時多数接続を行うアプリケーション

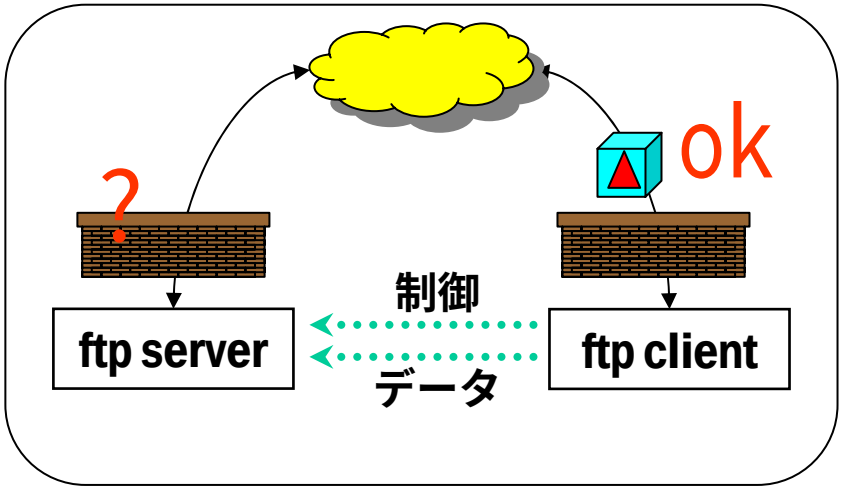


⑤複数のコネクションが利用される
(利用状態が不均一)

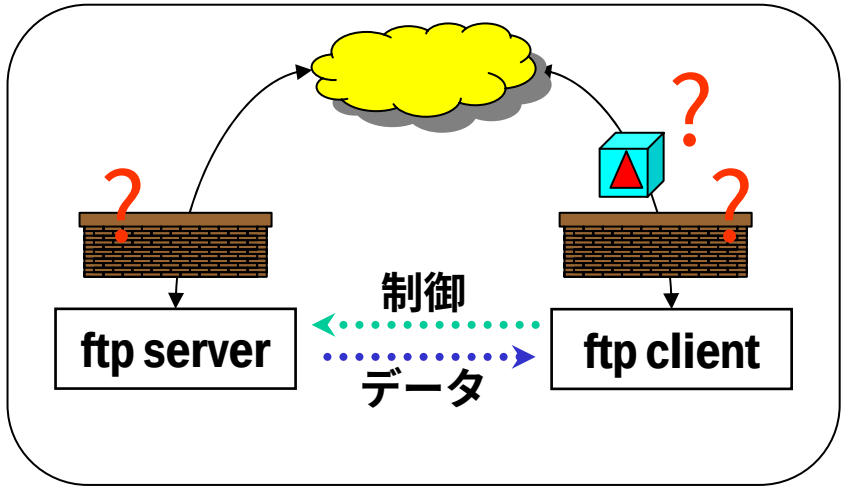


ftpのパッシブ転送(PASVコマンド)

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]

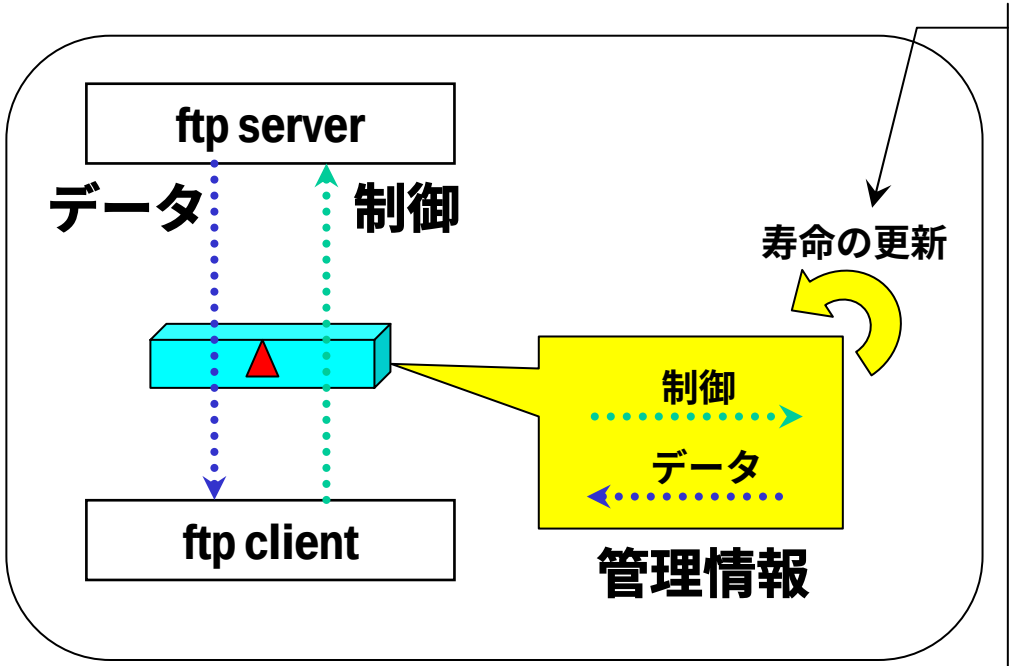
・アプリ/機能を実現するために複数のコネクションが必要

・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, …

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

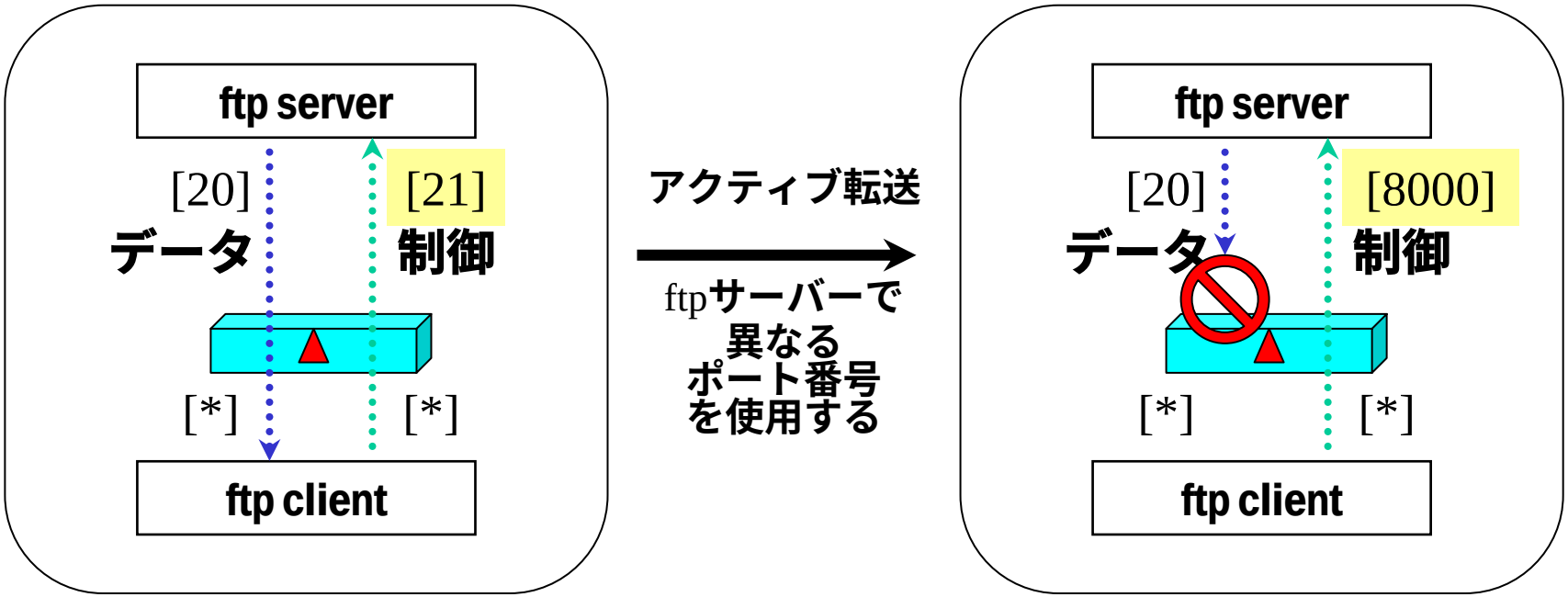
[説明]

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

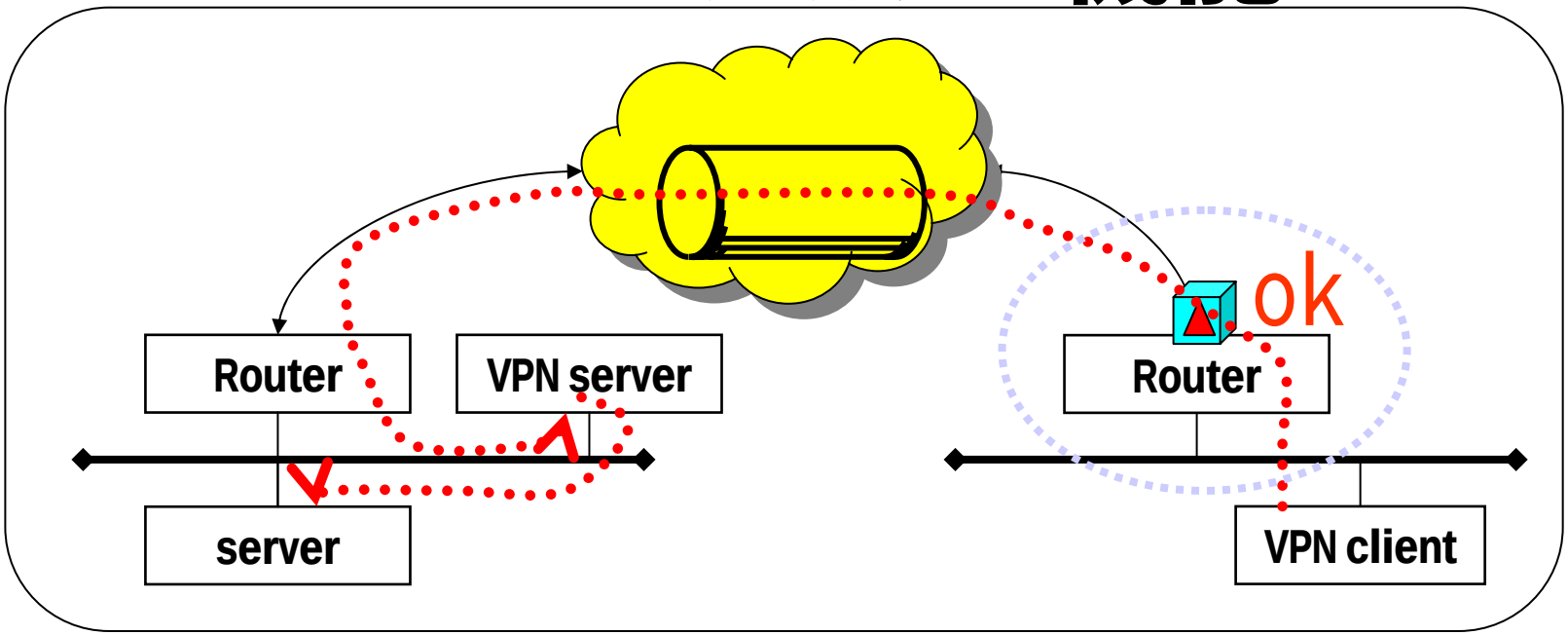
[説明]

