ヤマハ ルーター
ファイアウォール機能
～説明資料～

ヤマハ株式会社
AV･IT事業本部
マーケティング室

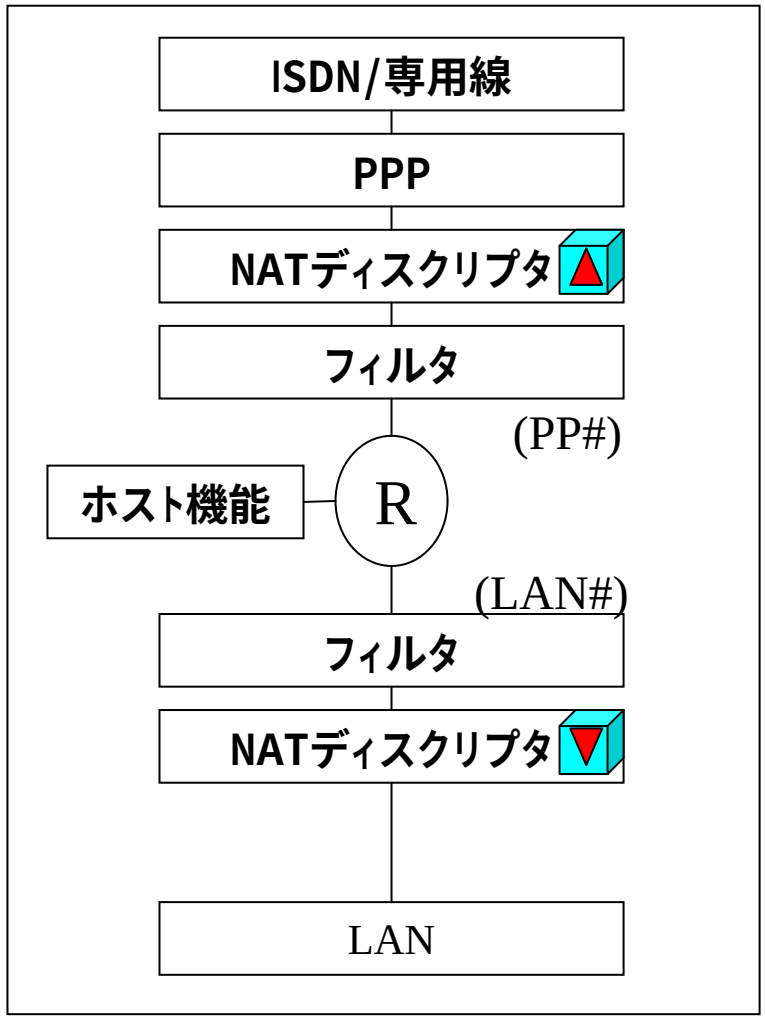
2002年9月

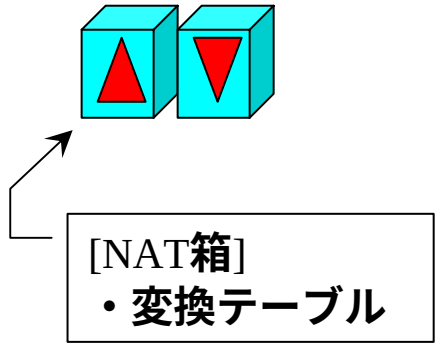
構造#1(PPP)

RT140i

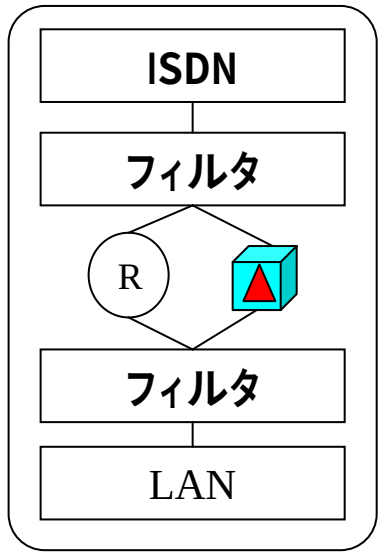
RT105i

RTA52i





比較構成例

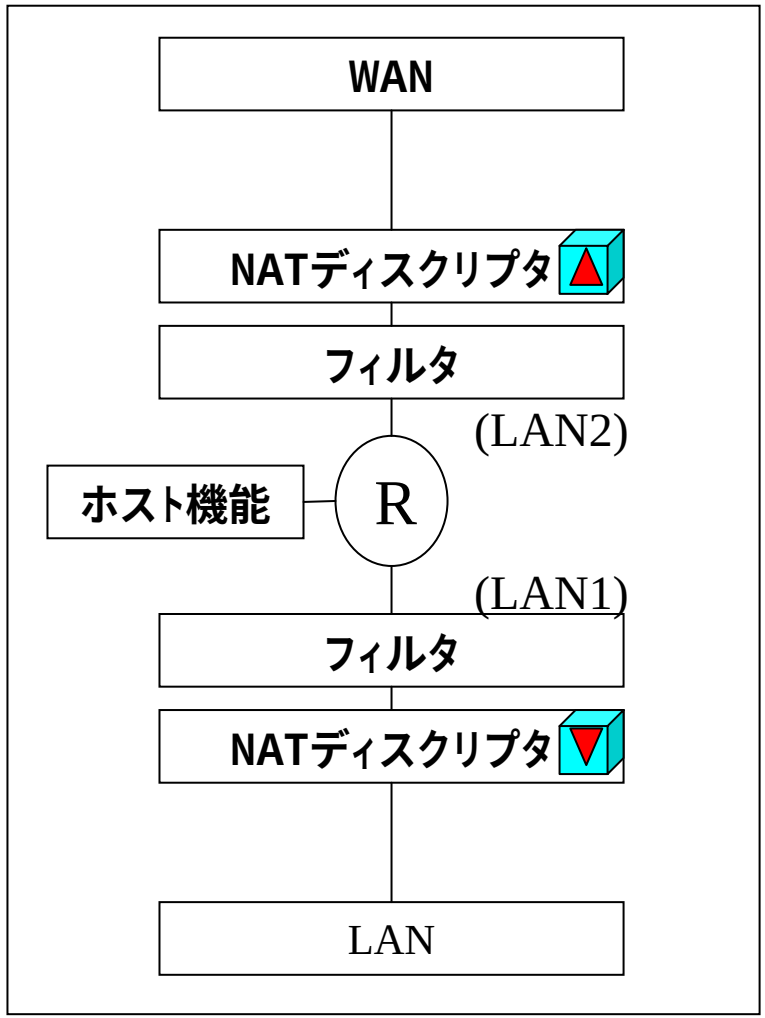


構造#2(ローカルルータ)

RT300i

RT140e

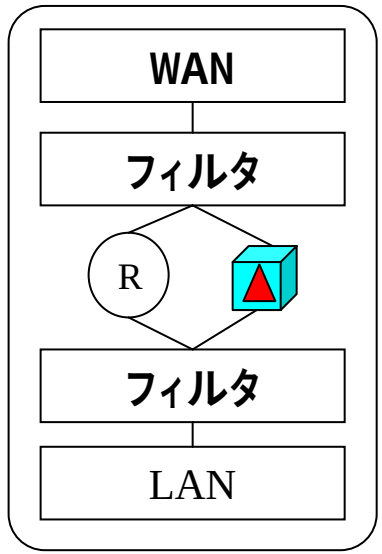
RT105e



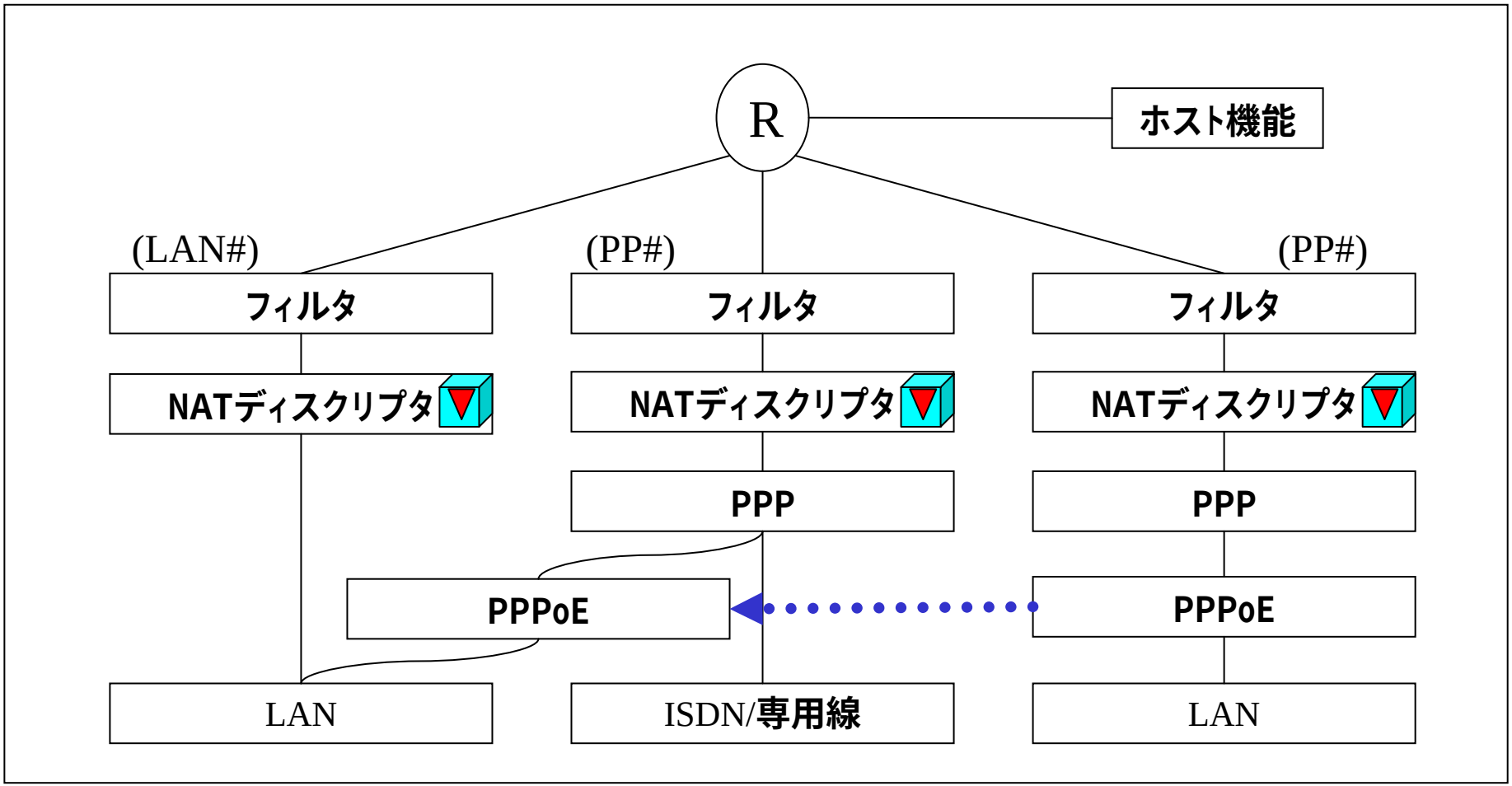
RTW65b

RTA55i

比較構成例



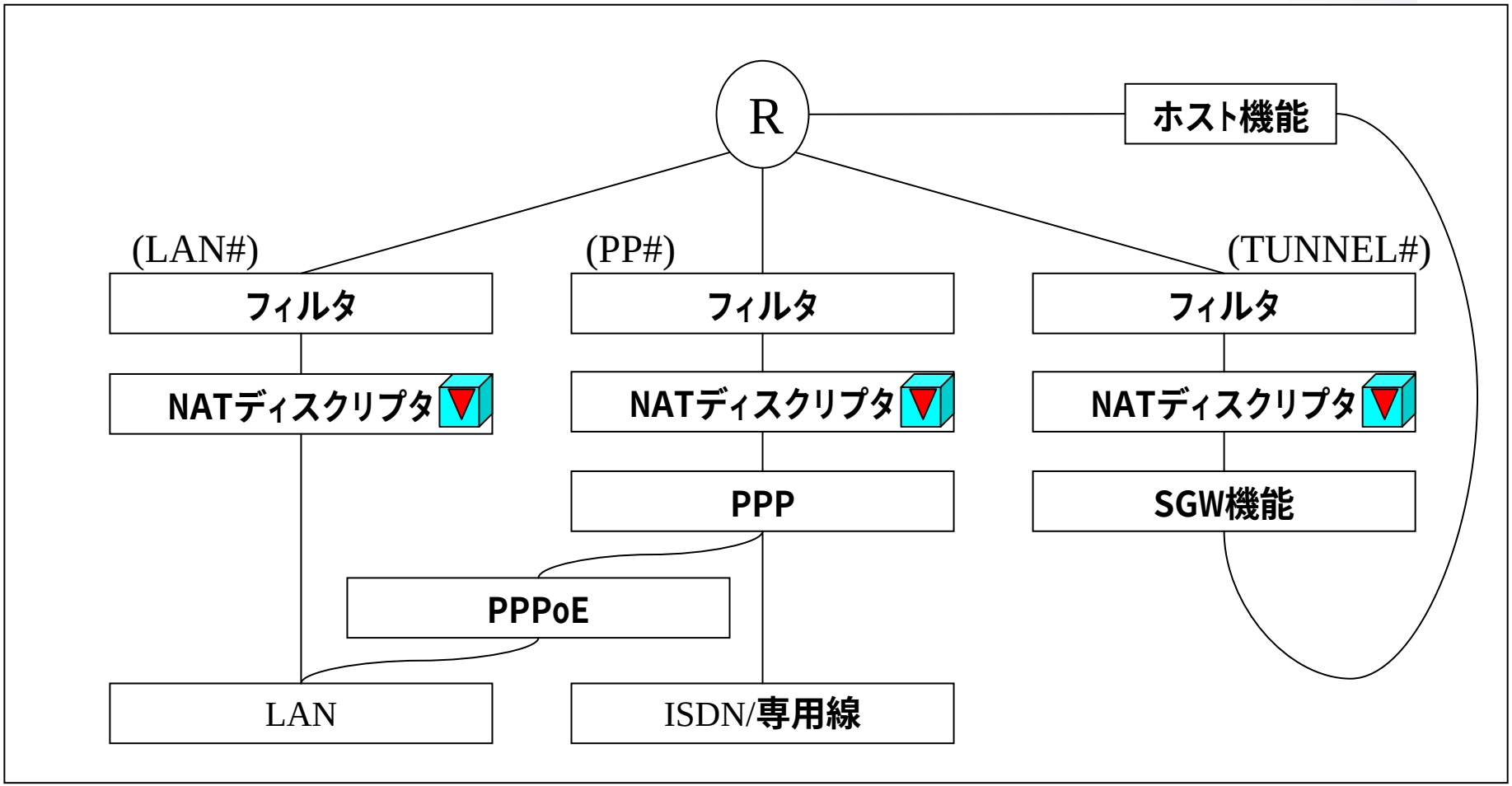
構造#3(PPPoE)



RT300i

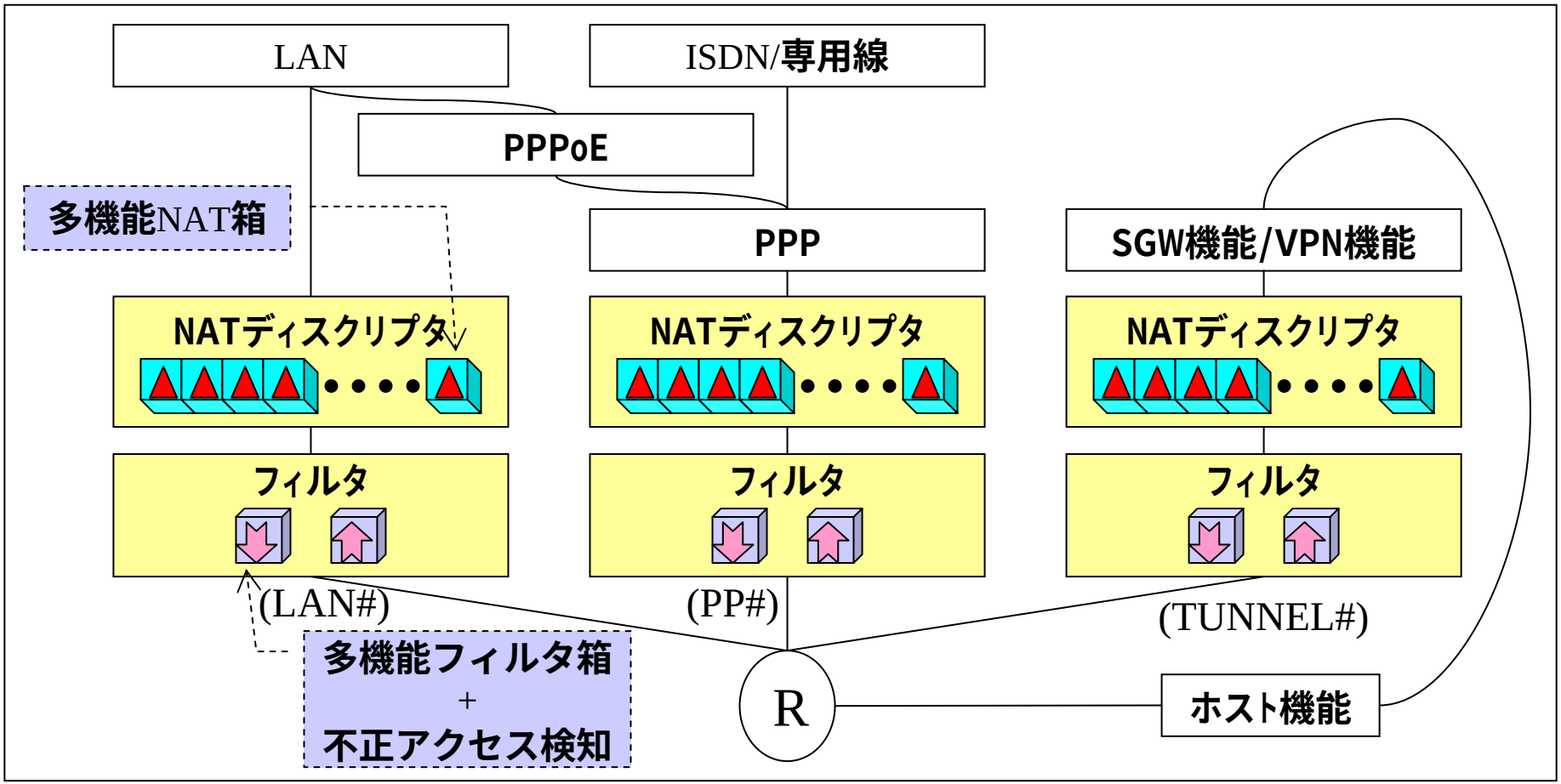
構造#4(VPN)

RT105シリーズ



ファイアウォールのフレキシビリティ

ファイアウォール機能を自由自在に利用できるしくみ



アドレス変換

- NATディスクリプタの特徴
- 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。

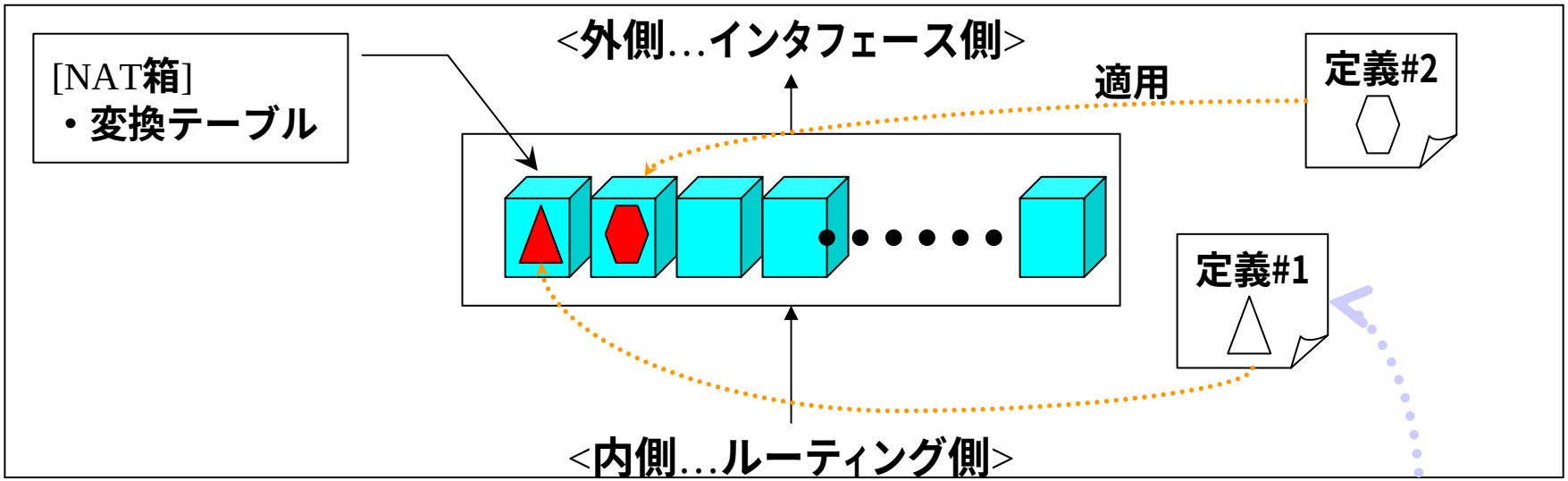
アドレス変換機能(NAT)への取り組み

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

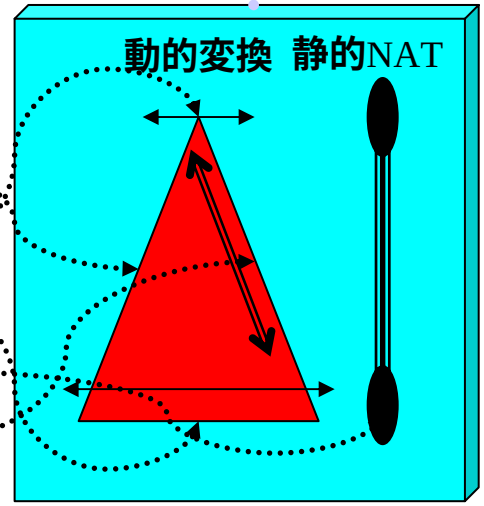
- LANインタフェースに対応
  - LANのprimary⇔secondaryの変換が可能
- TUNNELインタフェースに対応
  - VPNで変換が可能
- 3つの変換タイプ
  - NAT形式
  - IPマスカレード形式
  - NAT + IPマスカレード形式
- 機能統合、制限の緩和
  - 複数の変換規則を並列的に適用可能
    (ひとつのインタフェースに16組)

NATディスクリプタの構造



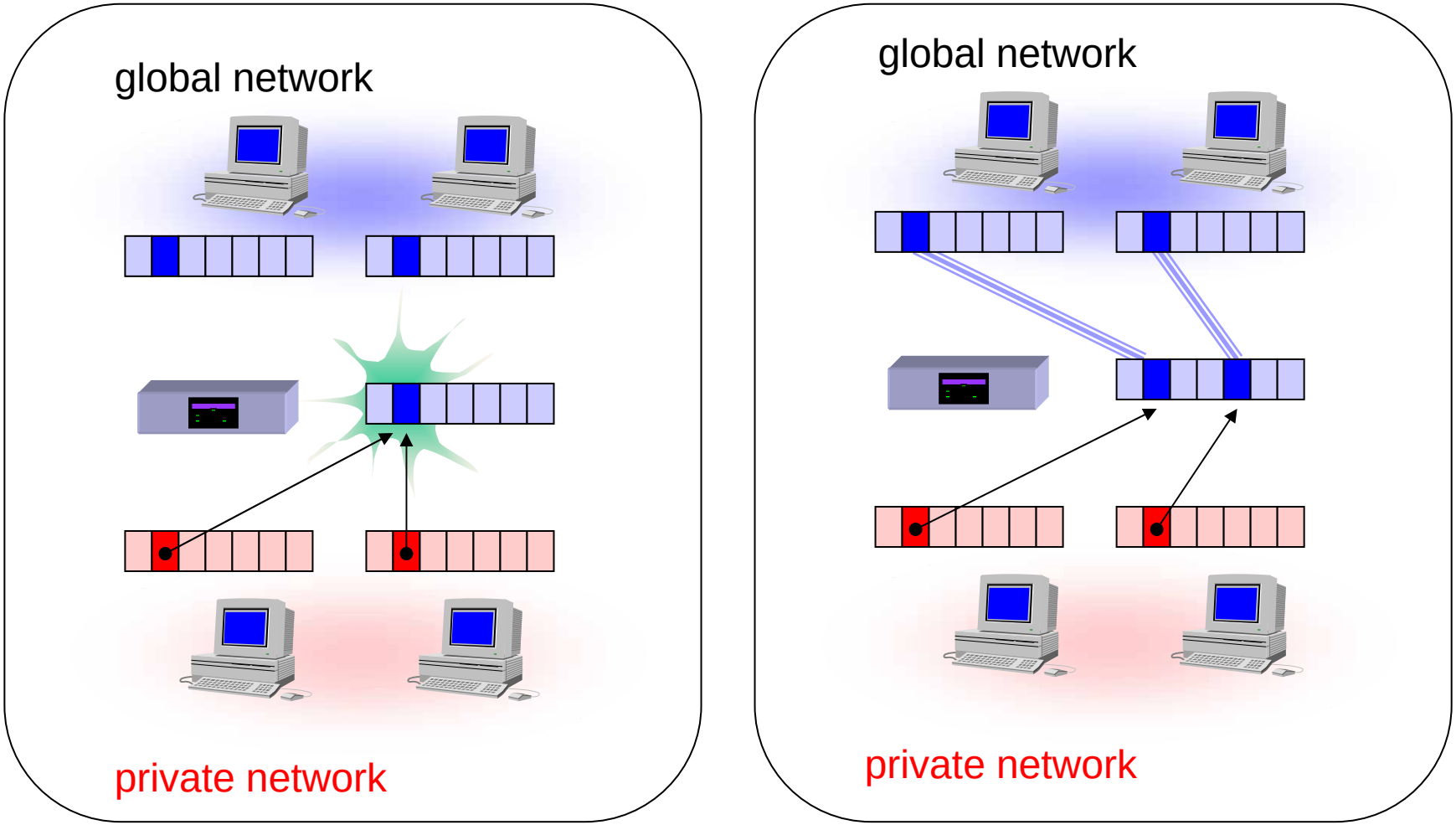
[定義→アドレス変換の設計図]

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



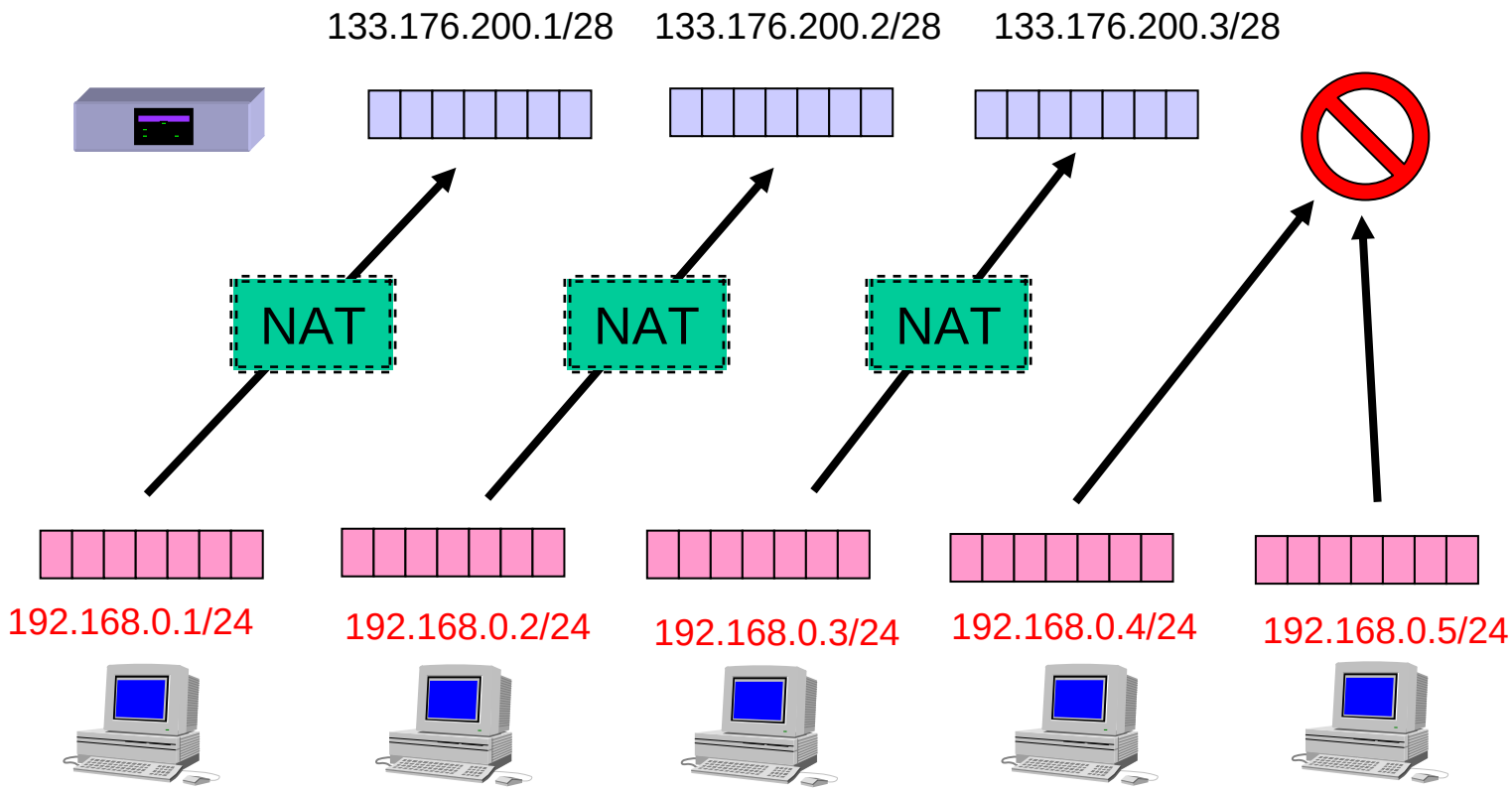
IPマスカレード(IP Masquerade)

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



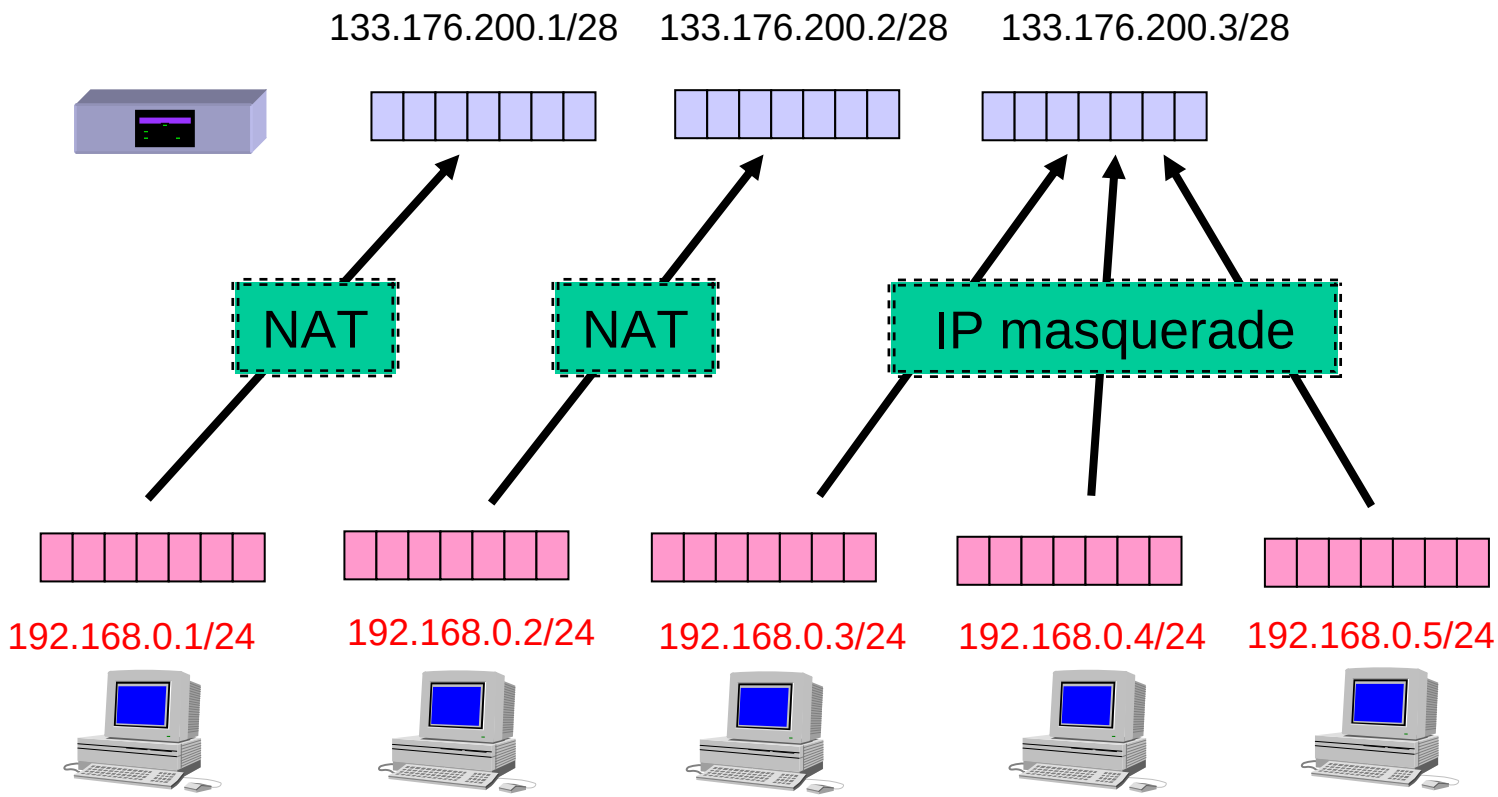
NAT (Network Address Translation)