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

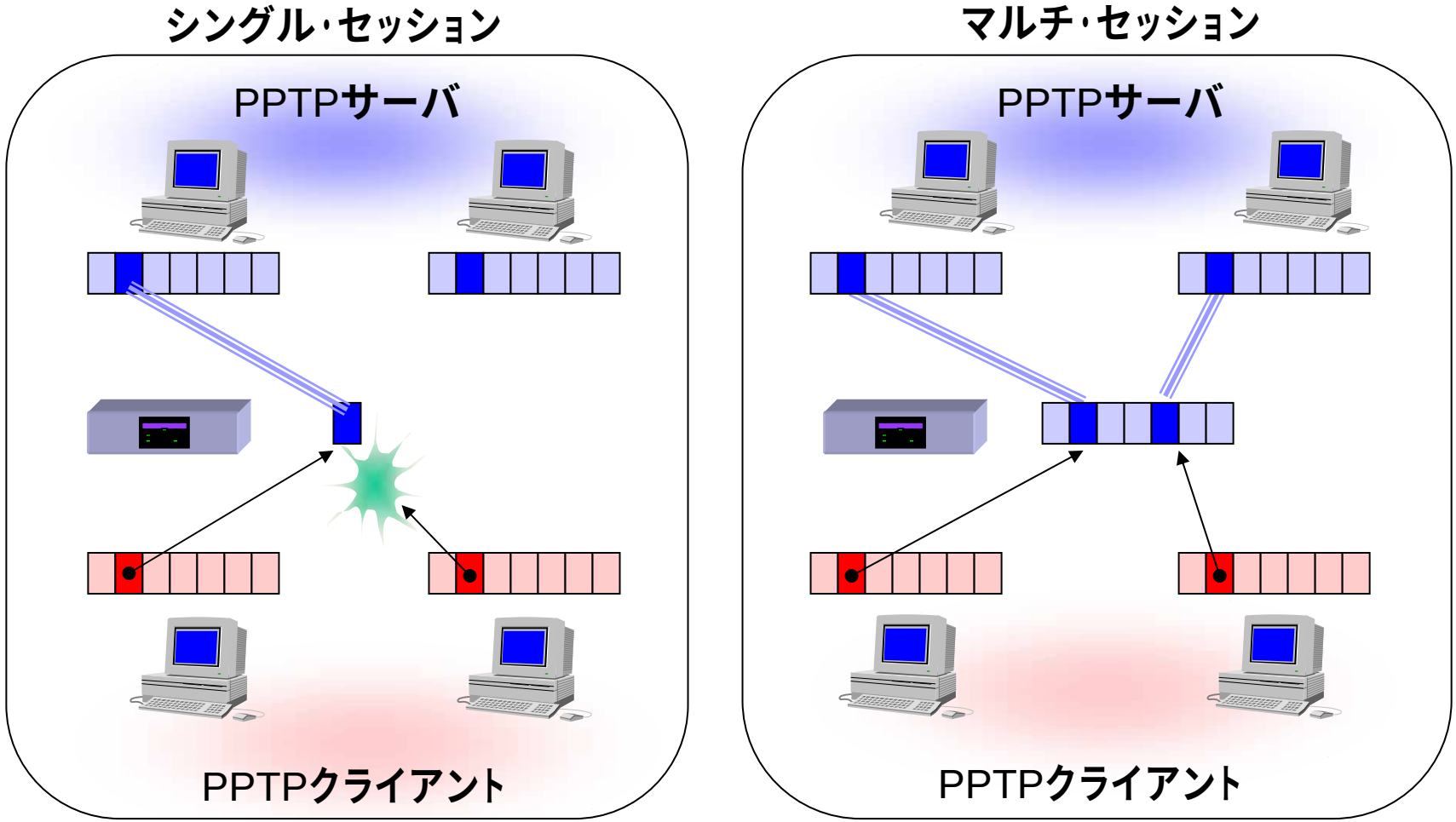


VPNやIPv6トンネルのためにICMP,TCP,UDPとは異なるプロトコルが利用される。これらのプロトコルに対しても、アドレス変換を行う機能。

⇒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)

PPTPのマルチセッション対応



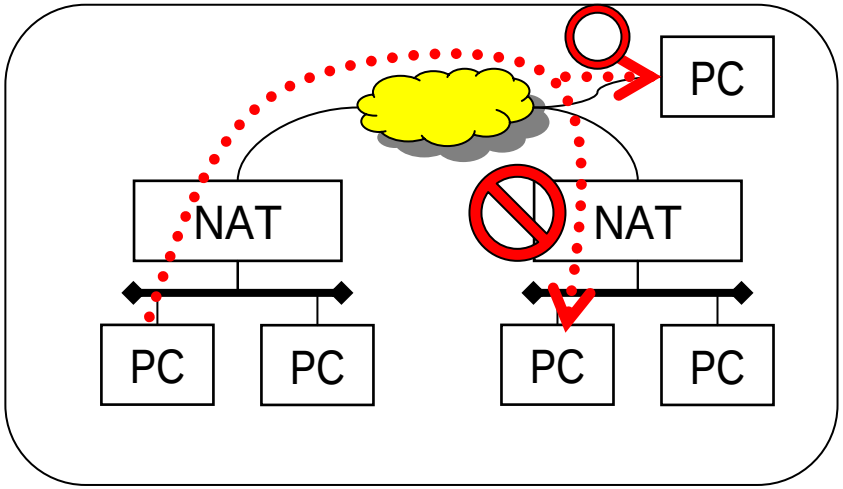
・同時に複数のMicrosoft VPN通信(PPTPによるVPN)が可能となる

PPTPのマルチセッション対応の仕様

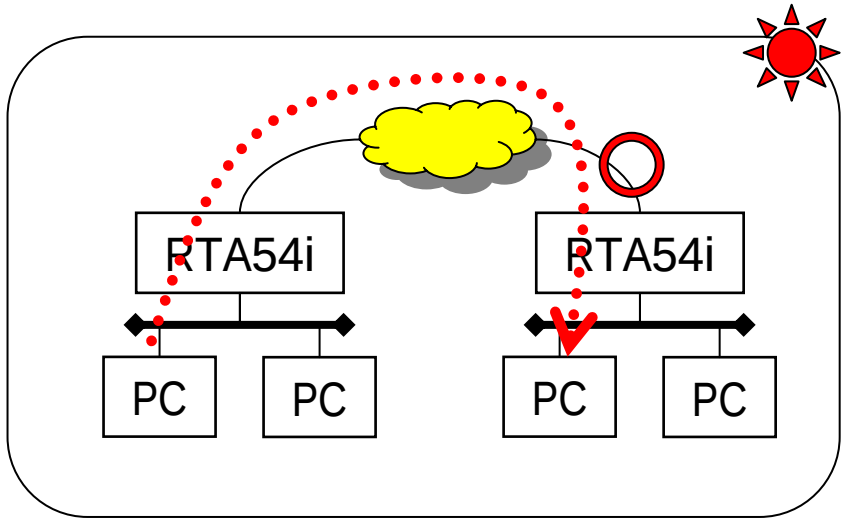
IPマスカレードを動作させている時に、PPTPによるMicrosoft VPNを変換できるようにした。ルータ、Windows PC、Windows サーバのすべてで特別な設定は必要なく、IPマスカレードの内側(プライベートアドレス側)にあるPPTPクライアントである Windows PCから外側(グローバルアドレス側)にあるPPTP サーバであるWindows サーバとの間にPPTPによるVPNトンネルを通常の動作で設定できる。

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/

ファイアウォール機能
(パケット・フィルタリング)

1) ファイアウォールの要素、優位点
2) 静的フィルタリング
3) 静的セキュリティ・フィルタ
4) 不正アクセス検知
5) 動的フィルタリング
6) ネットボランチのセキュリティ・レベル
7) 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
   ・動的セキュリティ・フィルタ

付録資料

常時接続時代のセキュリティ

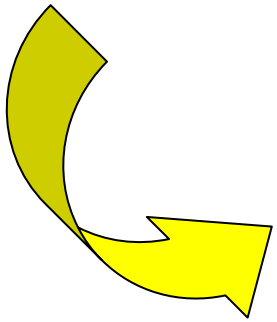
- 静的&動的パケットフィルタリング
  メモリの許す限り無制限
- 不正アクセス検知機能(IDS)
- サービス停止機能、ステルス機能
- 豊富な情報と設定例

[RTA55i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

ファイアウォールの要素

[必須]
- 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(無制限)
- VPNへの適用
- 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優位点

- **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、まず、パスワード設定

- **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

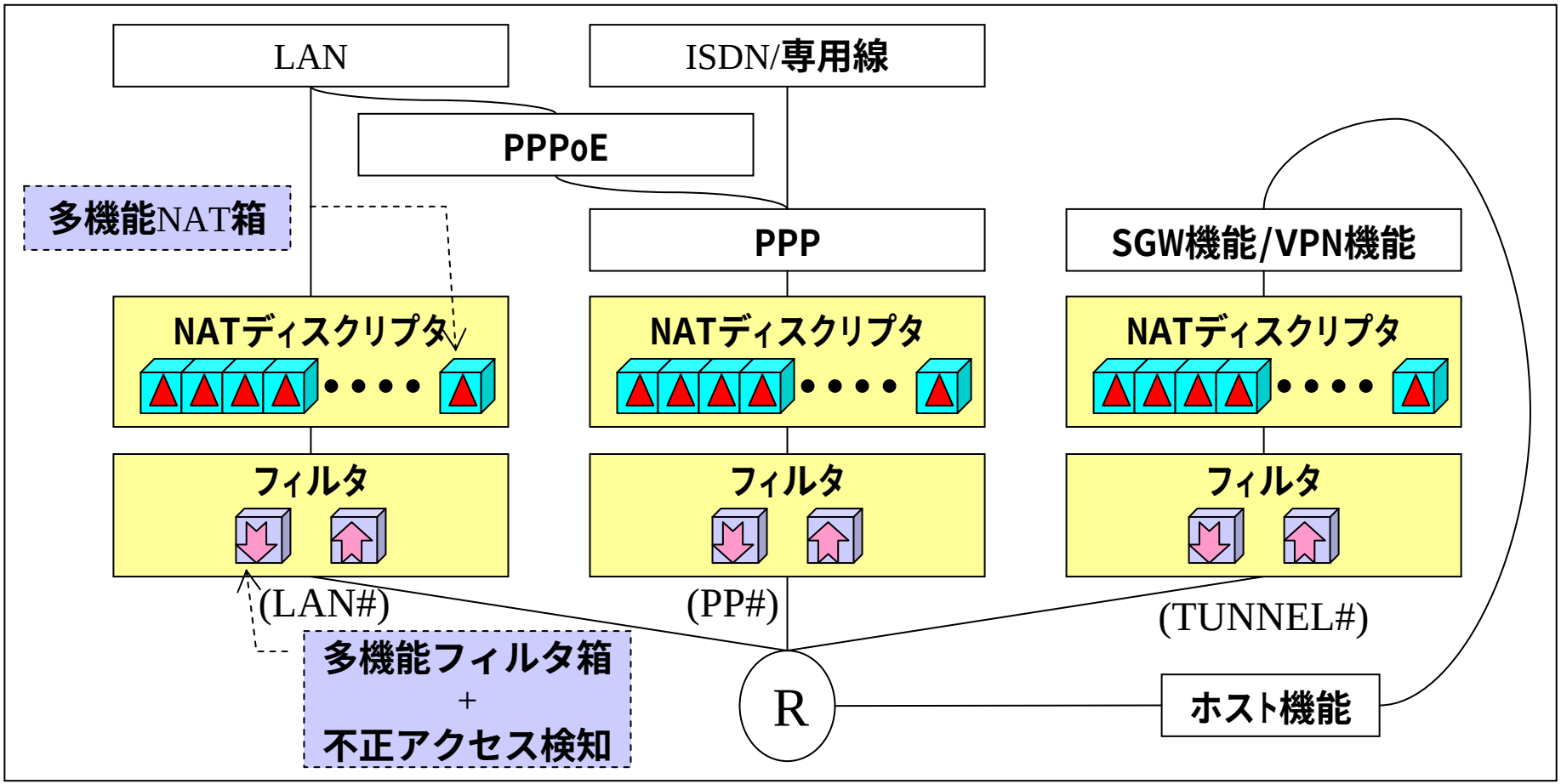
  侵入(Intrusion)や攻撃(attack)を目的とするパケットを受信したときに、それを検出してユーザに通知(ログ、ブザー、メール)