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

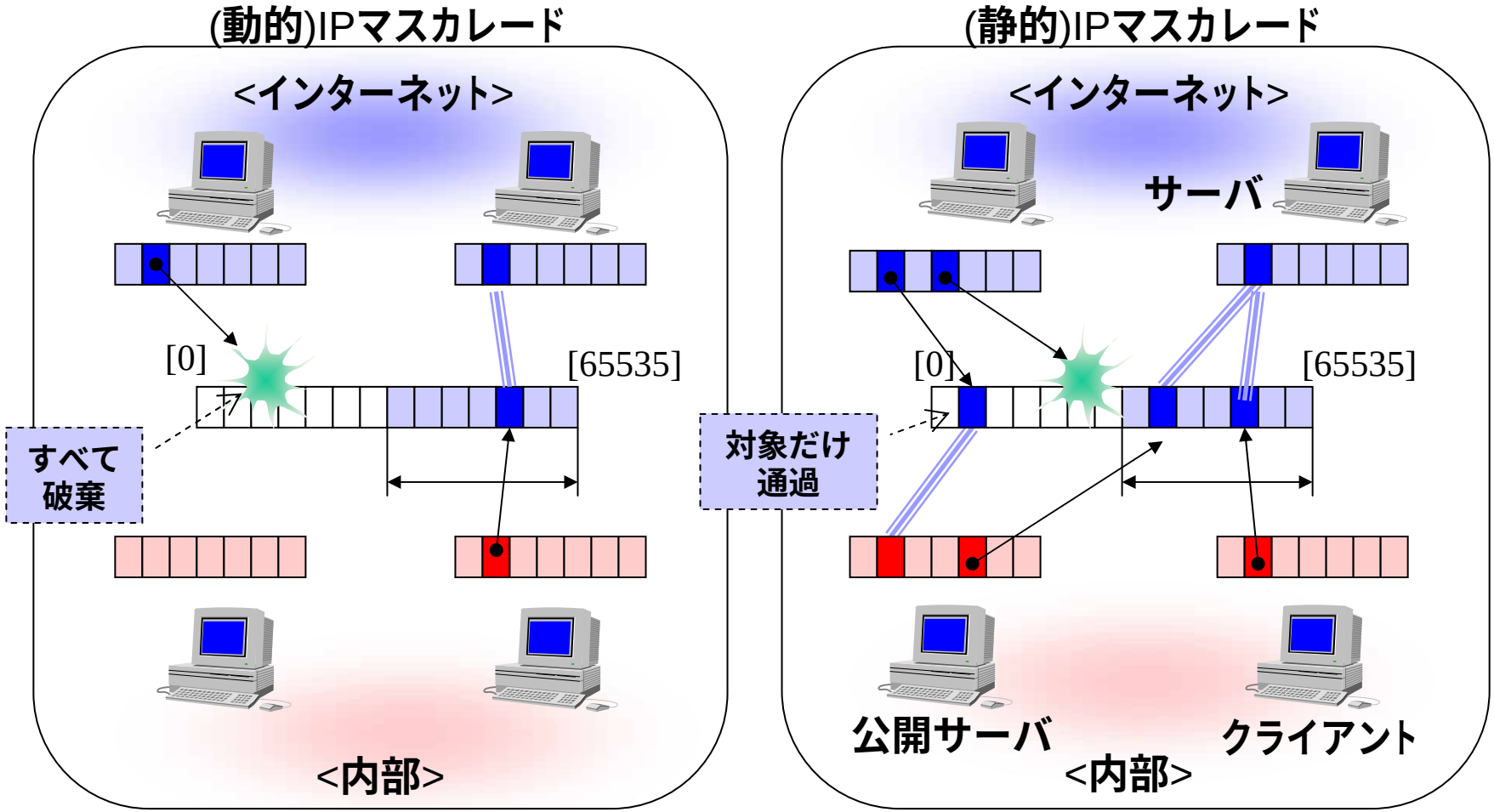


NAT + IPマスカレード形式

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



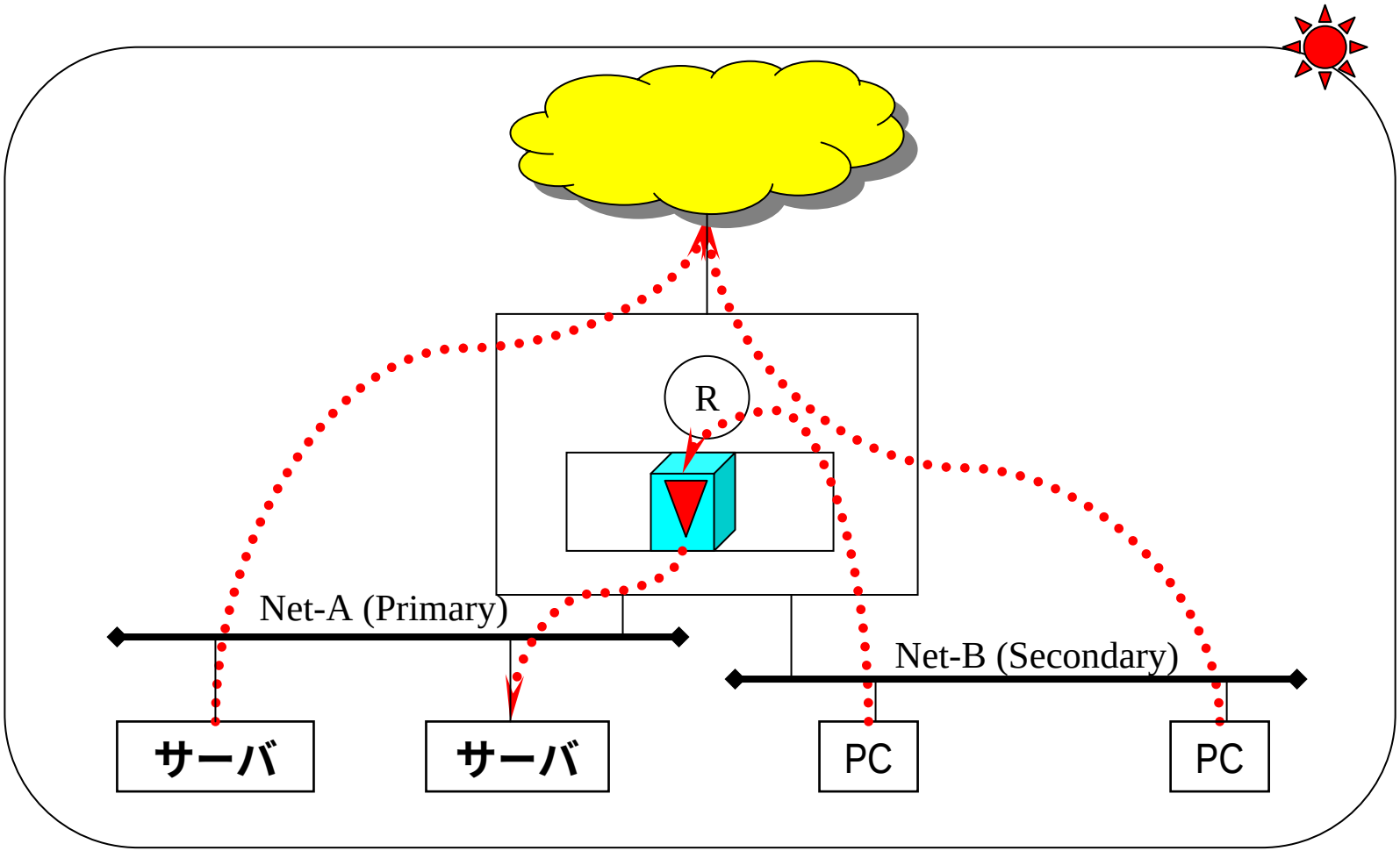
静的IPマスカレード



(静的IPマスカレード)

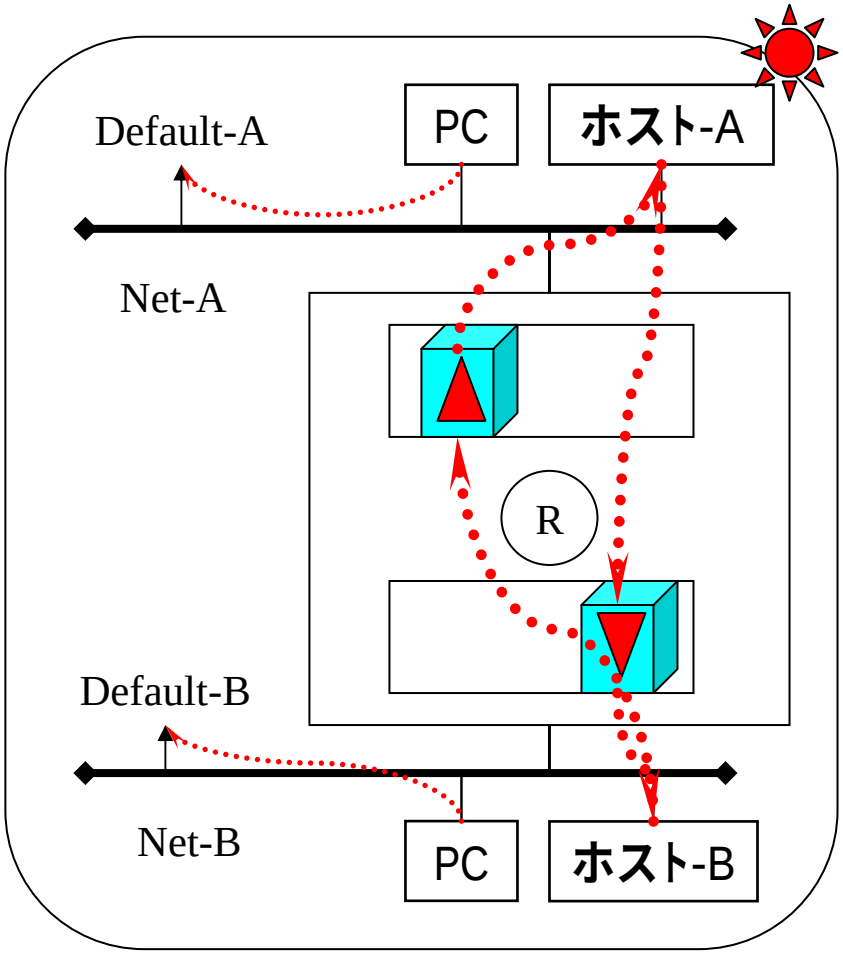
特定の通信だけ固定して、公開する。

NATディスクリプタの応用例#1

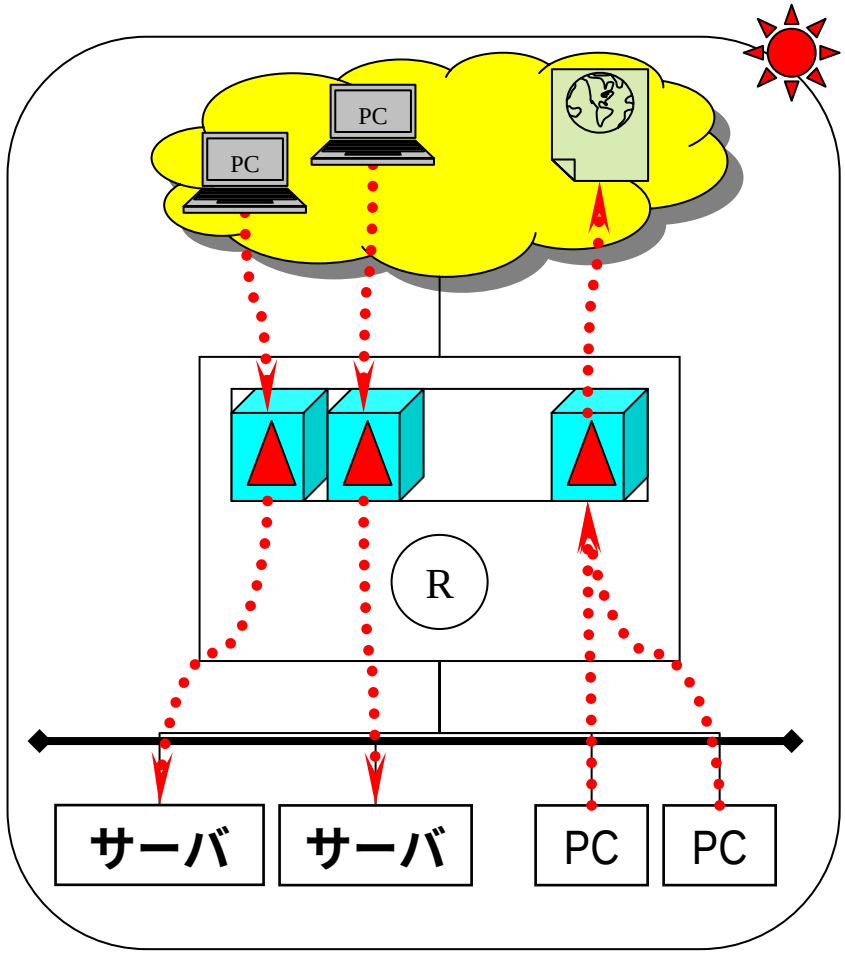


primary⇔secondary**間のIPマスカレード (逆マスカレード)**

NATディスクリプタの応用例#2



2つの隔離されたネット間での通信(hot line)



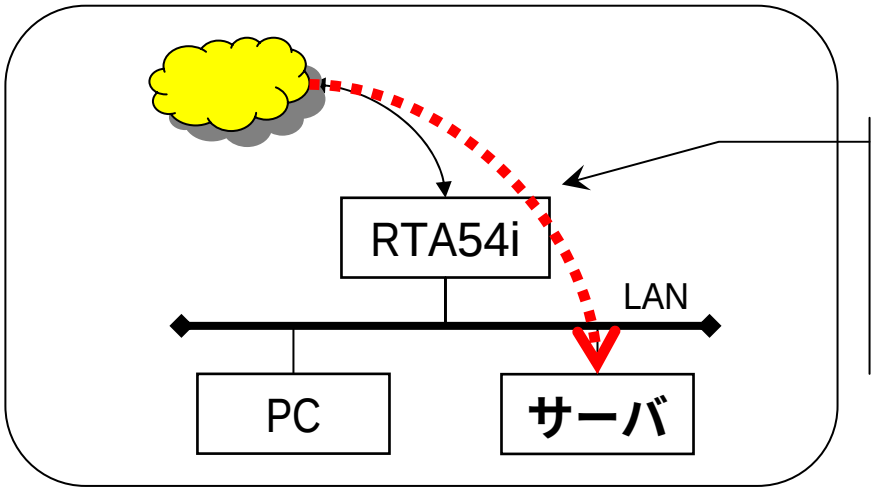
公開サーバにIPマスカレード適用

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

IPマスカレードの機能選択

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

DMZホスト機能



ISDN/ADSL/CATVプロバイダ接続(LAN)

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

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

DMZホスト機能
～コマンド仕様～

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

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

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

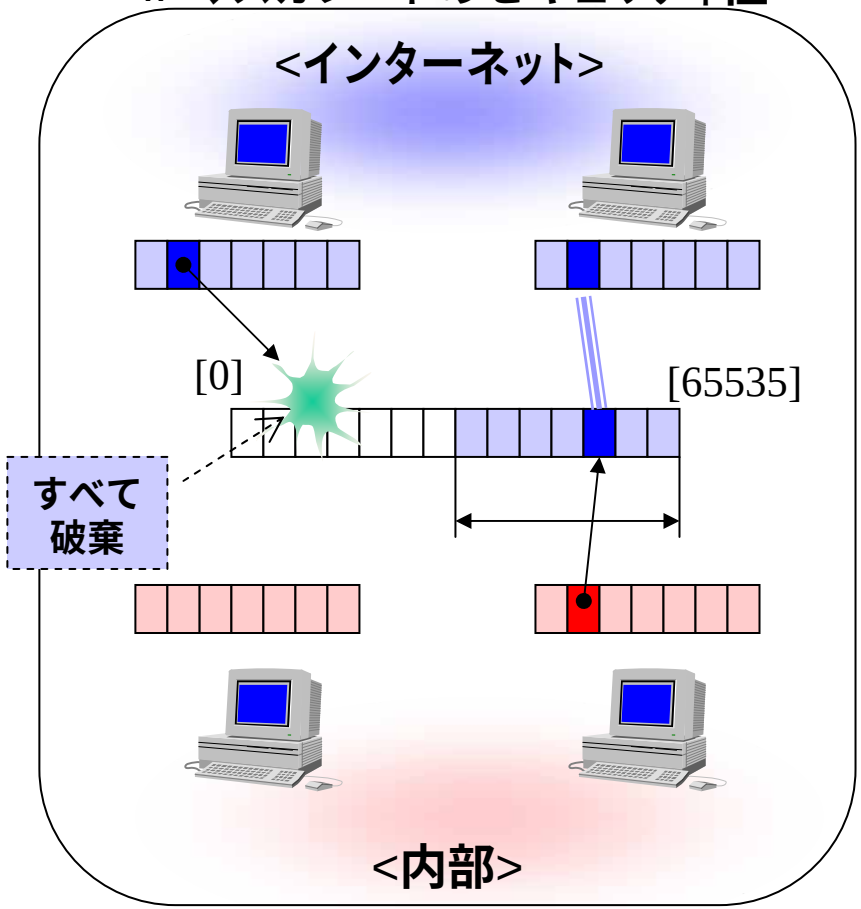
[パラメータ] - DESC_ID ..... NATディスクリプタ番号
- ACTION ..... 動作
  - through ... 変換せずに通す
  - reject .... 破棄して、TCPの場合はRSTを返す
  - discard ... 破棄して、何も返さない
  - forward ... 指定されたホストに転送する
- IP_ADDRESS ... 転送先のIPアドレス