- **フレキシビリティ**

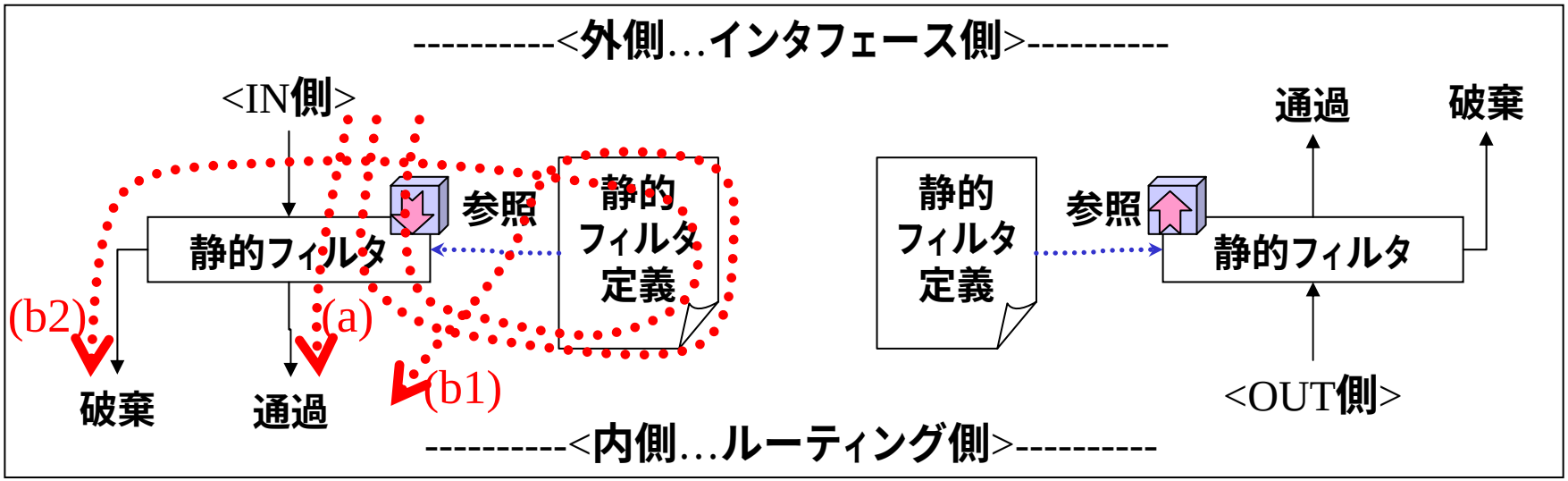
  a) フィルタ定義数の制限緩和(メモリの許す限り)

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



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。

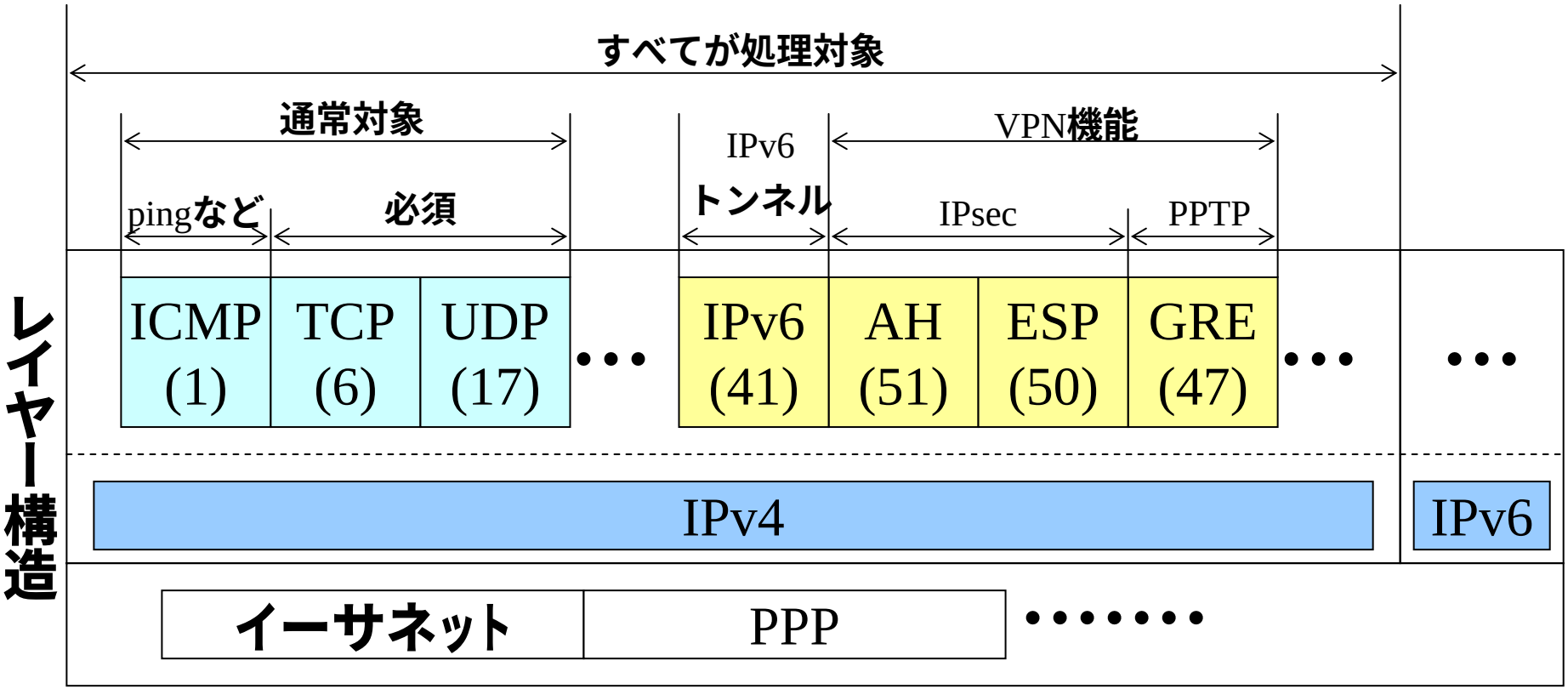
b) フィルタに何か適用されている場合、パケット単位で、

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。

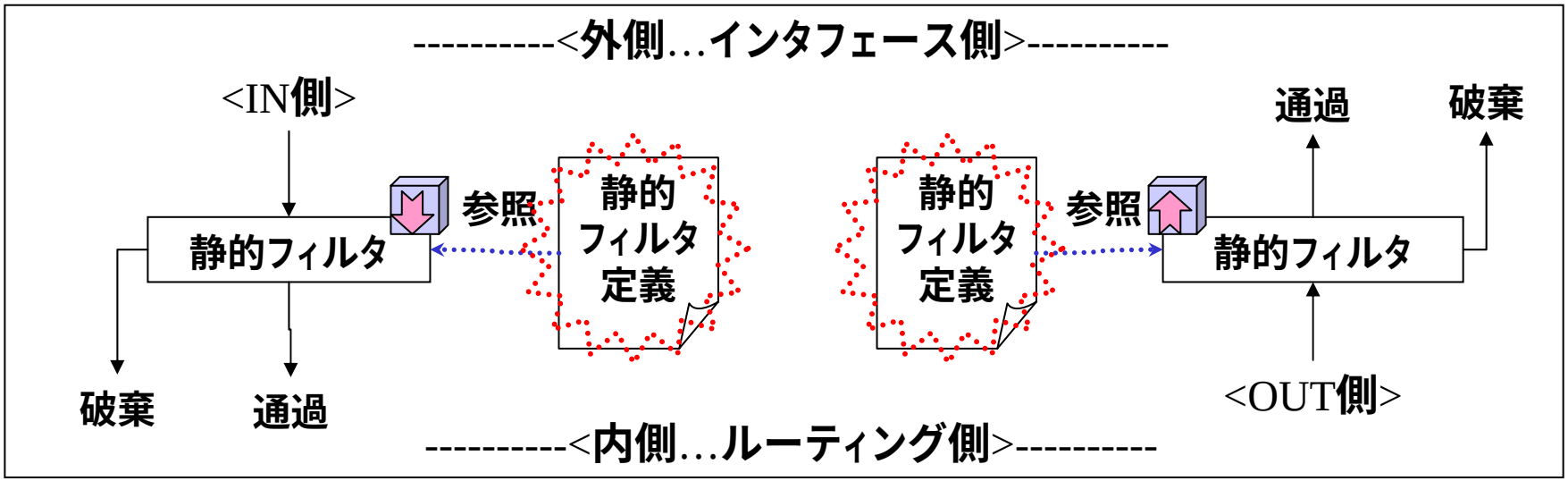


静的フィルタのタイプ

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/IPv6/AH/ESP/GRE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)

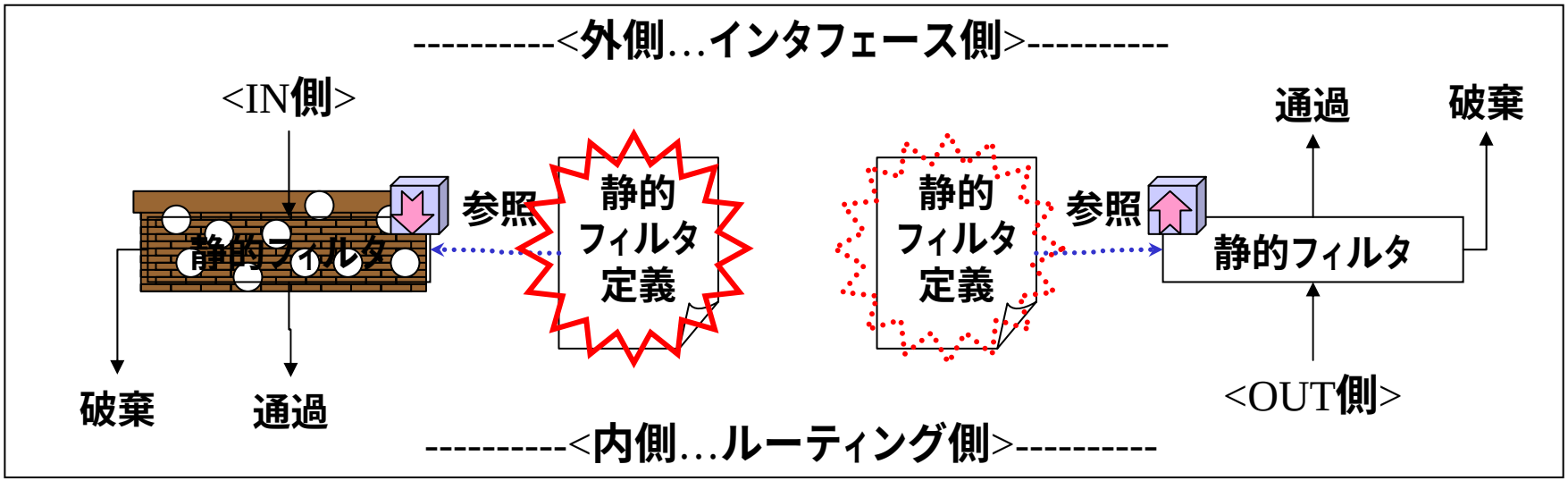
http://www.rtpro.yamaha.co.jp/RT/FAQ/IP-Filter/ip-packet-filter.html