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

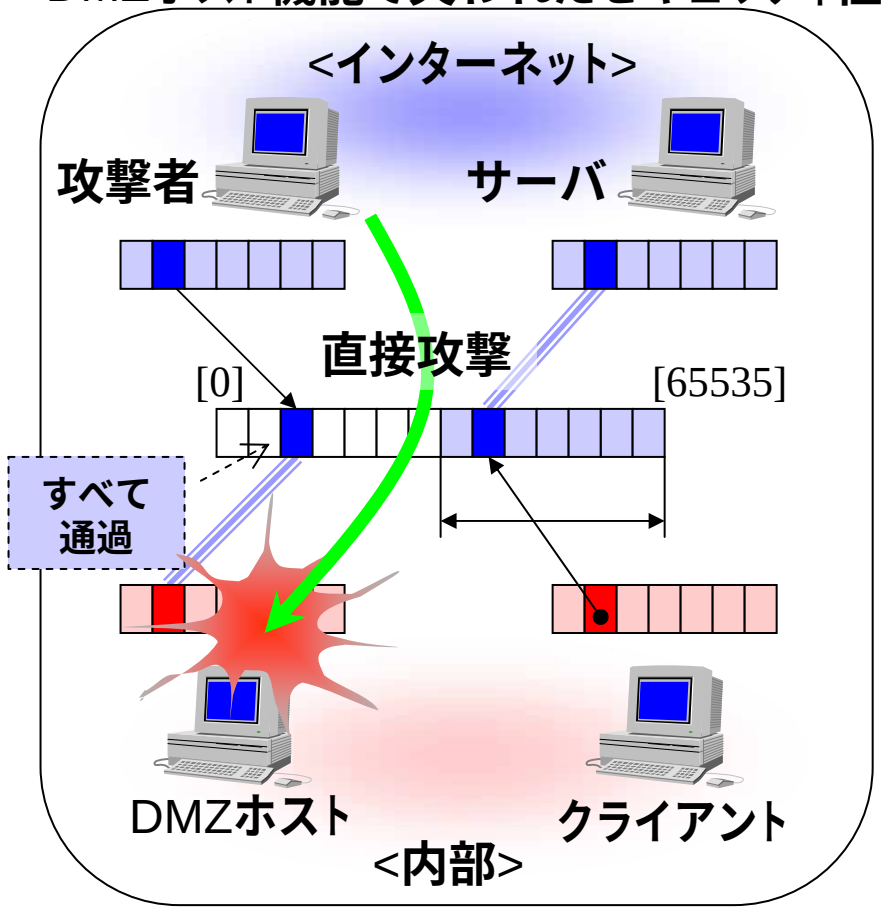
[デフォルト値] reject

DMZホスト機能の脆弱性

IPマスカレードのセキュリティ性



DMZホスト機能で失われたセキュリティ性

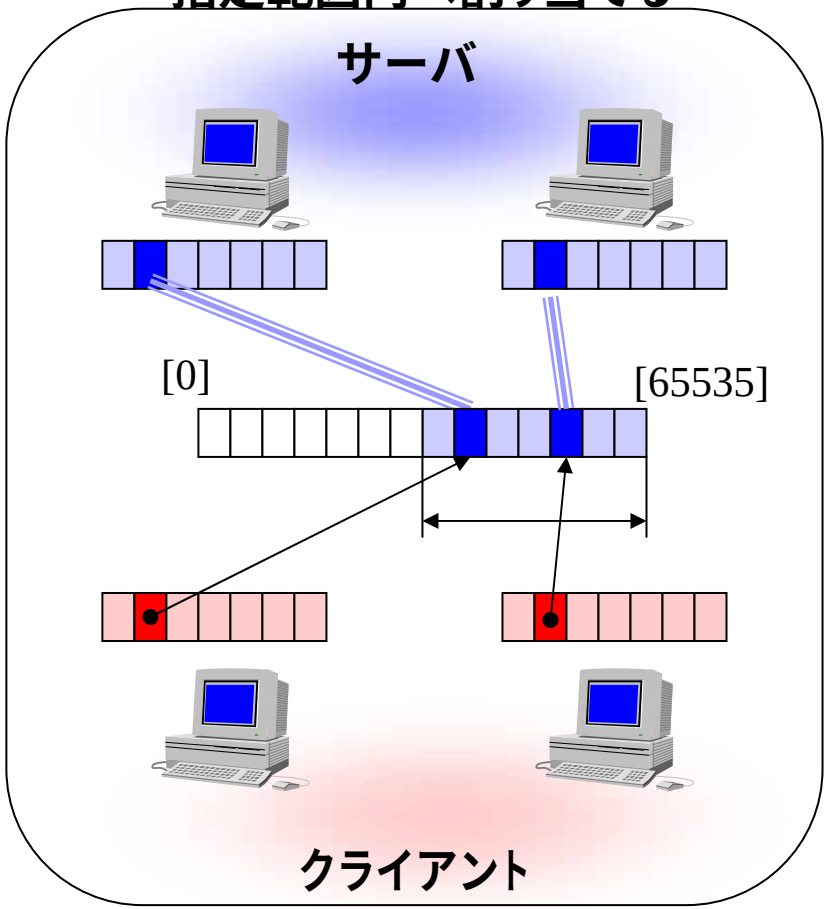


(利便性とセキュリティ性のトレードオフ)

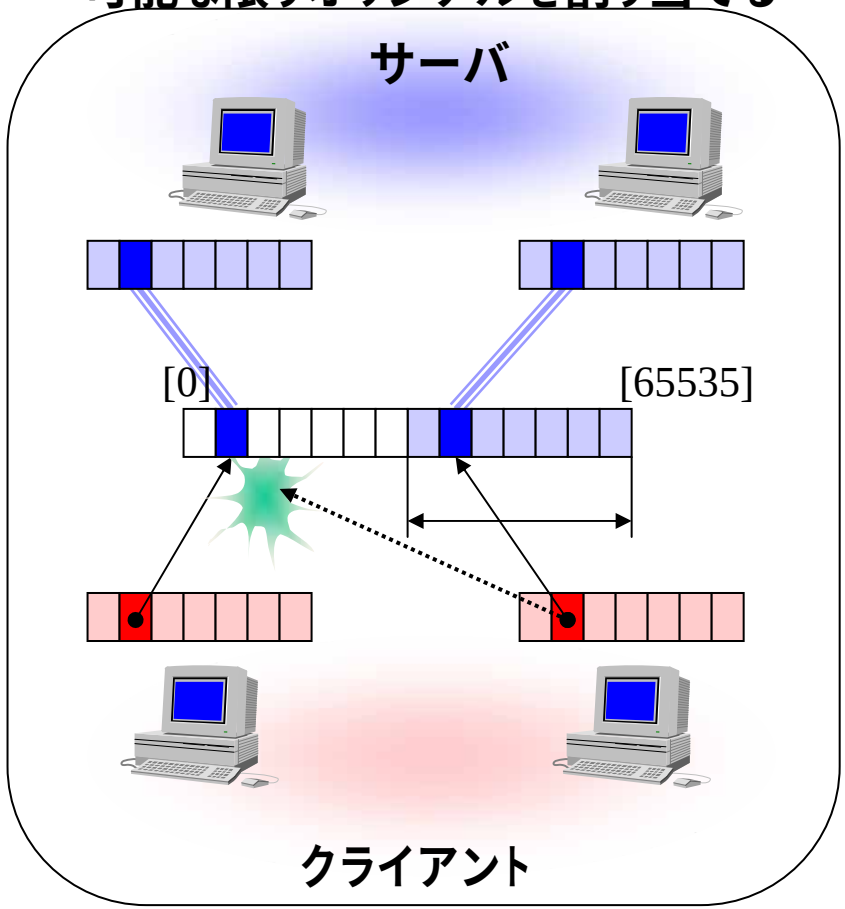
アドレス変換の苦手なアプリケーションが便利になるが、セキュリティ性は低下する。

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]

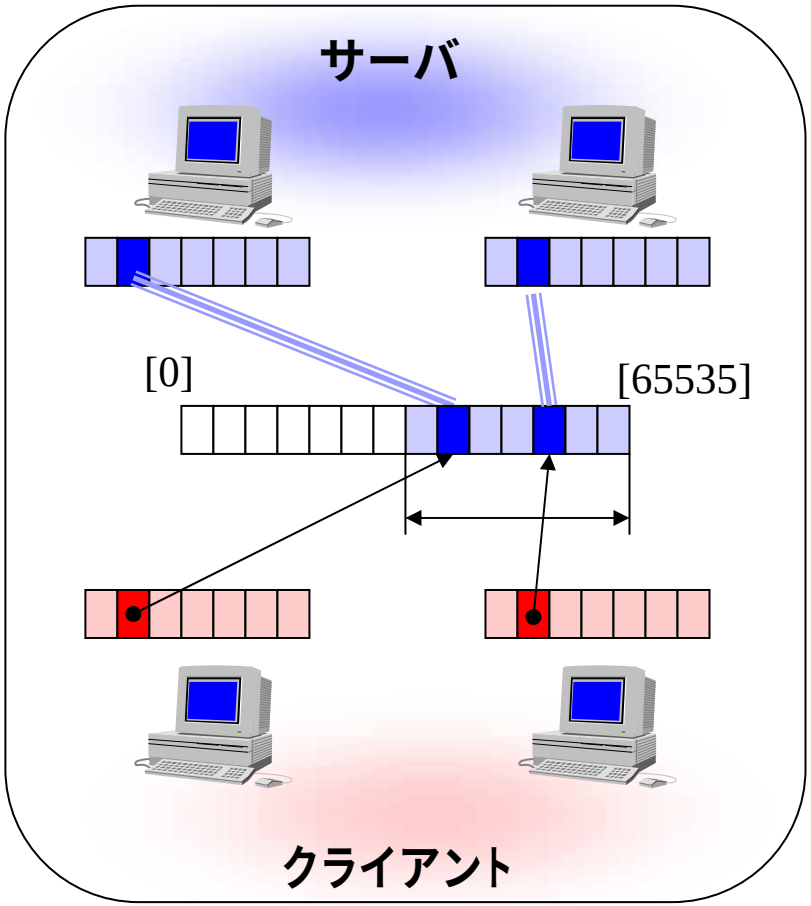
DESC ... ディスクリプタ番号
PROTOCOL ... プロトコル、'tcp'もしくは'udp'
PORT ... ポート番号の範囲

[説明]

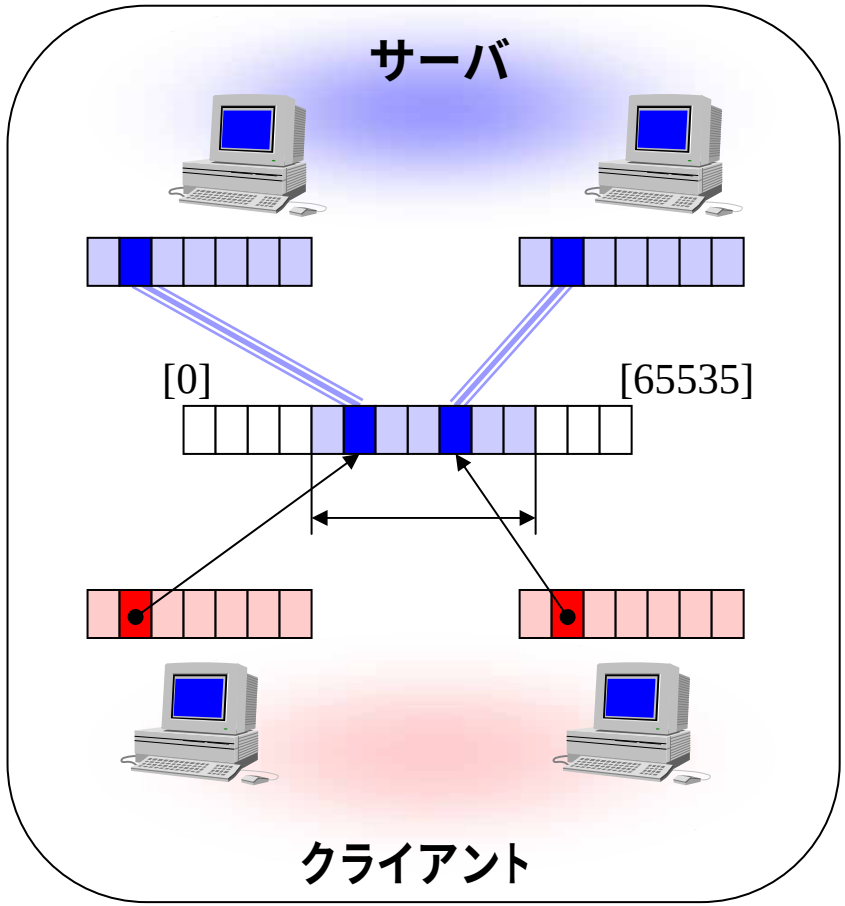
IPマスカレードで変換しないポート番号の範囲を設定する。
if-possibleが指定されている時には、処理しようとするポート番号が他の通信で使われていない場合には値を変換せずそのまま利用する。

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

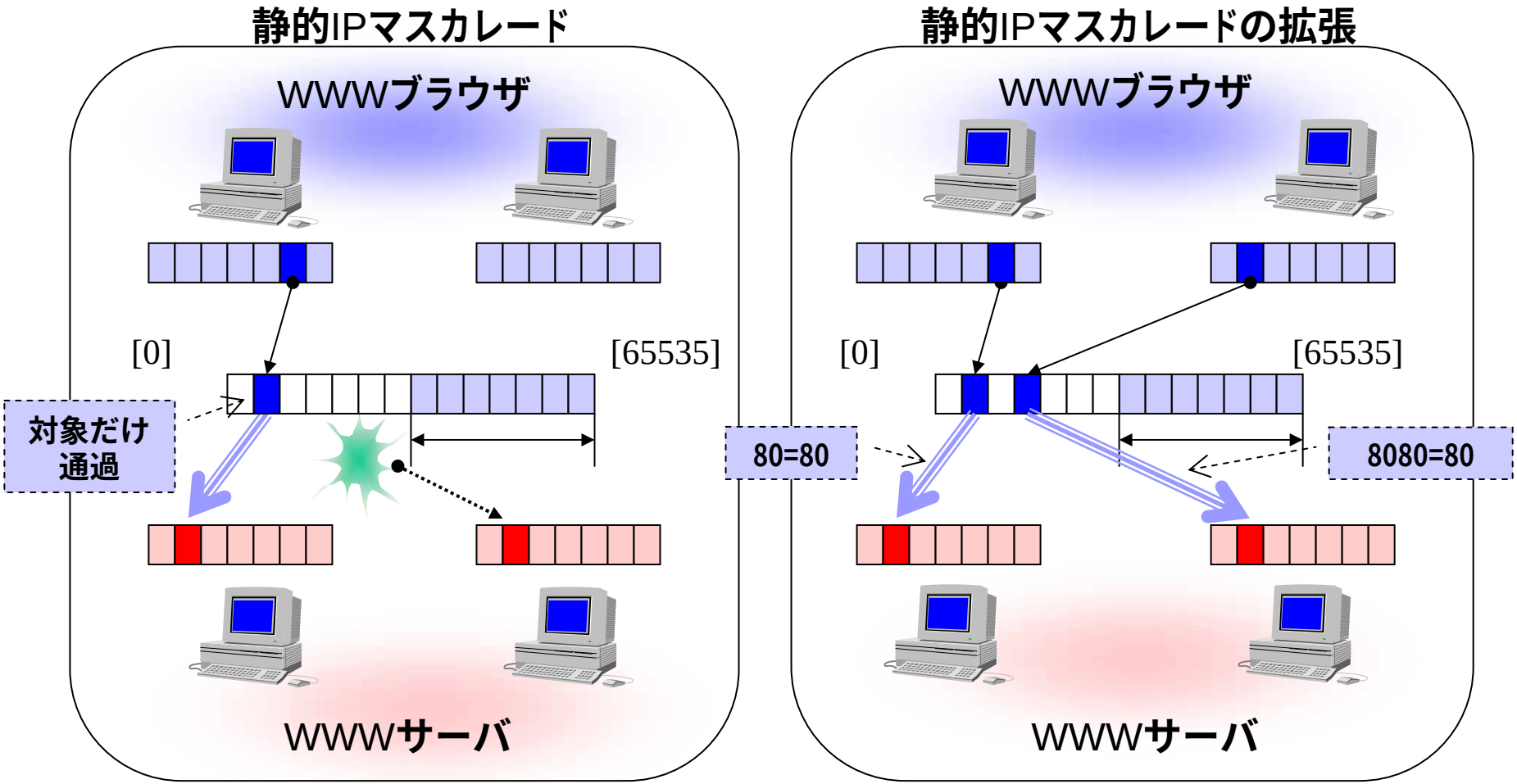
[説明]

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]