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

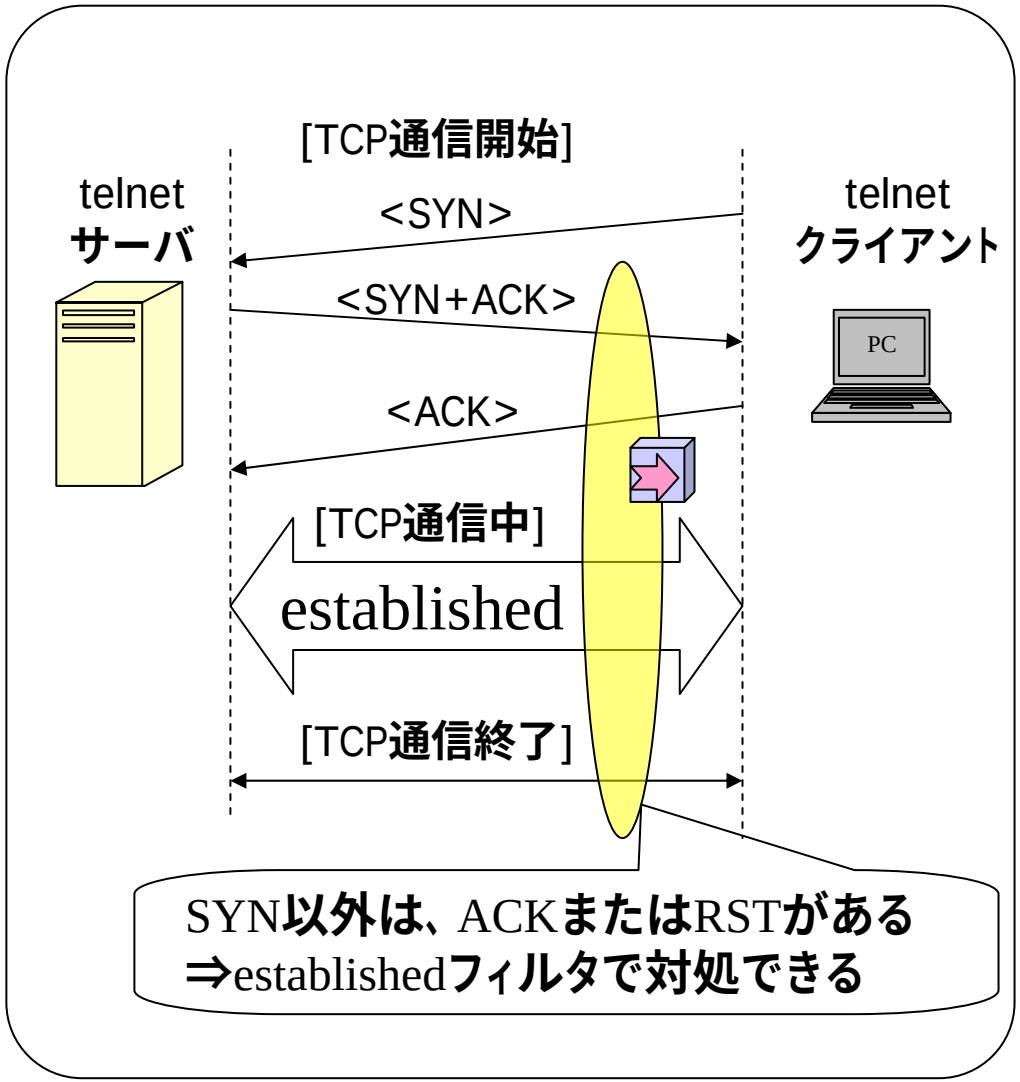
http://www.rtpro.yamaha.co.jp/RT/FAQ/IP-Filter/network-security-filter.html

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



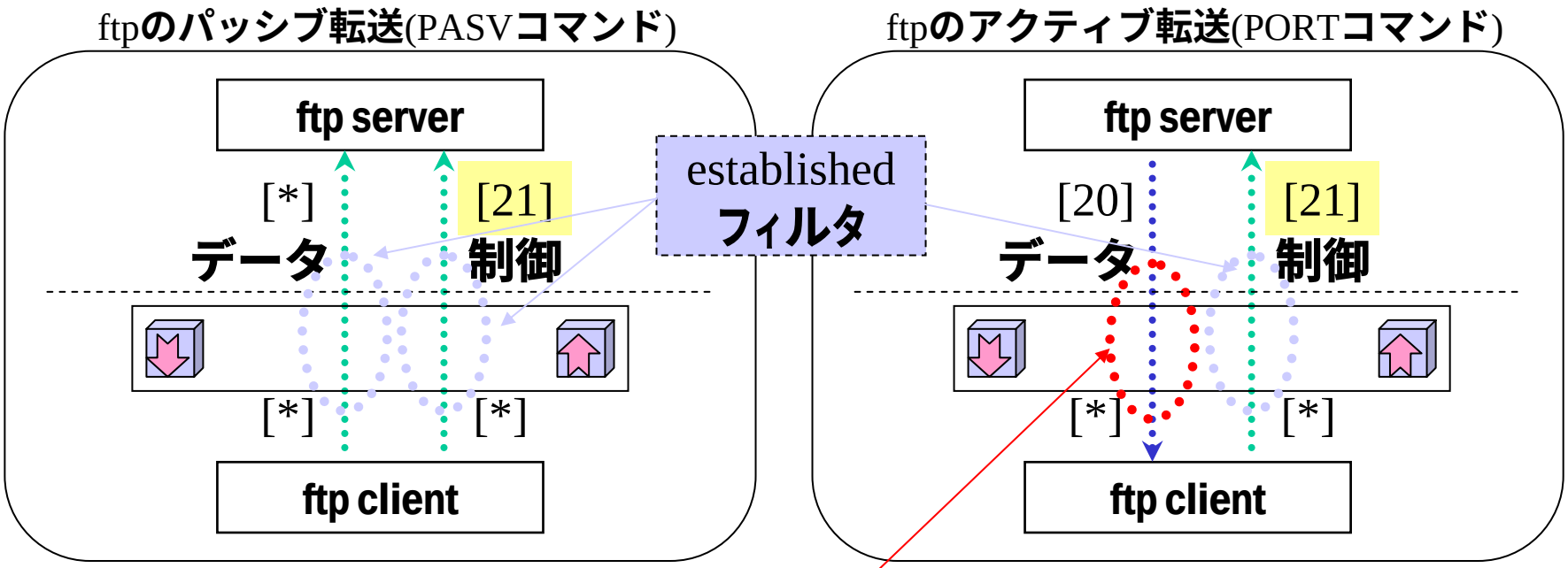
[目的]
- 静的フィルタリングにより外部からの不必要なTCP接続要求を破棄する。

[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

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。

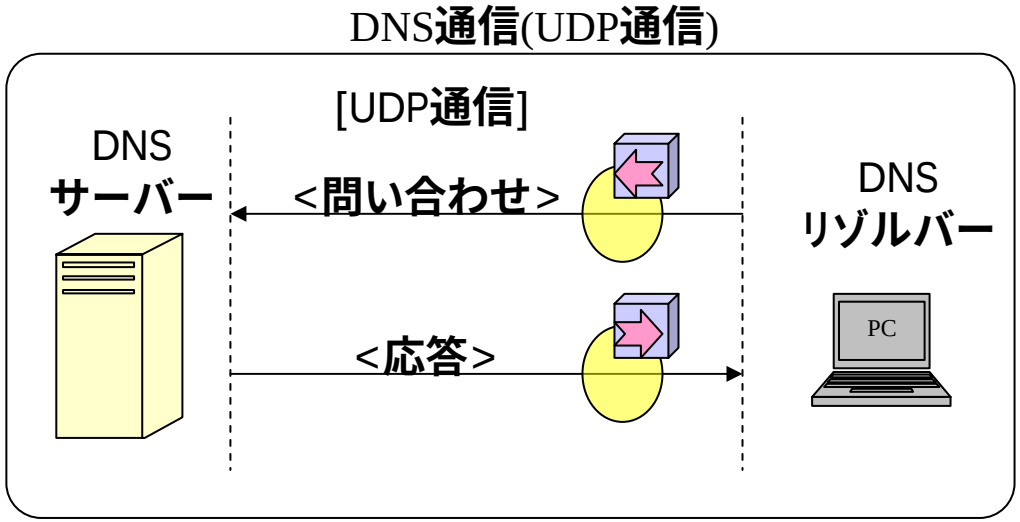
[解決策]

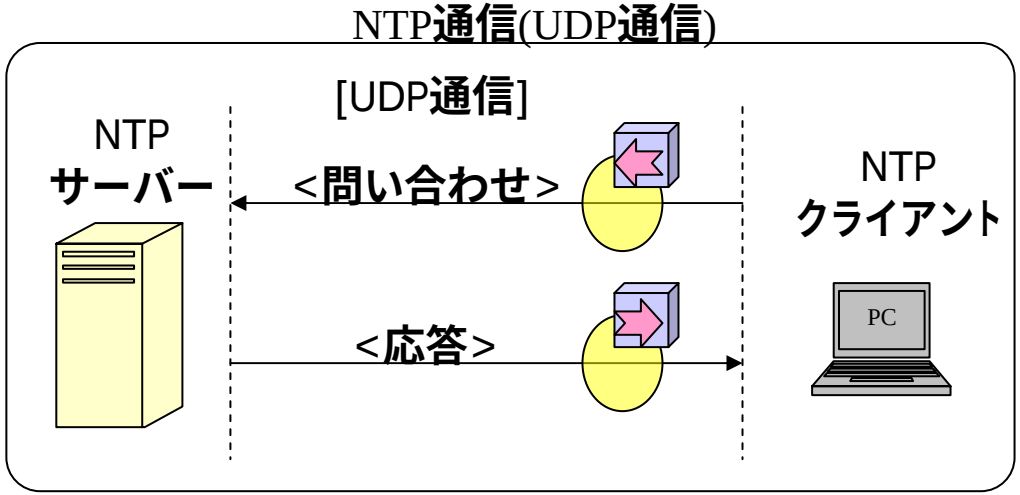
・動的フィルタリング

・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

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

不正アクセス検知の特徴

[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

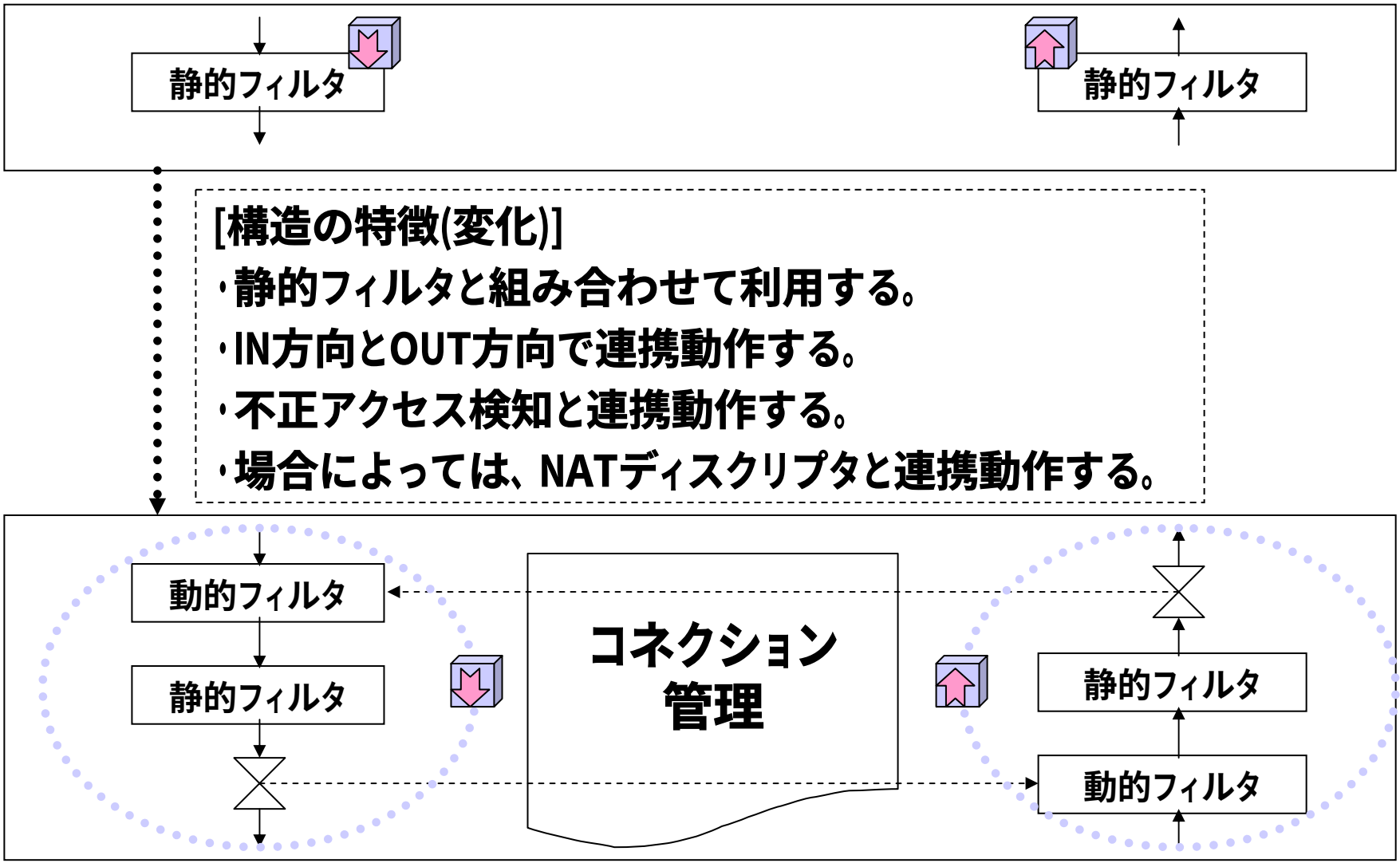
種別	名称	判定条件	
FTP	FTP improper port	PORTやPASVコマンドで指定されるポート番号が1024〜65535の範囲でないとき	★
SMTP	SMTP pipe attack	From:などのヘッダにパイプ「|」を含むとき	★
	SMTP decode alias	ヘッダに「: decode@」を含むとき	★
	SMTP DEBUG command	DEBUGコマンドを受信したとき	★
	SMTP EXPN command	EXPNコマンドを受信したとき	★
	SMTP VRFY command	VRFYコマンドを受信したとき	★
	SMTP WIZ command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

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
・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

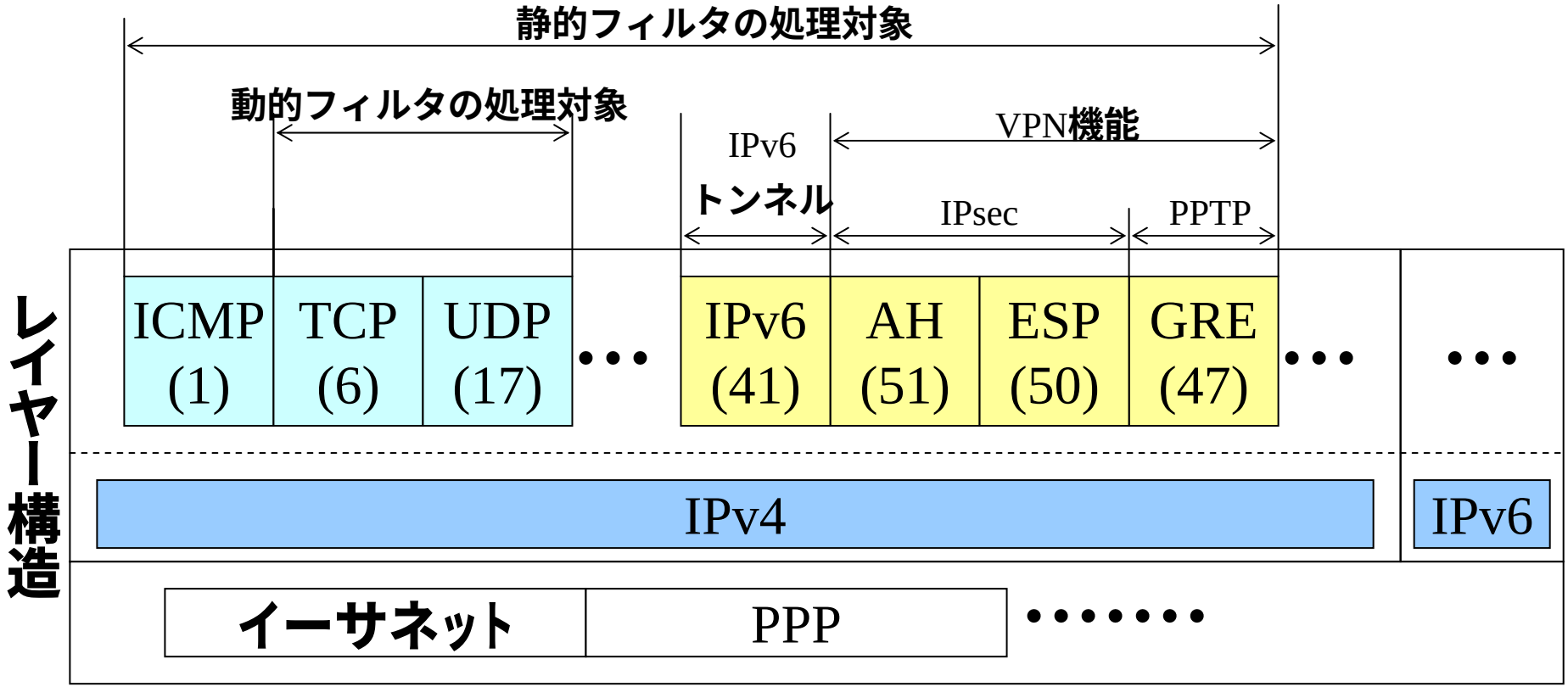
[静的フィルタリングの弱点]
・安全性と安定性を確保した十分なフィルタリングを行うためには、
高度な知識が求められる。
・ftp通信のフィルタリングにおける安全性
・UDP通信のためのフィルタの安全性
・TCP通信のためのestablishedフィルタの安全性

動的フィルタリング構造の特徴

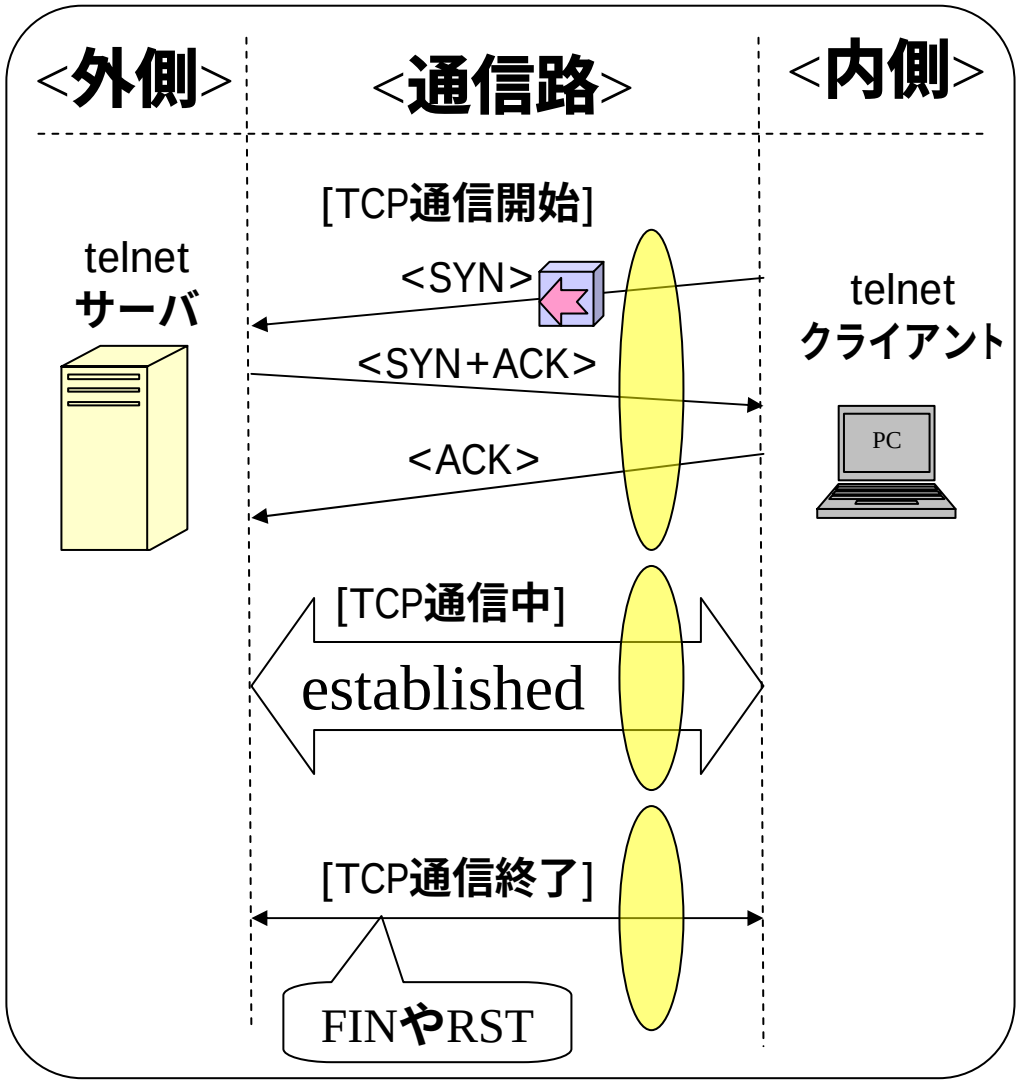


動的フィルタリングの処理対象

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。



TCPの動的フィルタ (基本動作)