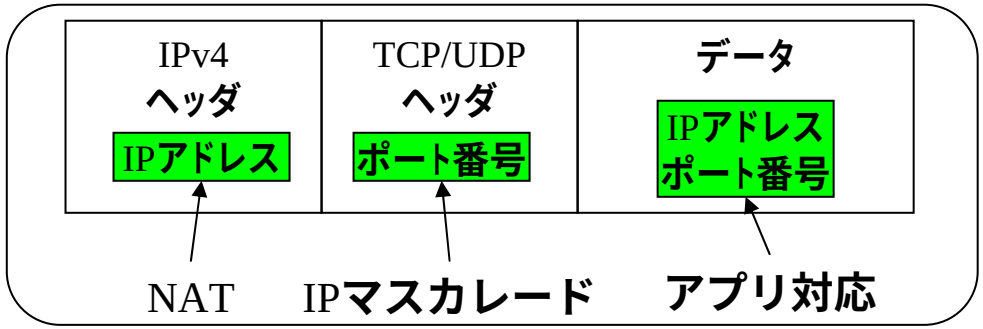
IPマスカレードによる通信でポート番号変換をしないように固定する。
また、外側ポートと内側ポートの関連付けも可能。

IPマスカレードのアプリケーション対応

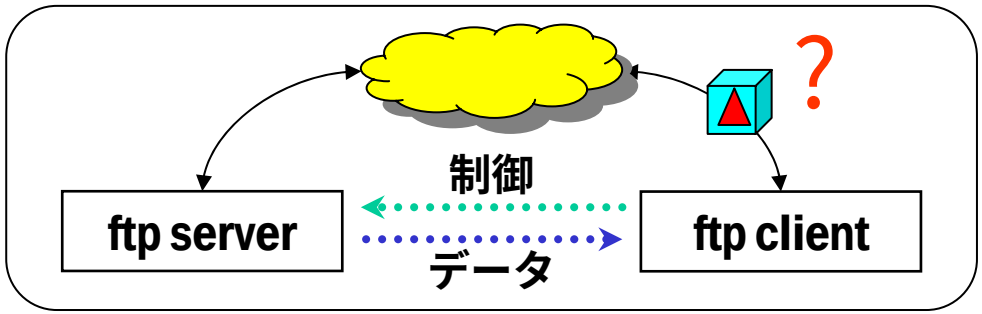
- FTP対応
  - FTP/アプリケーション対応の必要性
  - FTPセッション保持機能
  - FTP監視ポート指定機能
- NetMeeting 3.0対応
  - 可能な限りポート番号変換しない処理
- VPNパススルー機能
  - 同時1セッション、静的IPマスカレードの制限緩和
- PPTPのマルチセッション対応

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

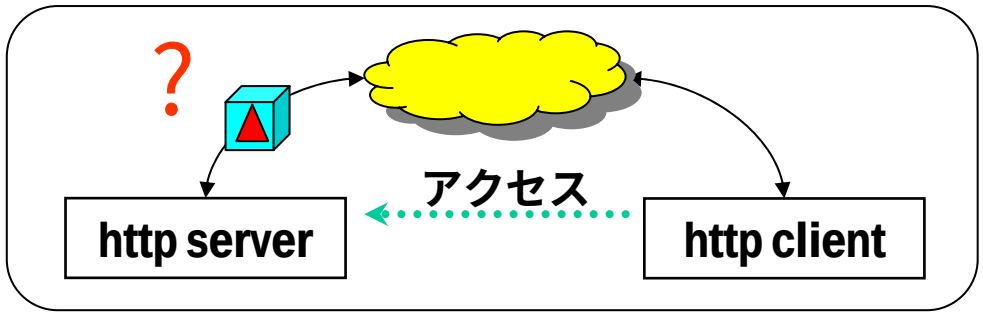


②複数のコネクションが利用される(異なる方向)



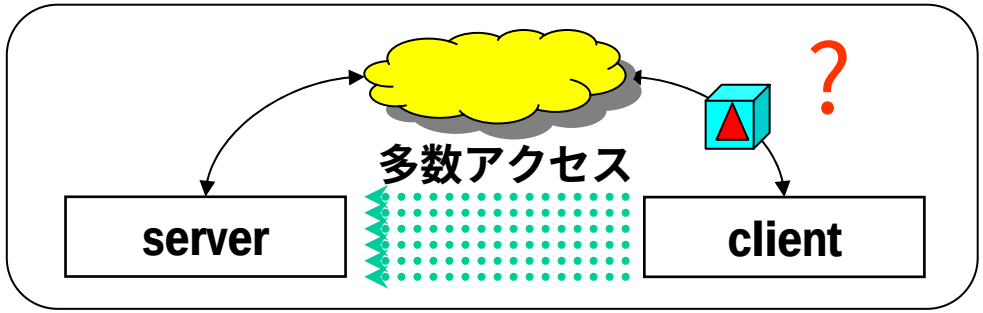
ftpのアクティブ転送(PORTコマンド)

③サーバ公開(サービス公開)

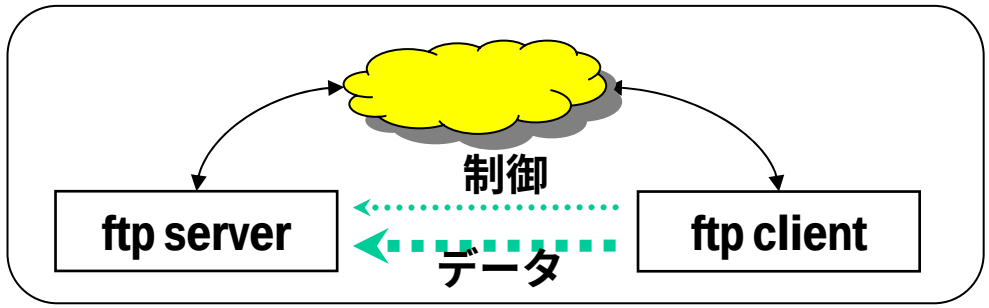


アプリケーション対応の概要#2

④同時多数接続を行うアプリケーション

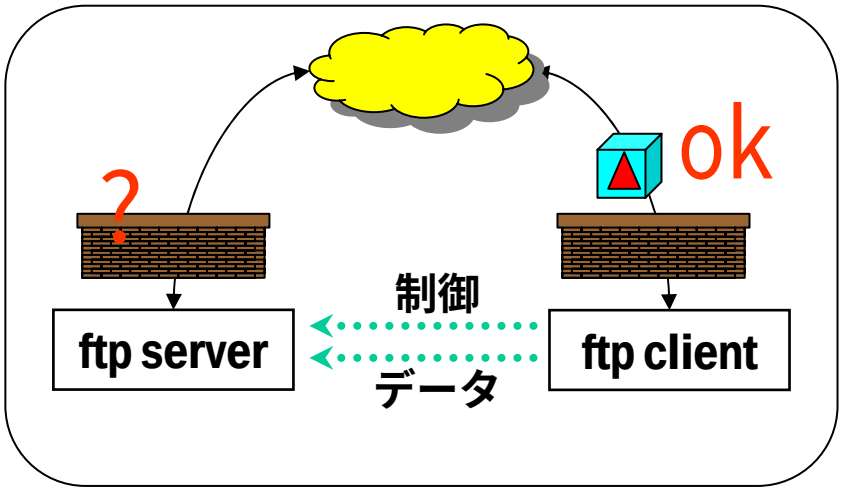


⑤複数のコネクションが利用される
(利用状態が不均一)

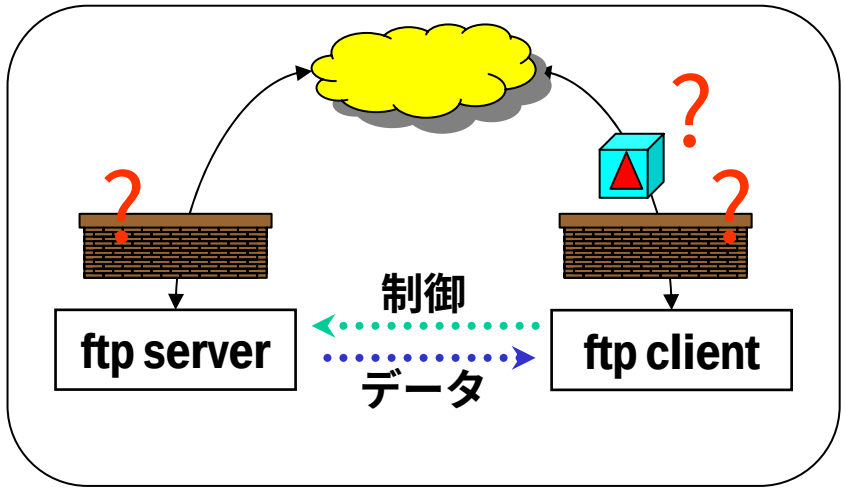


ftpのパッシブ転送(PASVコマンド)

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]

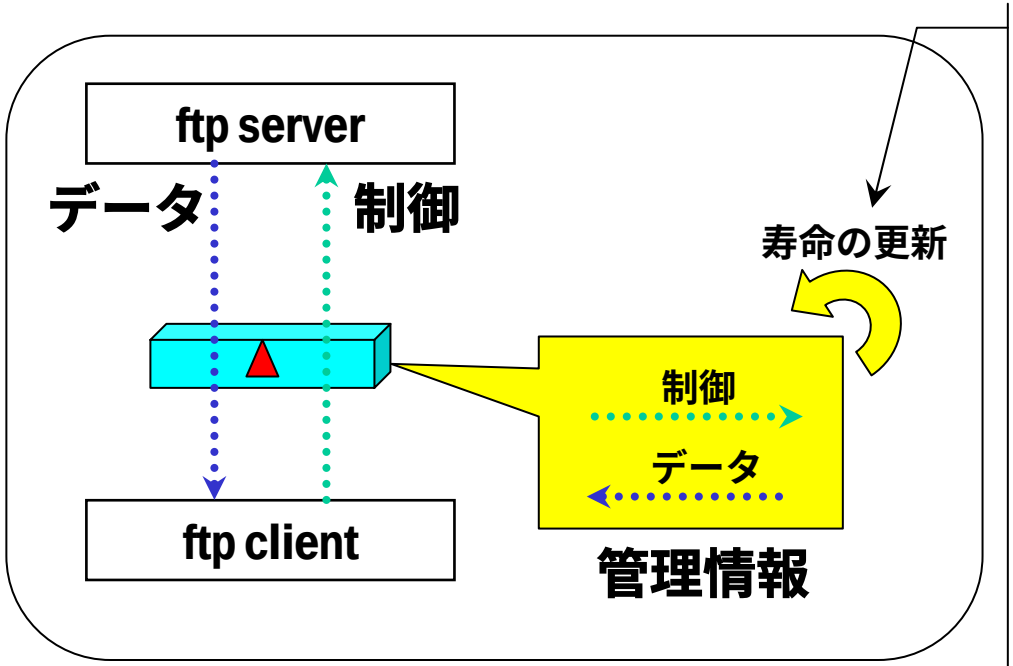
・アプリ/機能を実現するために複数のコネクションが必要

・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

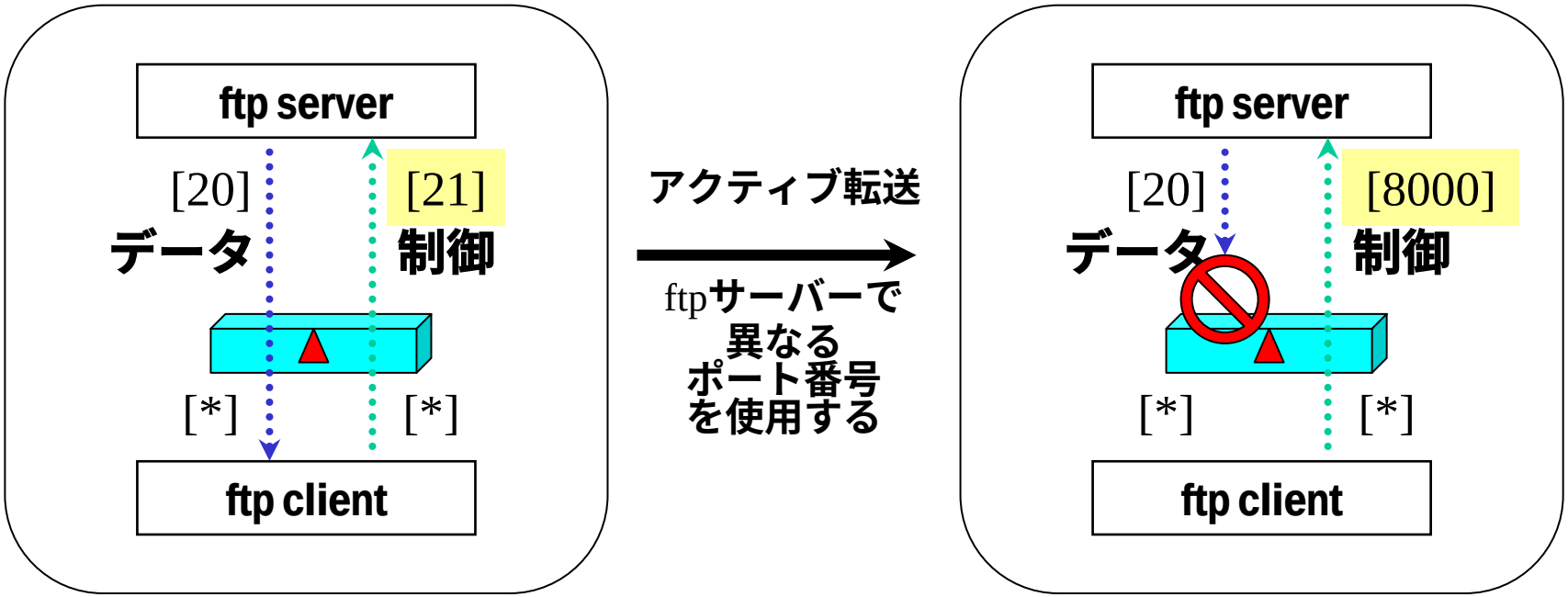
[説明]

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

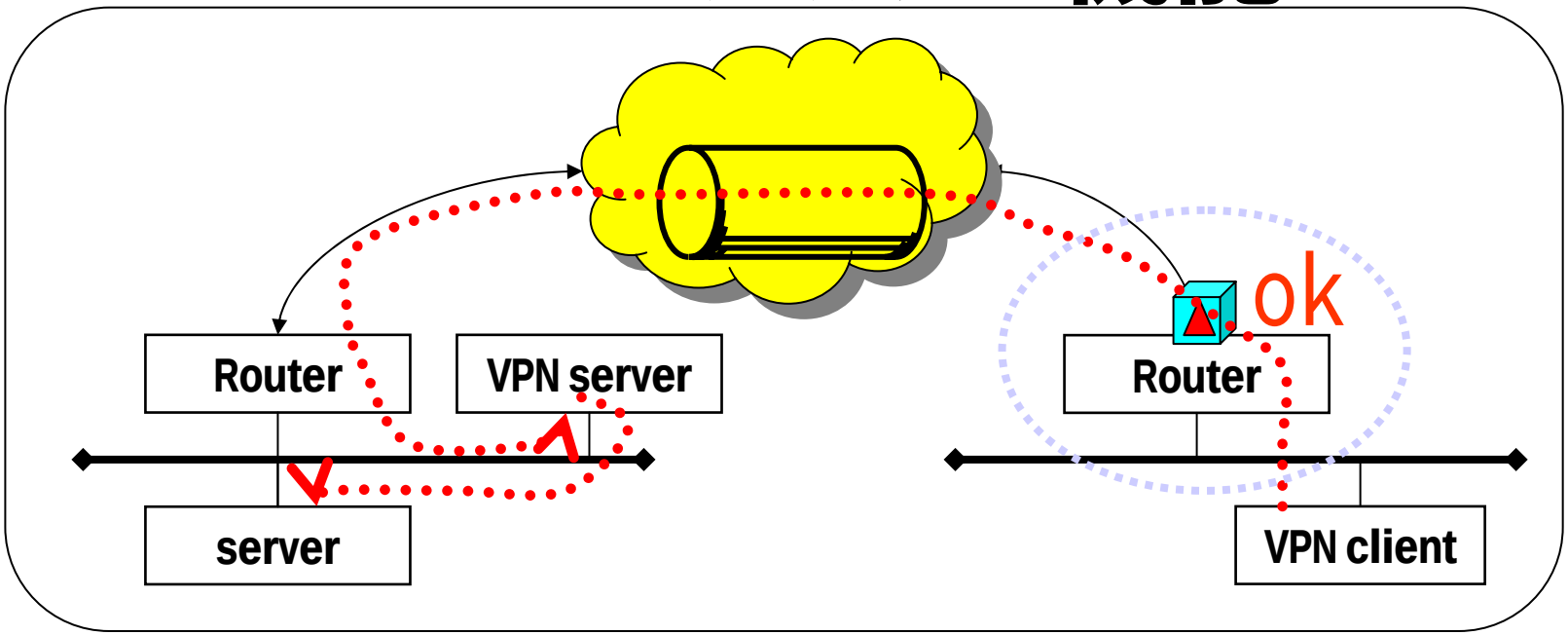
[説明]

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

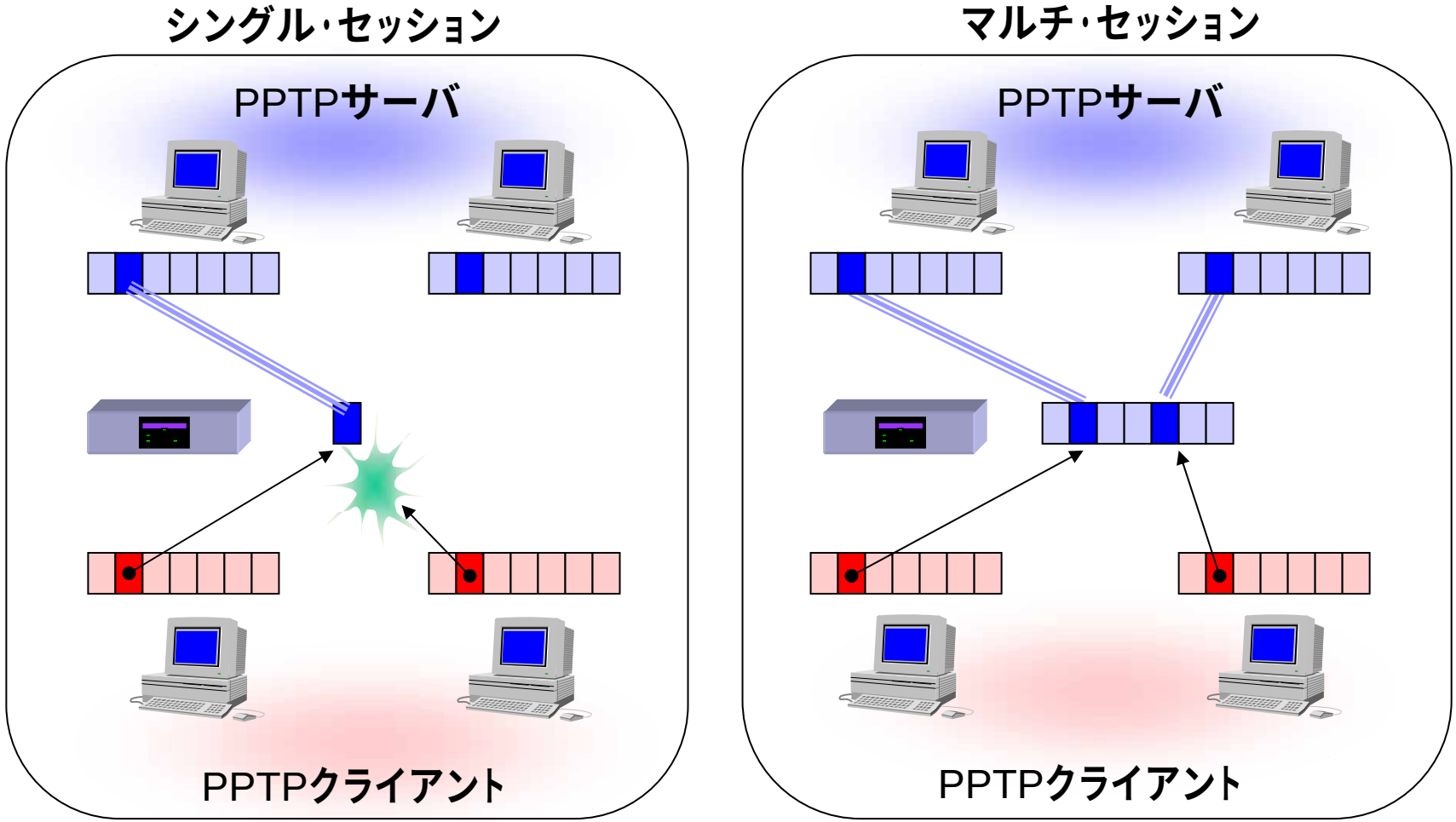


VPNやIPv6トンネルのためにICMP,TCP,UDPとは異なるプロトコルが利用される。これらのプロトコルに対しても、アドレス変換を行う機能。

⇒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



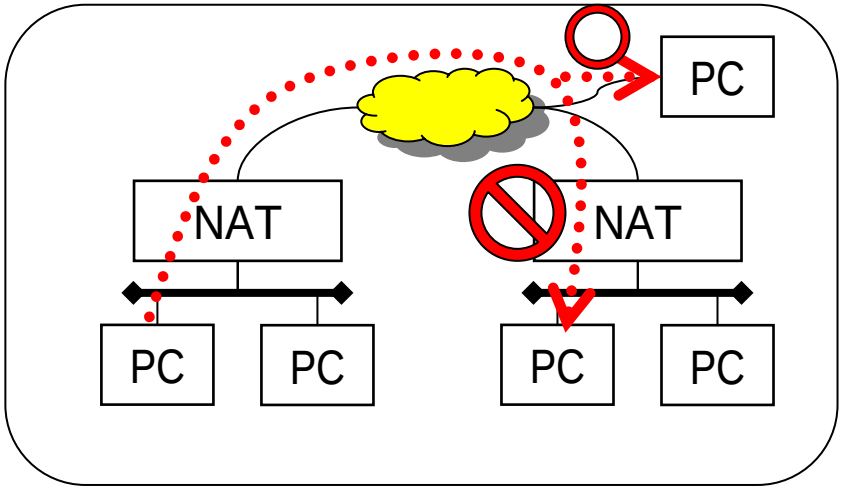
･同時に複数のMicrosoft VPN通信(PPTPによるVPN)が可能となる

PPTPのマルチセッション対応の仕様

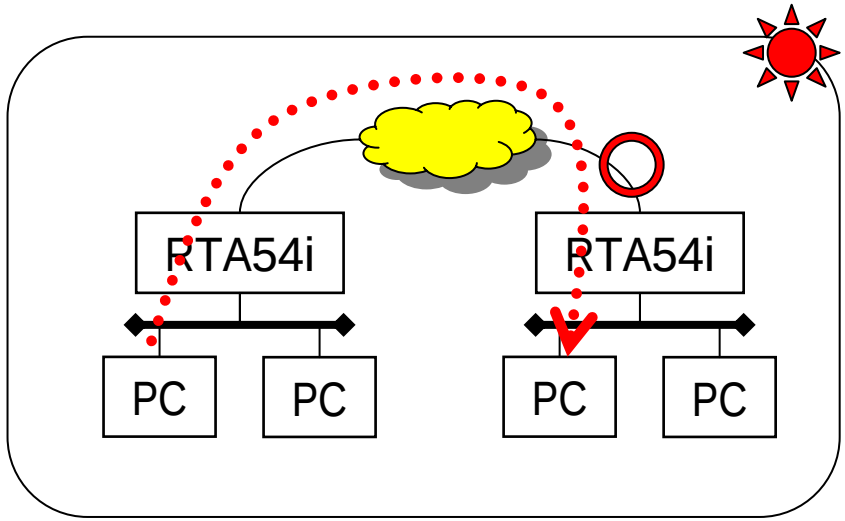
IPマスカレードを動作させている時に、PPTPによるMicrosoft VPNを変換できるようにした。ルータ、Windows PC、Windows サーバのすべてで特別な設定は必要なく、IPマスカレードの内側(プライベートアドレス側)にあるPPTPクライアントである Windows PCから外側(グローバルアドレス側)にあるPPTP サーバであるWindows サーバとの間にPPTPによるVPNトンネルを通常の動作で設定できる。

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/

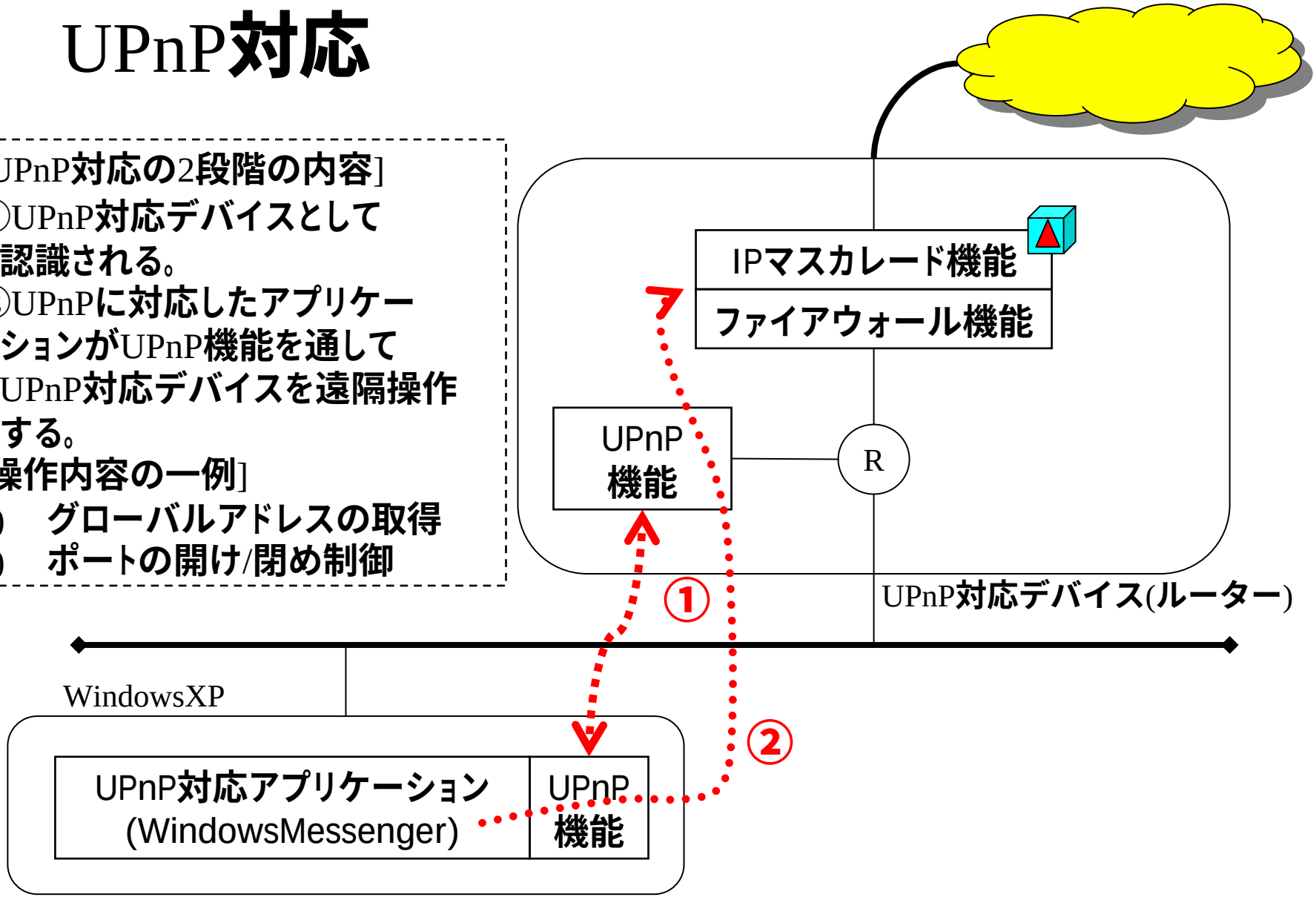
UPnP対応とWindowsMessenger

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

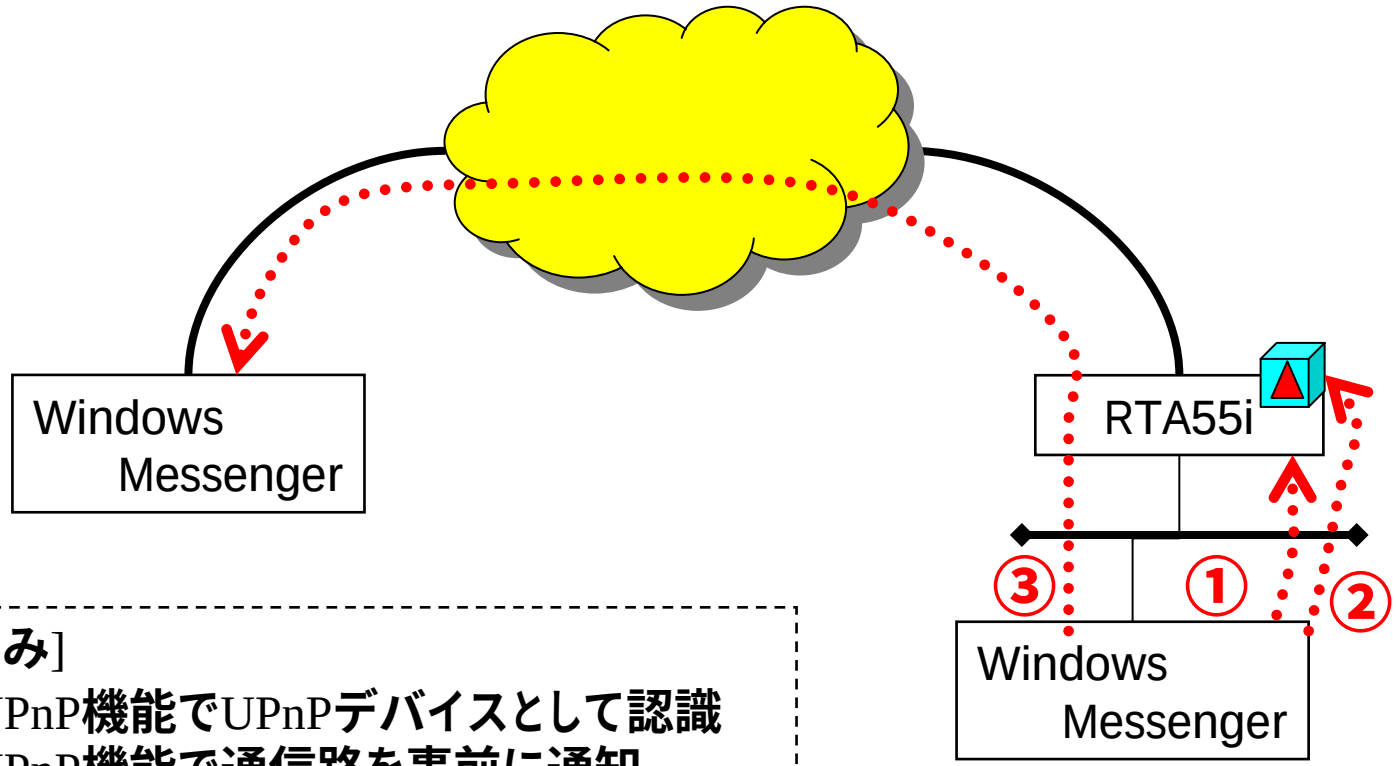
[UPnP対応の2段階の内容]
①UPnP対応デバイスとして
認識される。
②UPnPに対応したアプリケーションがUPnP機能を通して
UPnP対応デバイスを遠隔操作する。
[操作内容の一例]
1) グローバルアドレスの取得
2) ポートの開け/閉め制御



Windows Messenger対応とは？

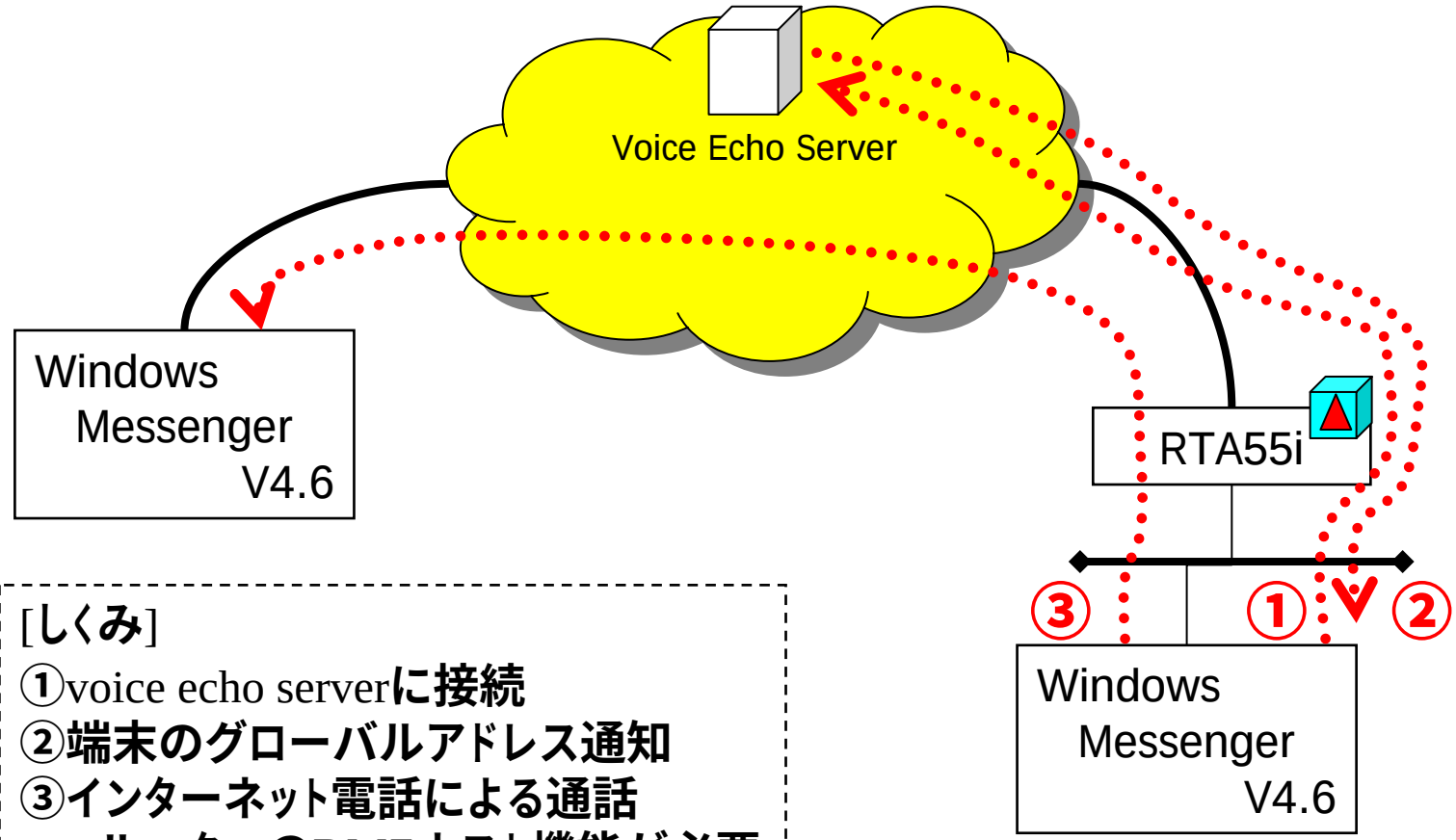
[やりたいこと]
・IPマスカレード利用環境でWindowsMessengerの
　機能を確実に使いたい。
[手段]
1) UPnP機能による対応
2) WindowsMessenger V4.6のNAT Traversal機能
　＋　DMZホスト機能
3) IPマスカレードでSIPのアドレス書換えによる対応