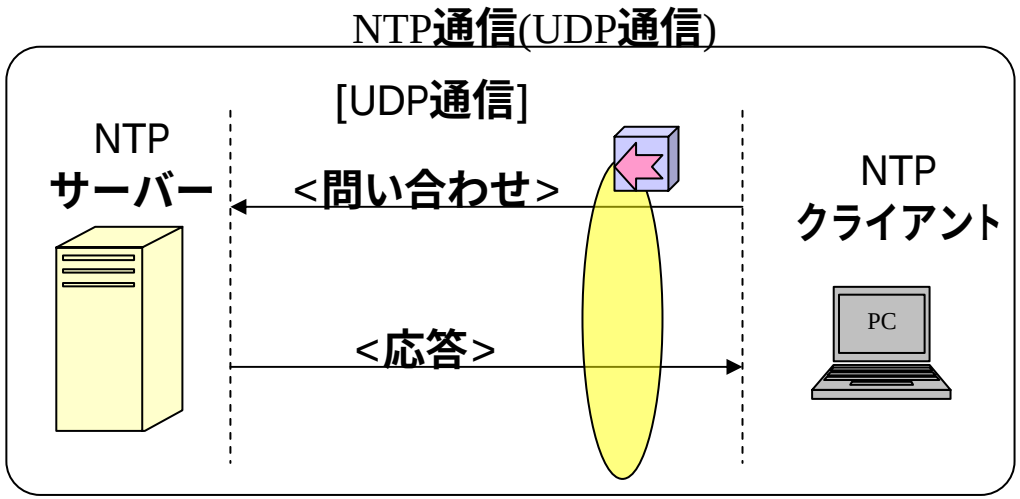


[開くトリガー]
- コネクションを開くSYN情報を持ったパケット

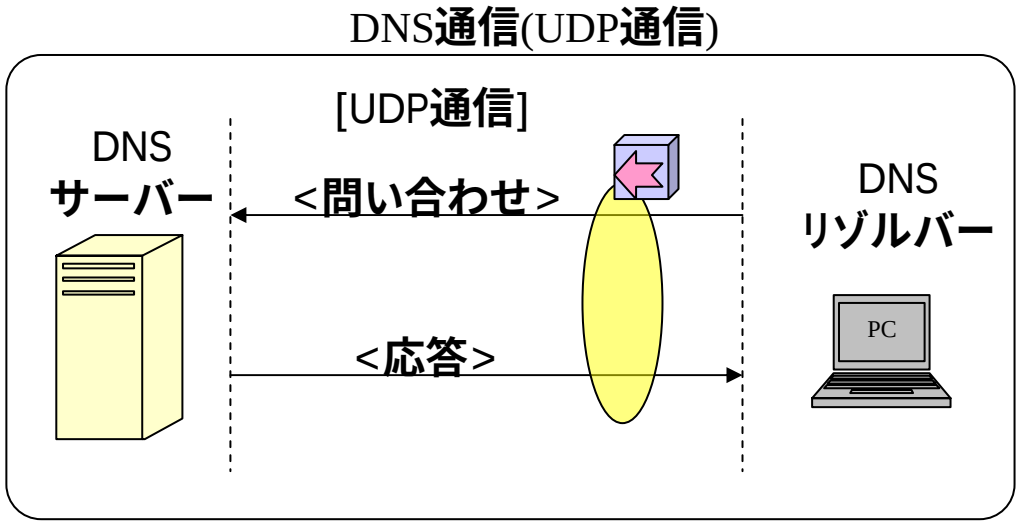
[確立の監視]
- TCPコネクションを開始するハンドシェイクの監視

[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

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。

動的フィルタのアプリケーション名

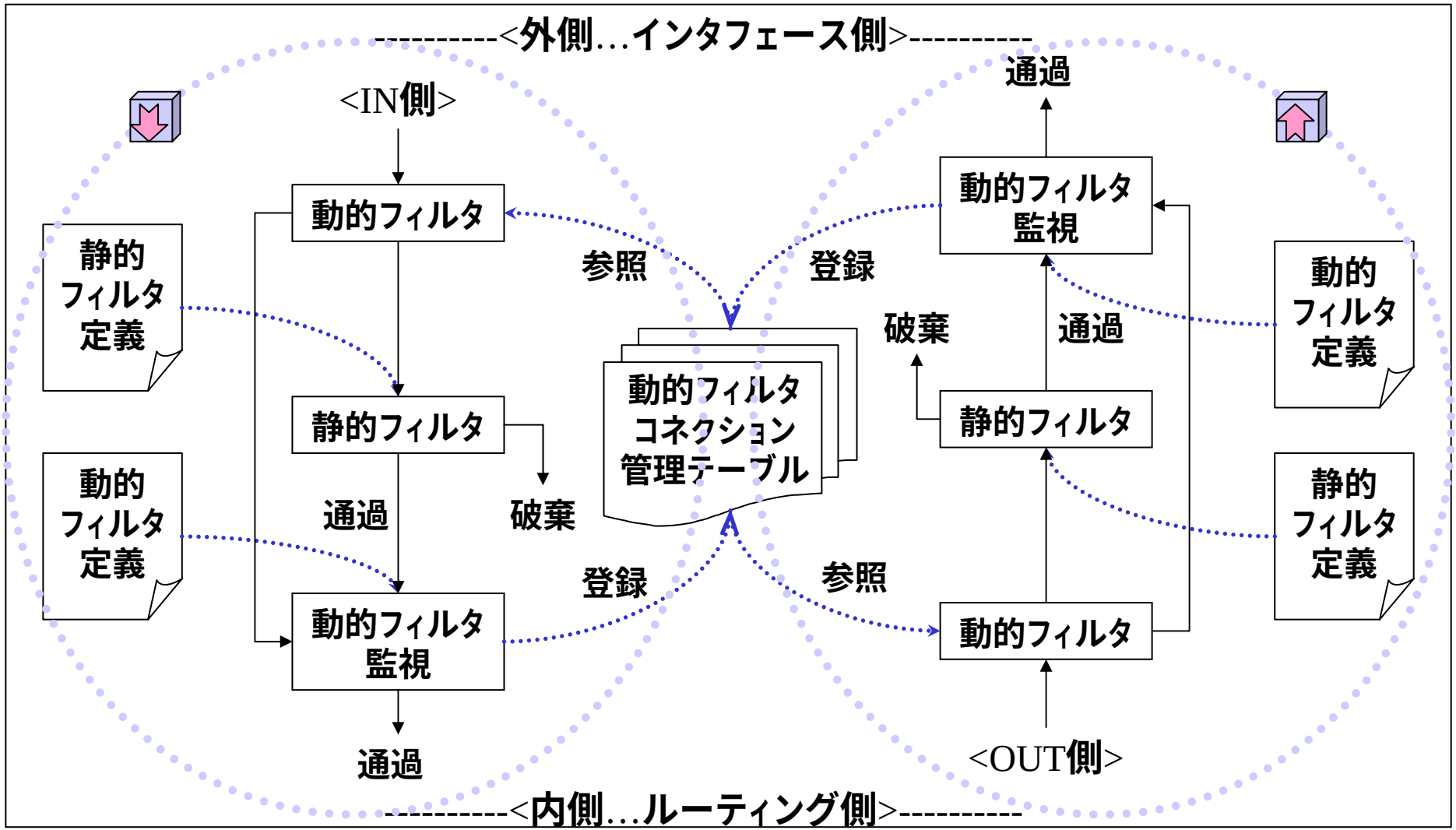
名称	プロトコル	説明
tcp	tcp	一般的なtcp通信 (コネクションの確立など)
udp	udp	一般的なudp通信(タイマーによる監視など)
ftp	tcp	ftp通信
tftp	udp	tftp通信
domain	udp(tcp)	DNS通信
www	tcp	www通信
smtp	tcp	電子メール(送信)
pop3	tcp	電子メール(受信)
telnet	tcp	telnet通信
netmeeting	tcp,udp	NetMeeting 3.0の通信
自由定義	tcp,udp	トリガー監視、順方向、逆方向を自由定義

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)

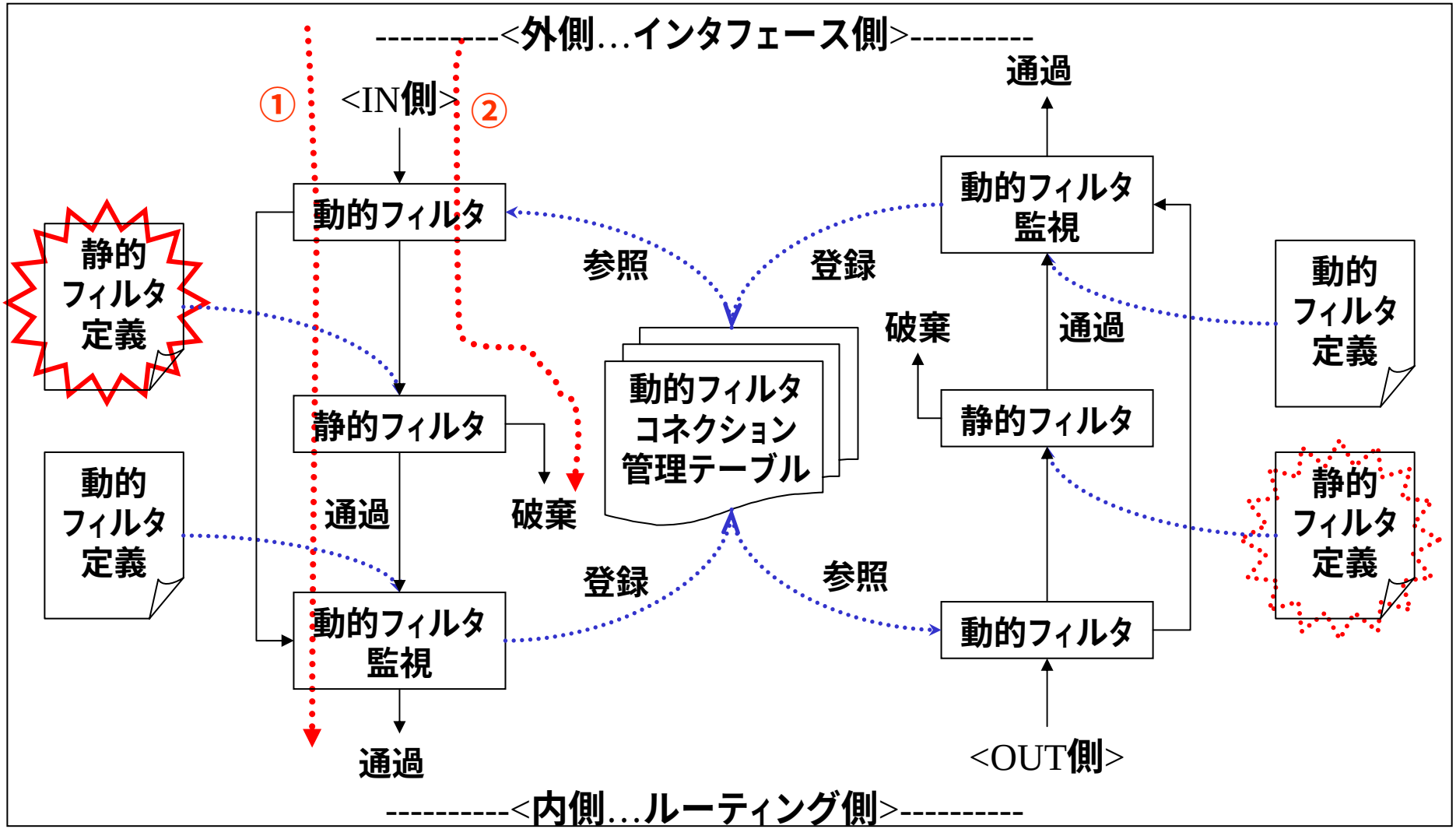
セキュリティ・レベル	1	2	3	4	5	6	7
予期しない発呼を防ぐフィルタ	○	○	○	○	○	○	○
NetBIOS等を塞ぐフィルタ (ポート番号:135,137,138,139,445)		○	○	○	○	○	○
プライベートアドレスのままの通信を禁止するフィルタ			○		○		○
静的セキュリティ・フィルタ (従来のセキュリティフィルタ)				◎	◎		
動的セキュリティ・フィルタ (強固なセキュリティ・フィルタ)						☆	☆