Windows MessengerのNAT越え#1
(UPnP機能対応)



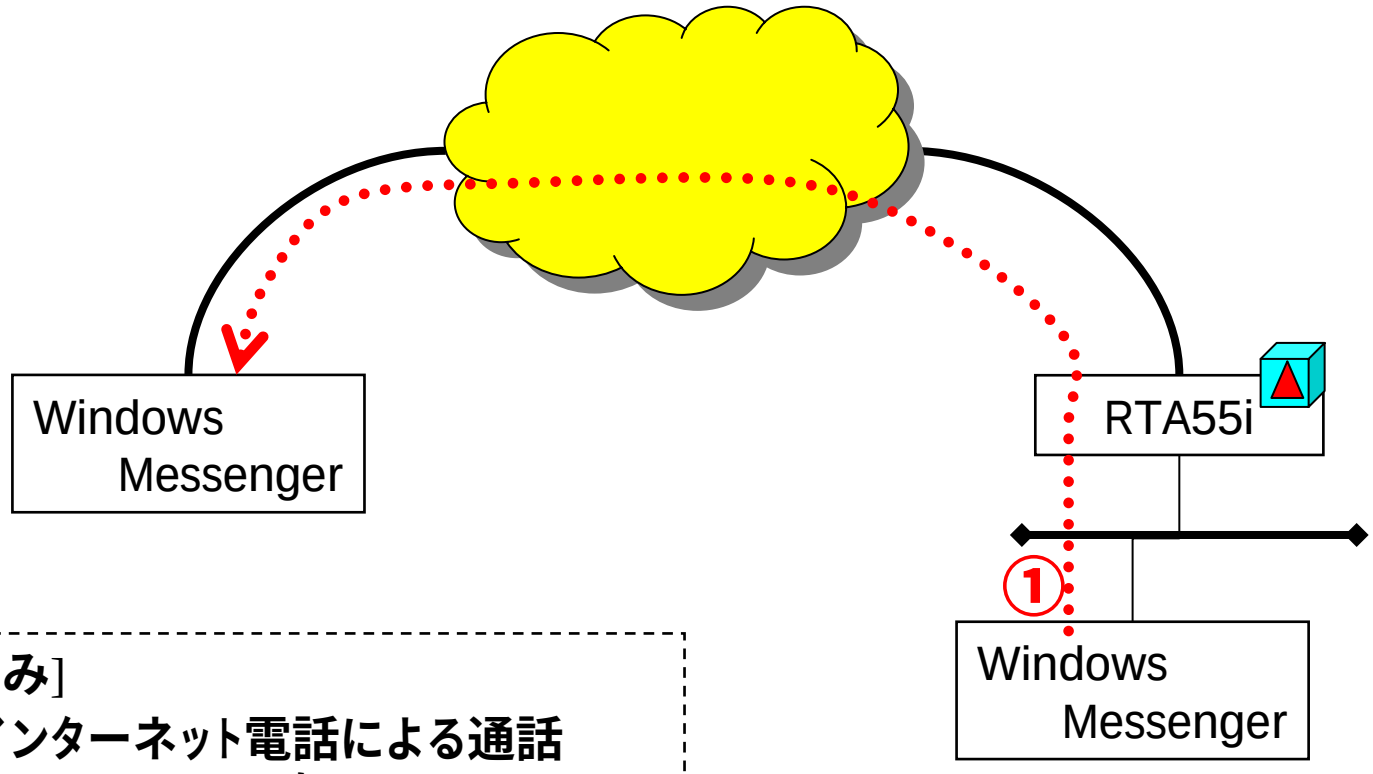
[しくみ]
①UPnP機能でUPnPデバイスとして認識
②UPnP機能で通信路を事前に通知
→ルーターが通信路の開閉
③インターネット電話による通話

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]

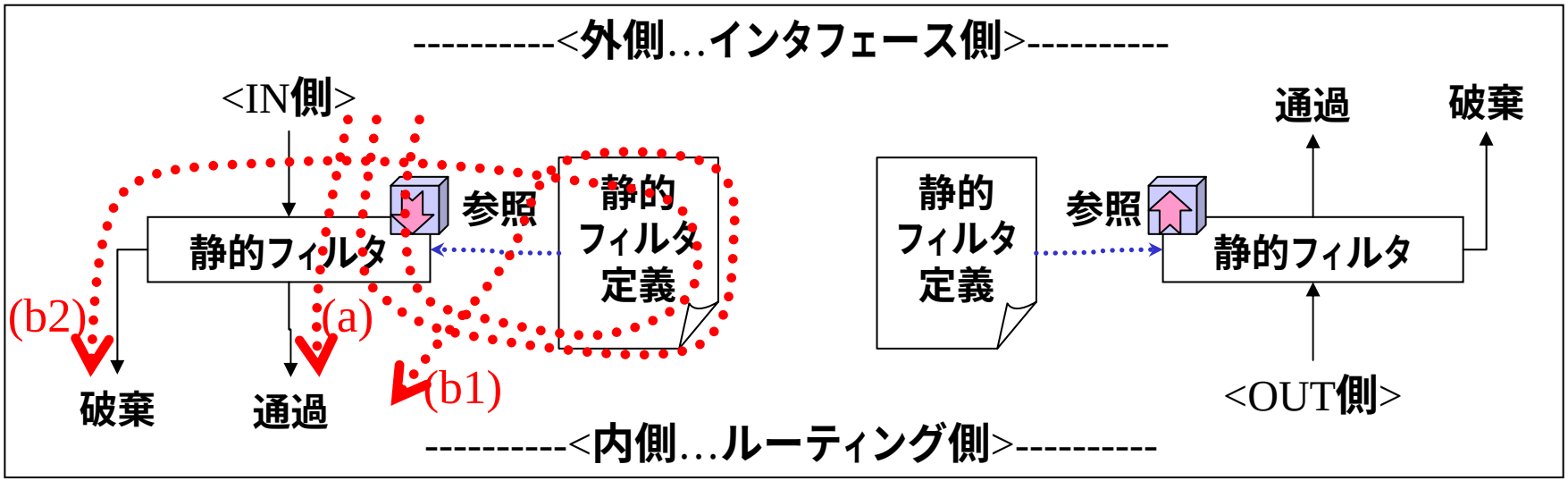
・Windows XPのリモートデスクトップを利用する場合には、静的IPマスカレードで「TCPの3389番ポート」を通すように設定する必要があります。

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

フィルタリング

1) 静的フィルタリング
2) 静的セキュリティ・フィルタ
3) 不正アクセス検知
4) 動的フィルタリング
5) ネットボランチのセキュリティ・レベル
6) 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