ファイアウォールの構造

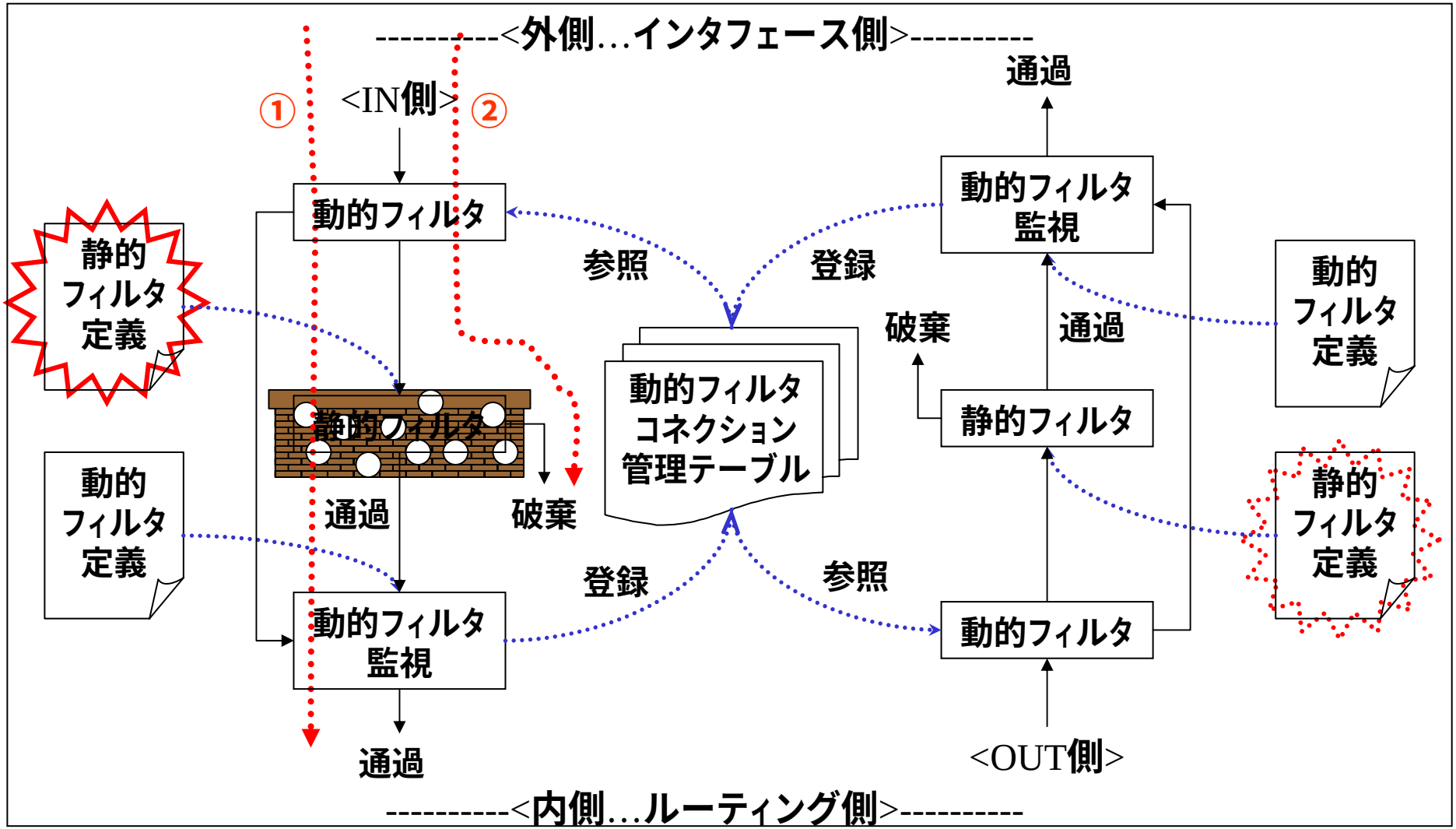


http://www.rtpro.yamaha.co.jp/RT/docs/firewall/index.html

一部の通信路を塞ぐ



静的セキュリティ・フィルタ



```
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]

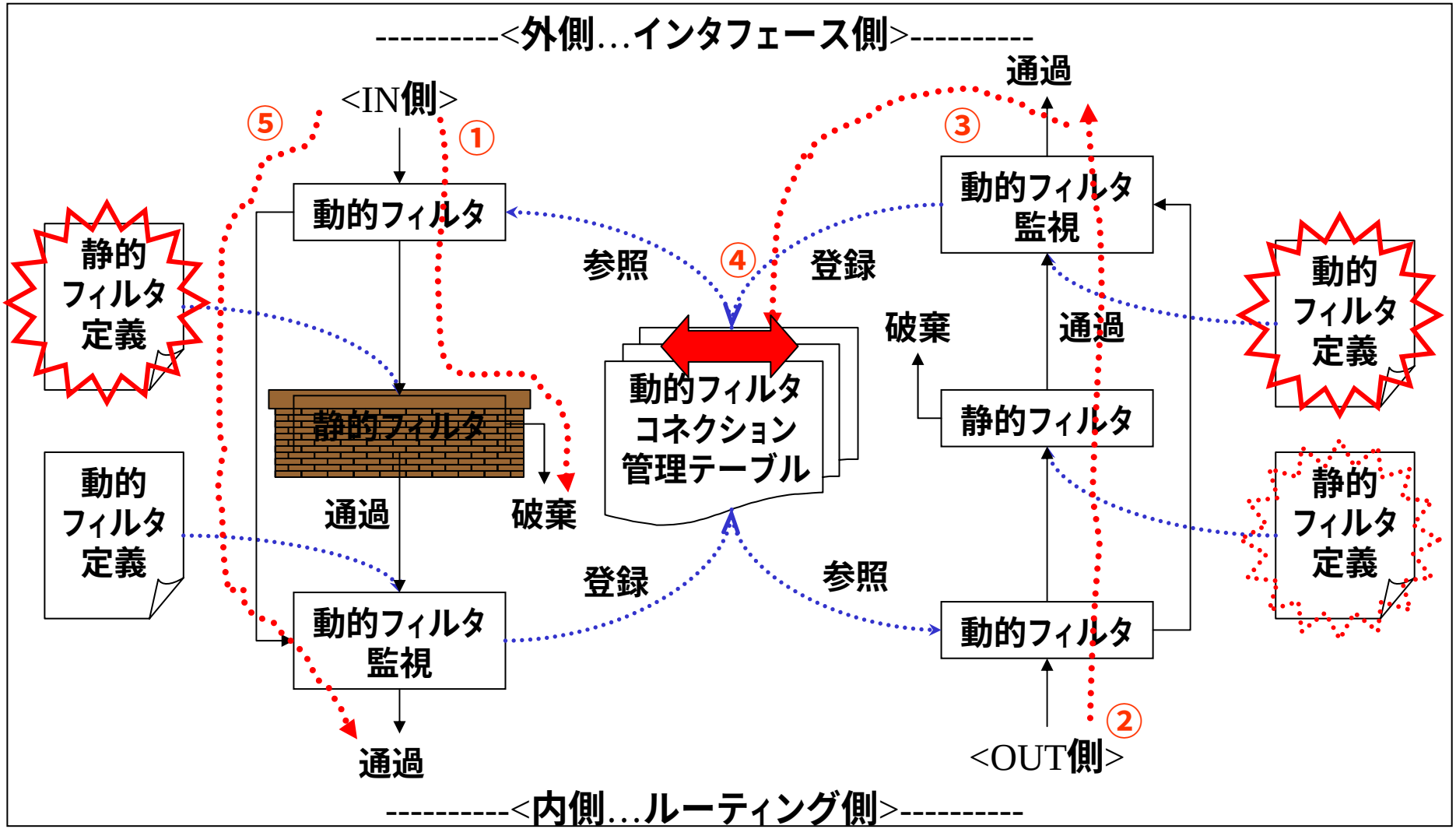
- ネットボランチ RTA54i
- プロバイダ接続設定の
  セキュリティ・レベル5

```
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
```


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

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)

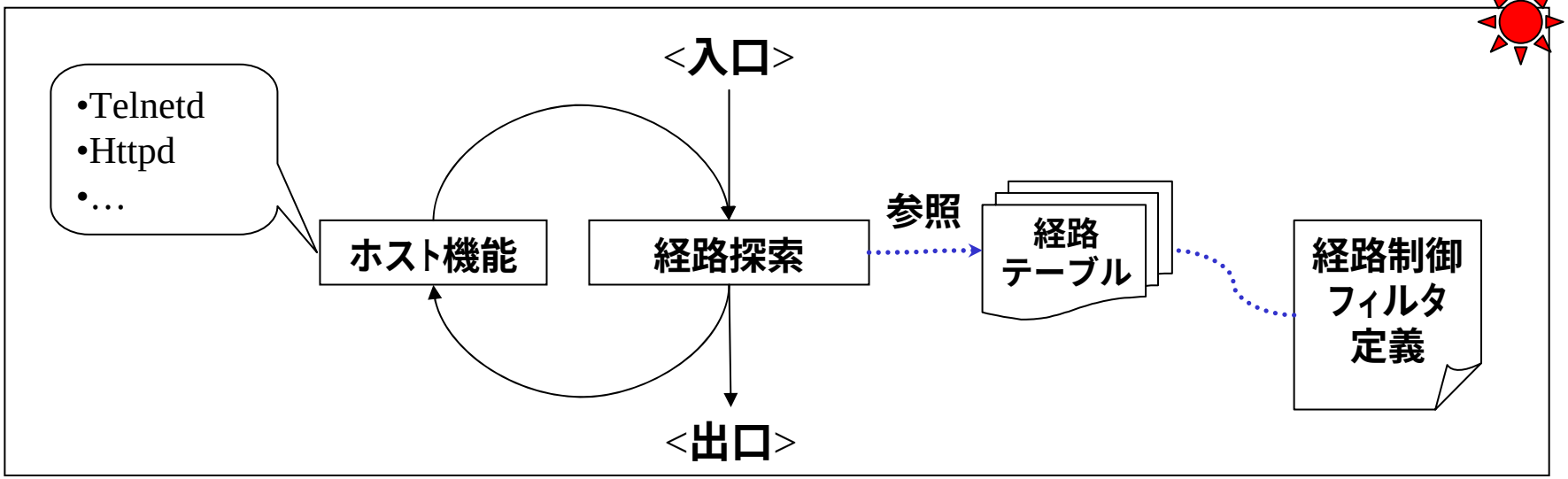
RTA50i

RTA52i *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]

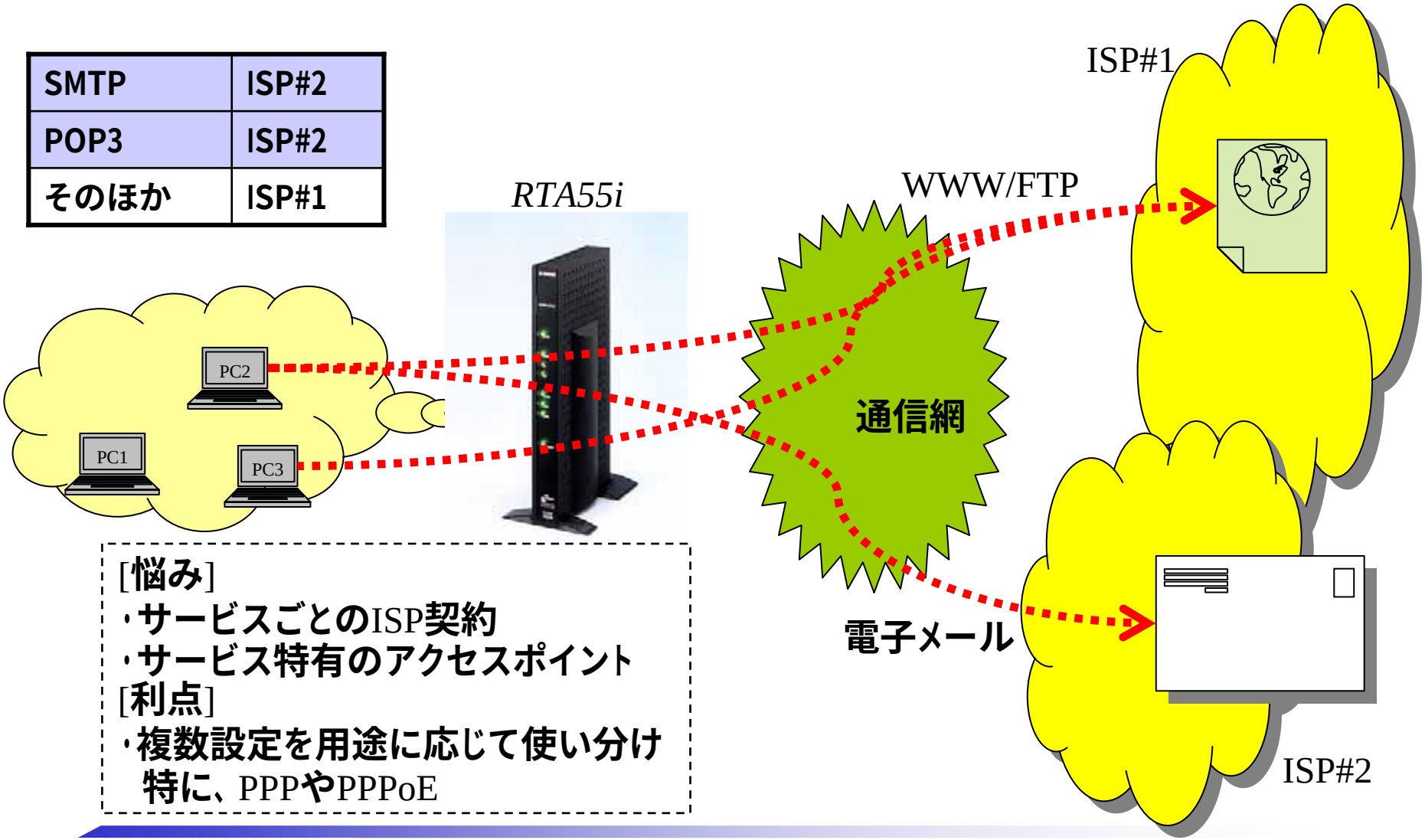
☆宛先の経路

- **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

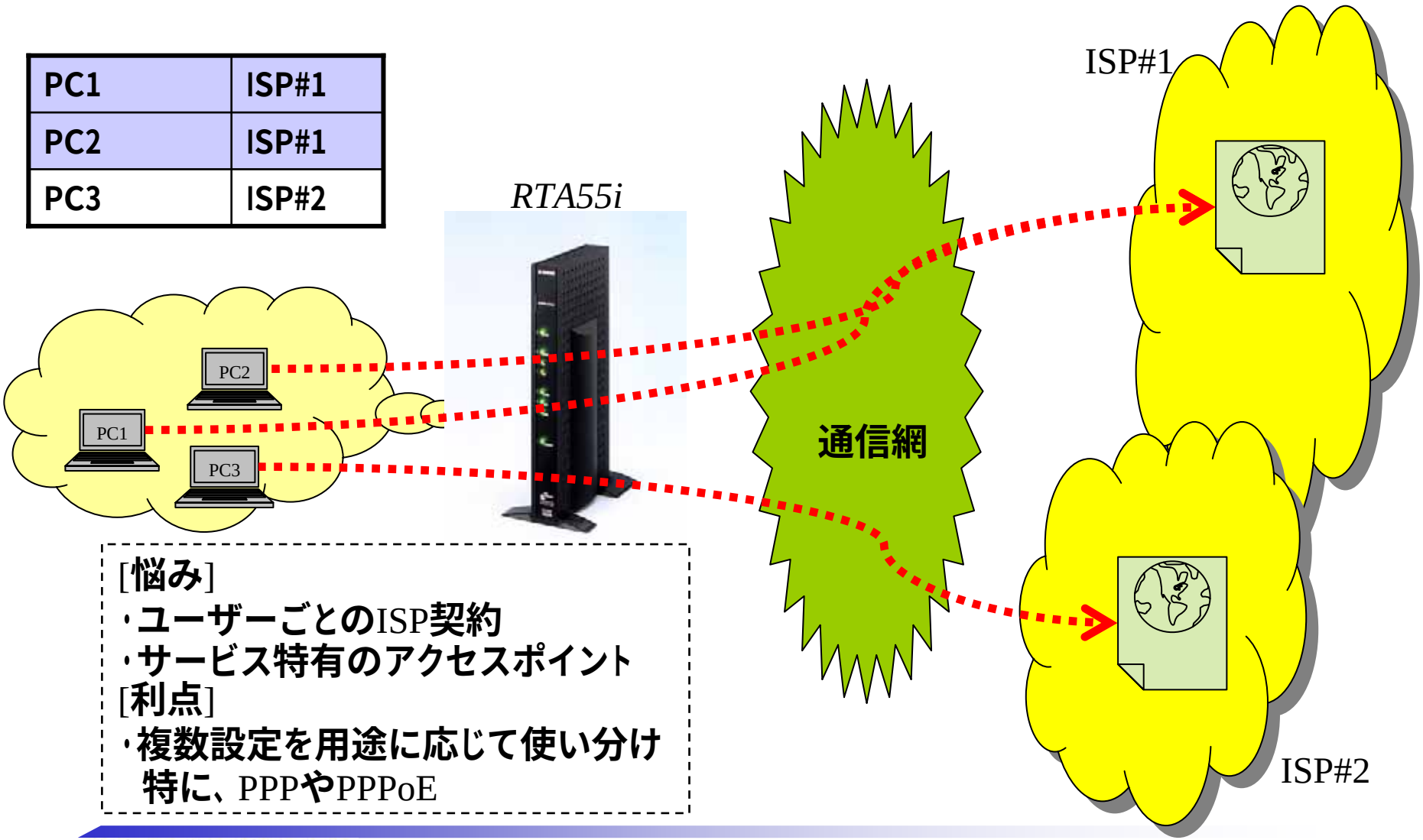
SMTP	ISP#2
POP3	ISP#2
そのほか	ISP#1



[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

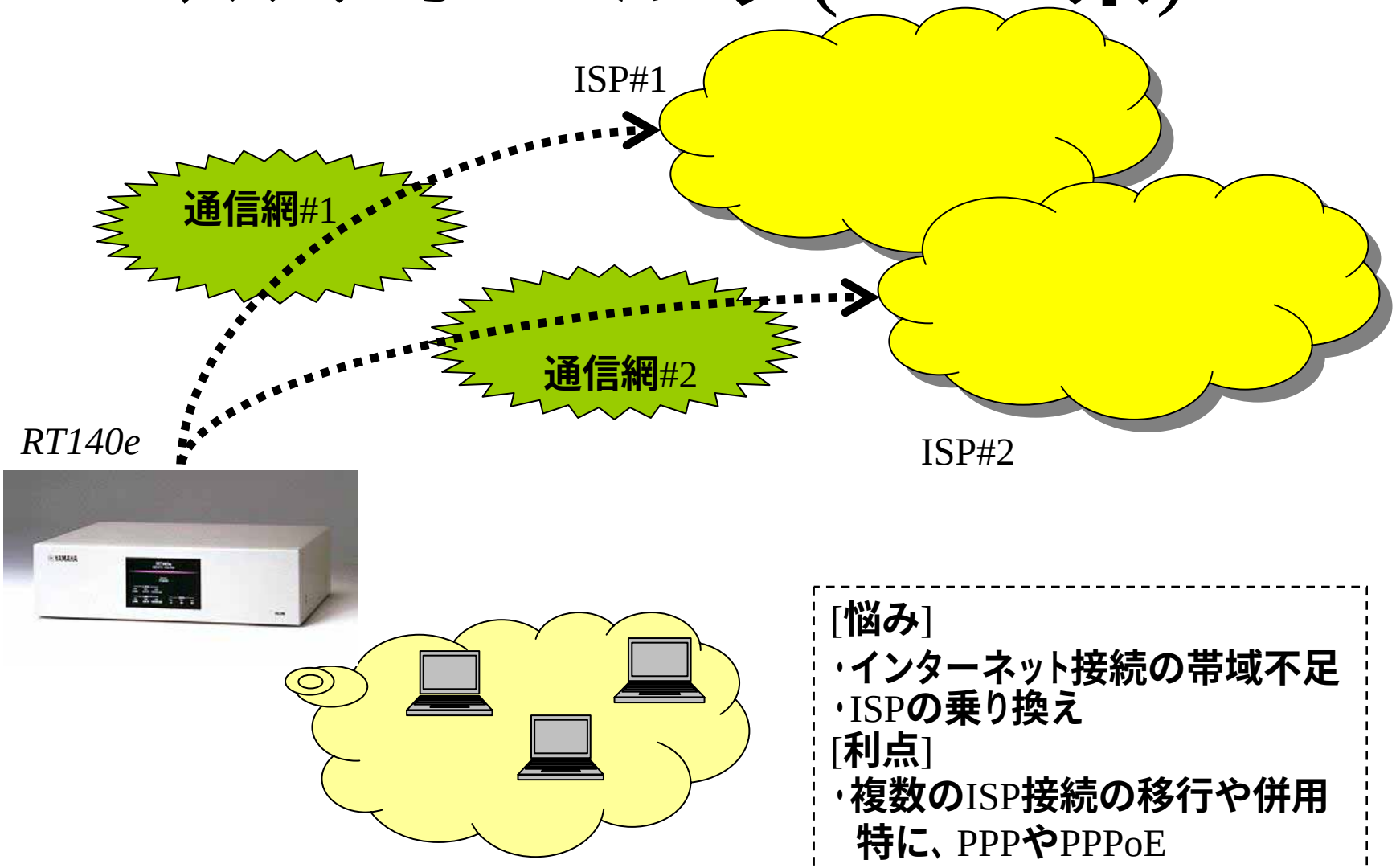


[悩み]
・ユーザーごとのISP契約
・サービス特有のアクセスポイント
[利点]
・複数設定を用途に応じて使い分け
　特に、PPPやPPPoE

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