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。

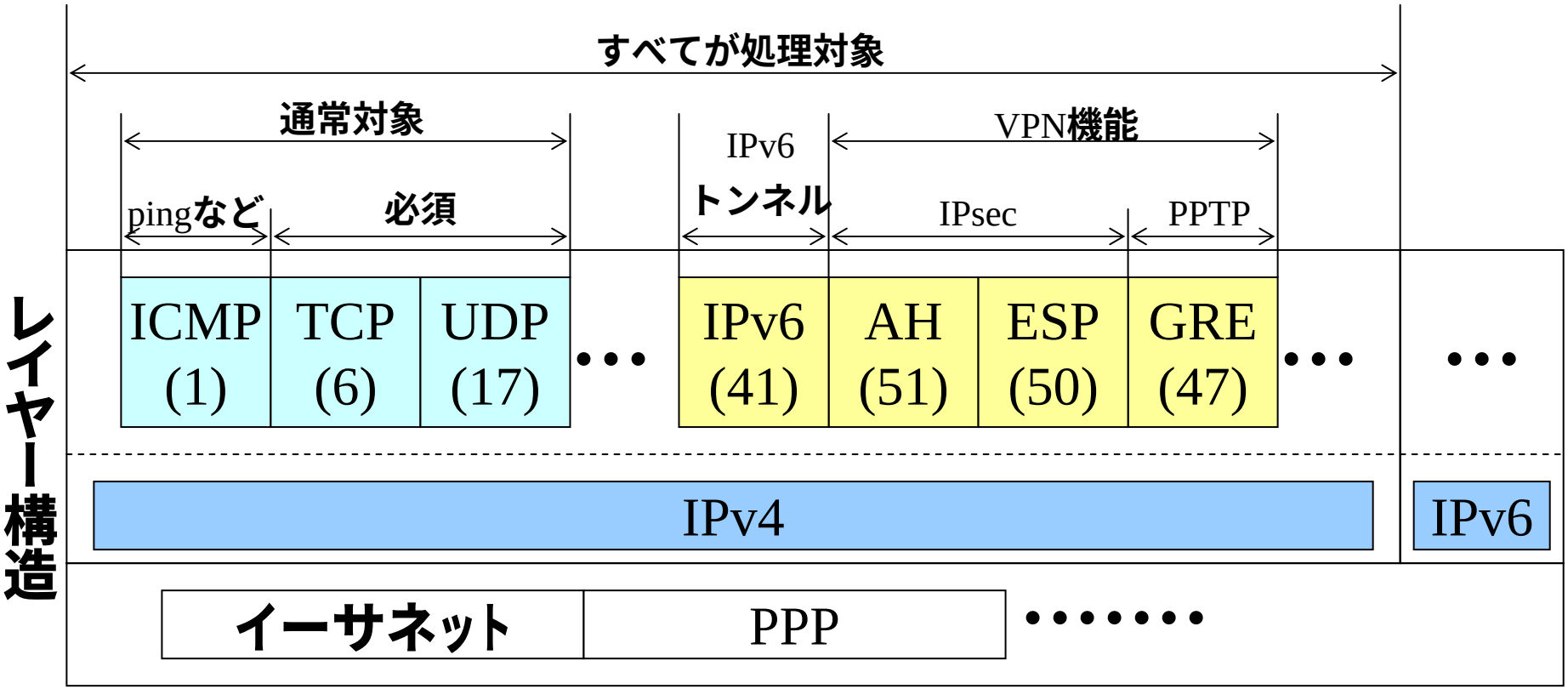
b) フィルタに何か適用されている場合、パケット単位で、

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。

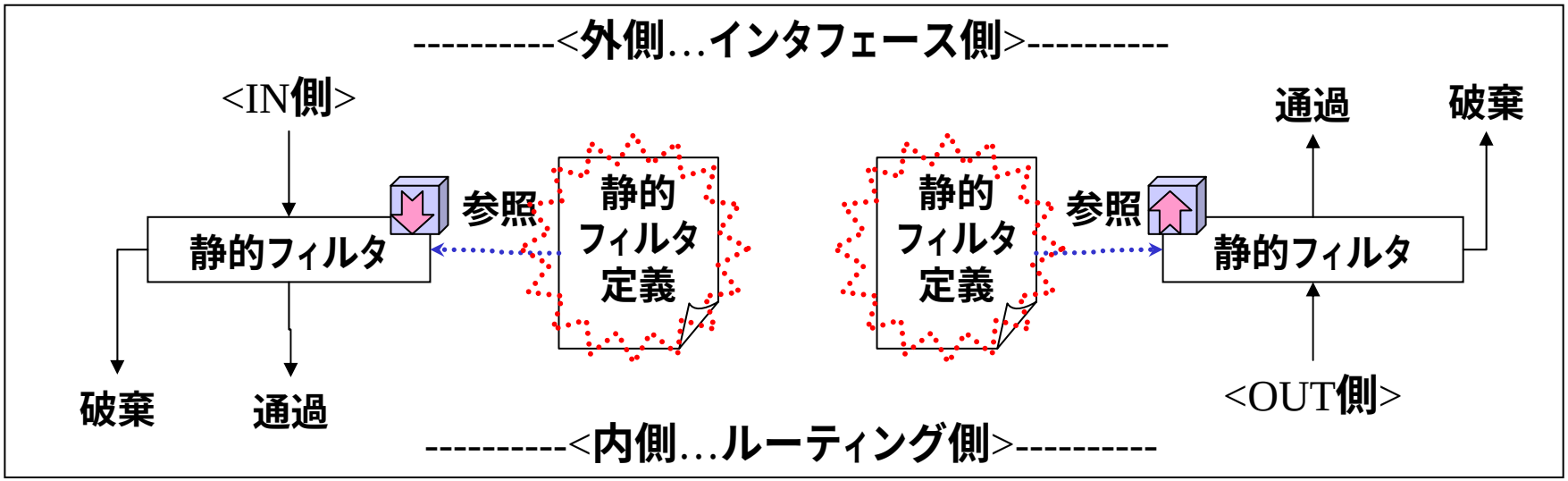
b2) すべてのパターンにマッチングしなければ、破棄される。

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。

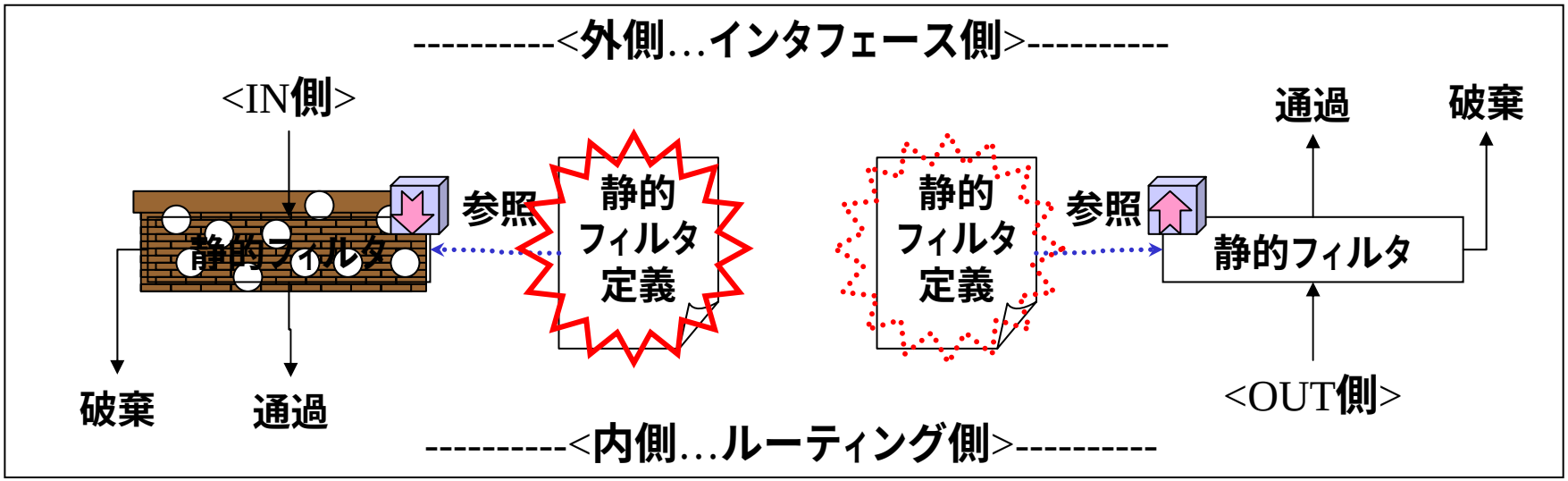


危険なポートを閉じるフィルタ



[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



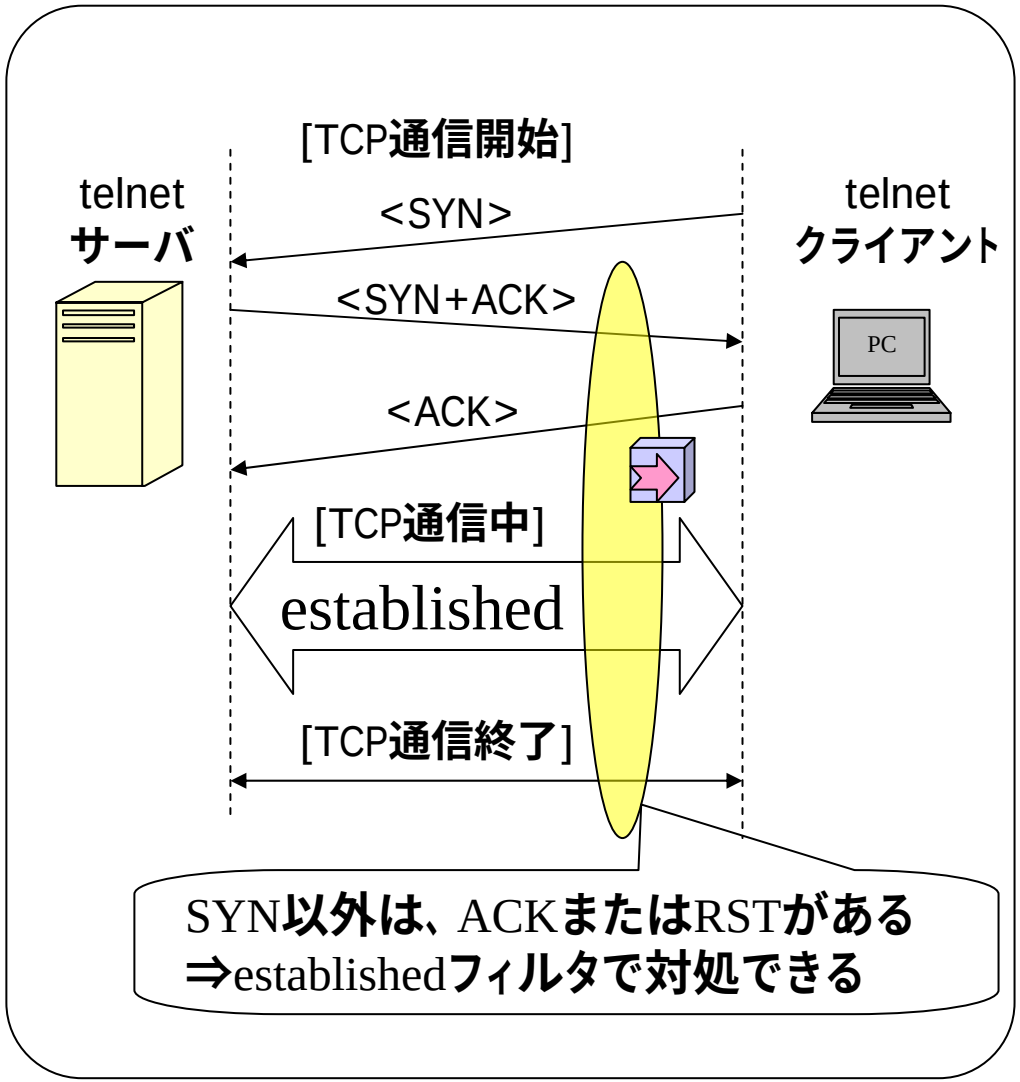
[ポリシー]
・基本的に全閉。使用する通信だけを通す。
[使用する通信]
・TCPは、establishedで確保される通信。
・UDPは必要最低限。
[悩み]
・「establishedフィルタで対処できないこと」、「ftpのアクティブ転送」、
「常に開けておくUDP」など

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



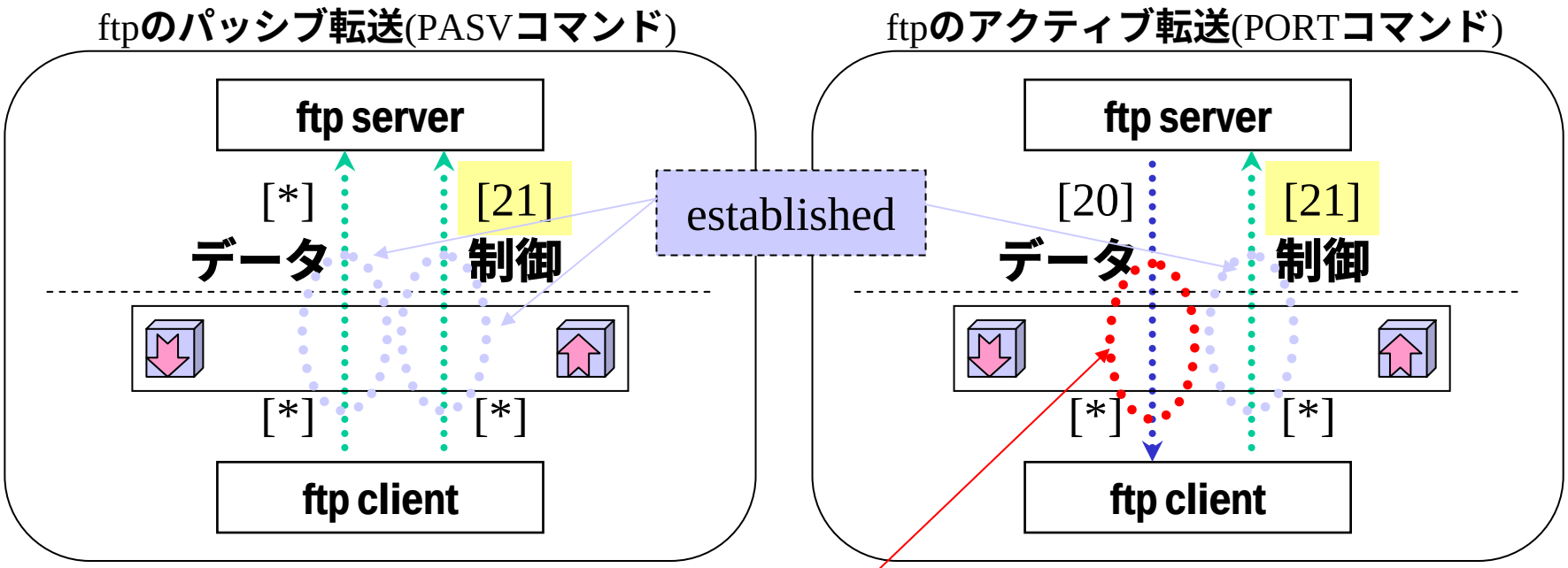
[目的]
- 静的フィルタリングにより外部からの不必要なTCP接続要求を破棄する。

[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。

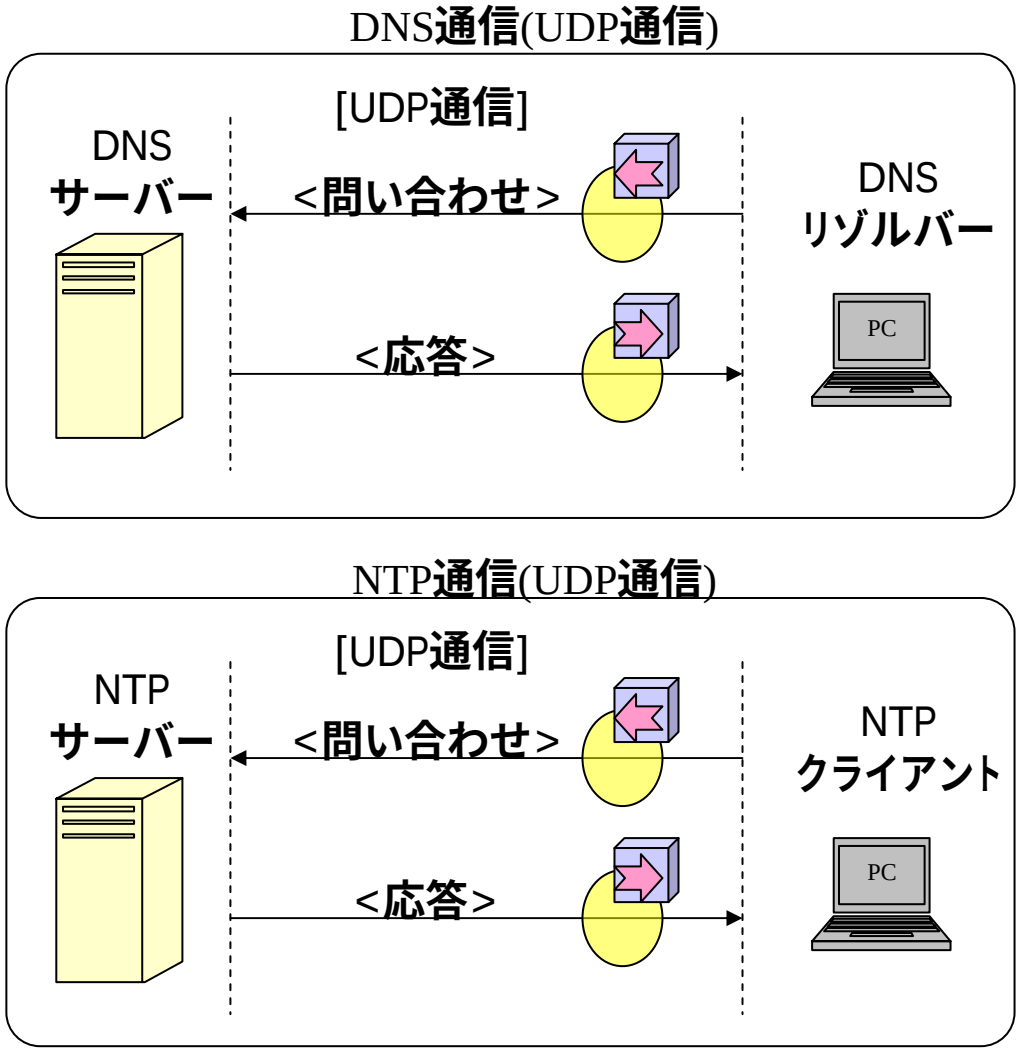
[解決策]

・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

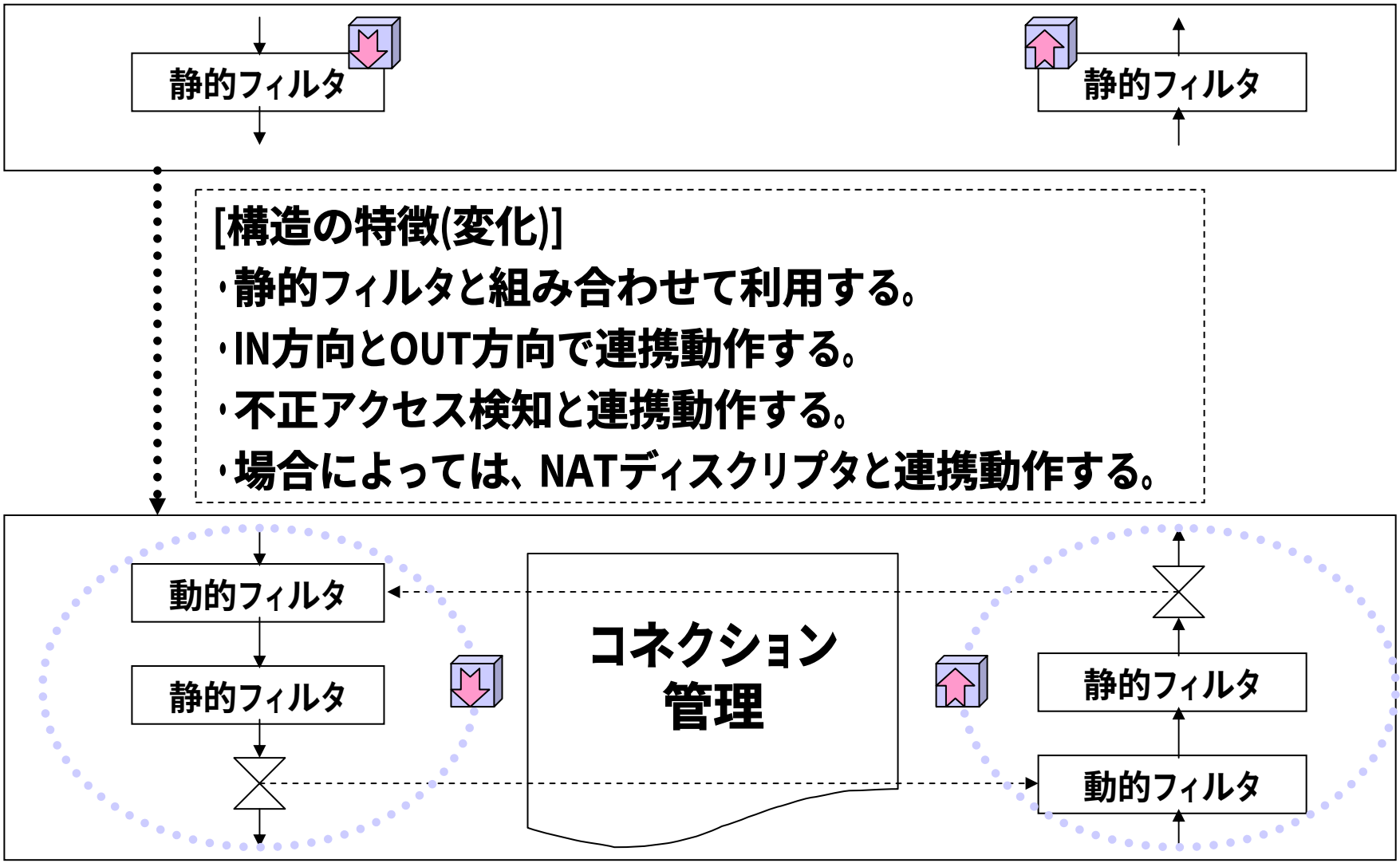
・セキュリティ的に強固な代理サーバを用意する

動的フィルタリングの特徴

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

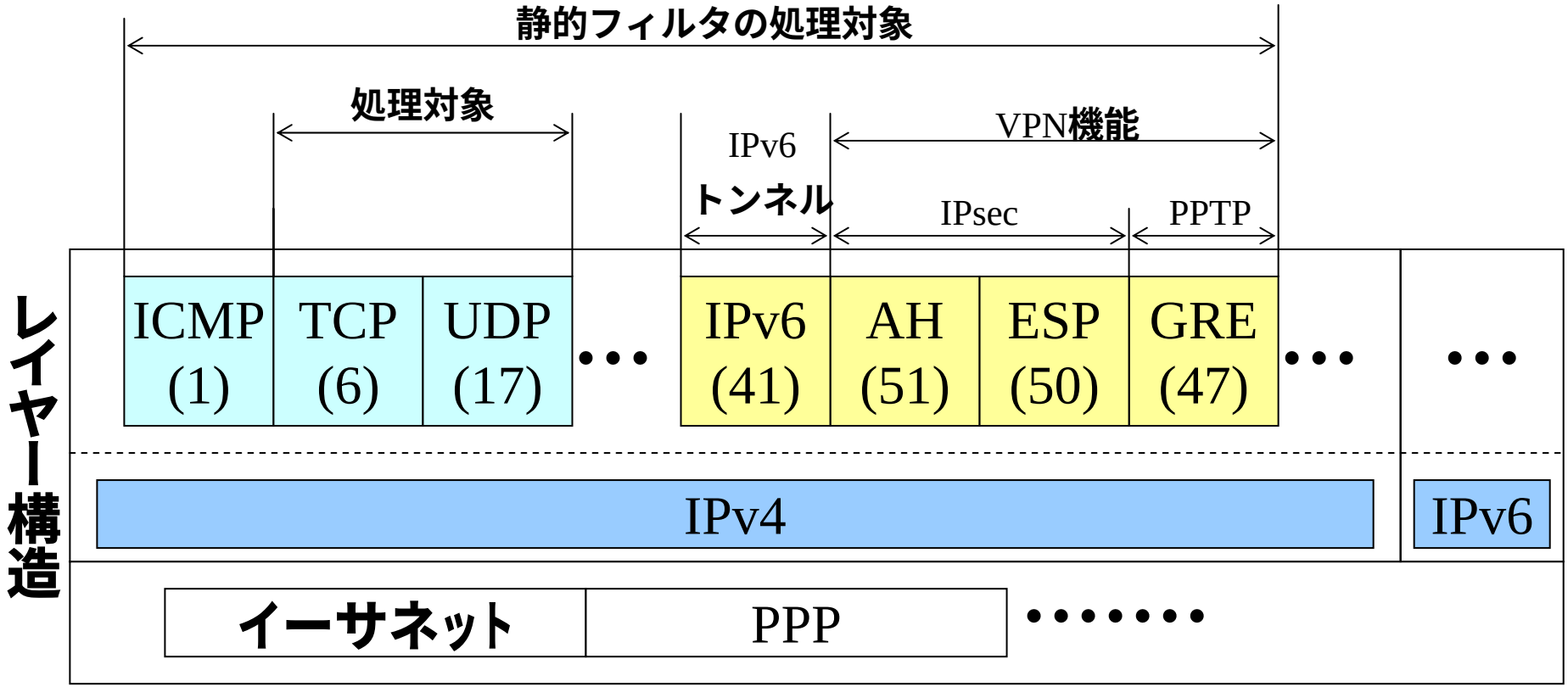
[静的フィルタリングの弱点]
・安全性と安定性を確保した十分なフィルタリングを行うためには、
高度な知識が求められる。
・ftp通信のフィルタリングにおける安全性
・UDP通信のためのフィルタの安全性
・TCP通信のためのestablishedフィルタの安全性

動的フィルタリング構造の特徴

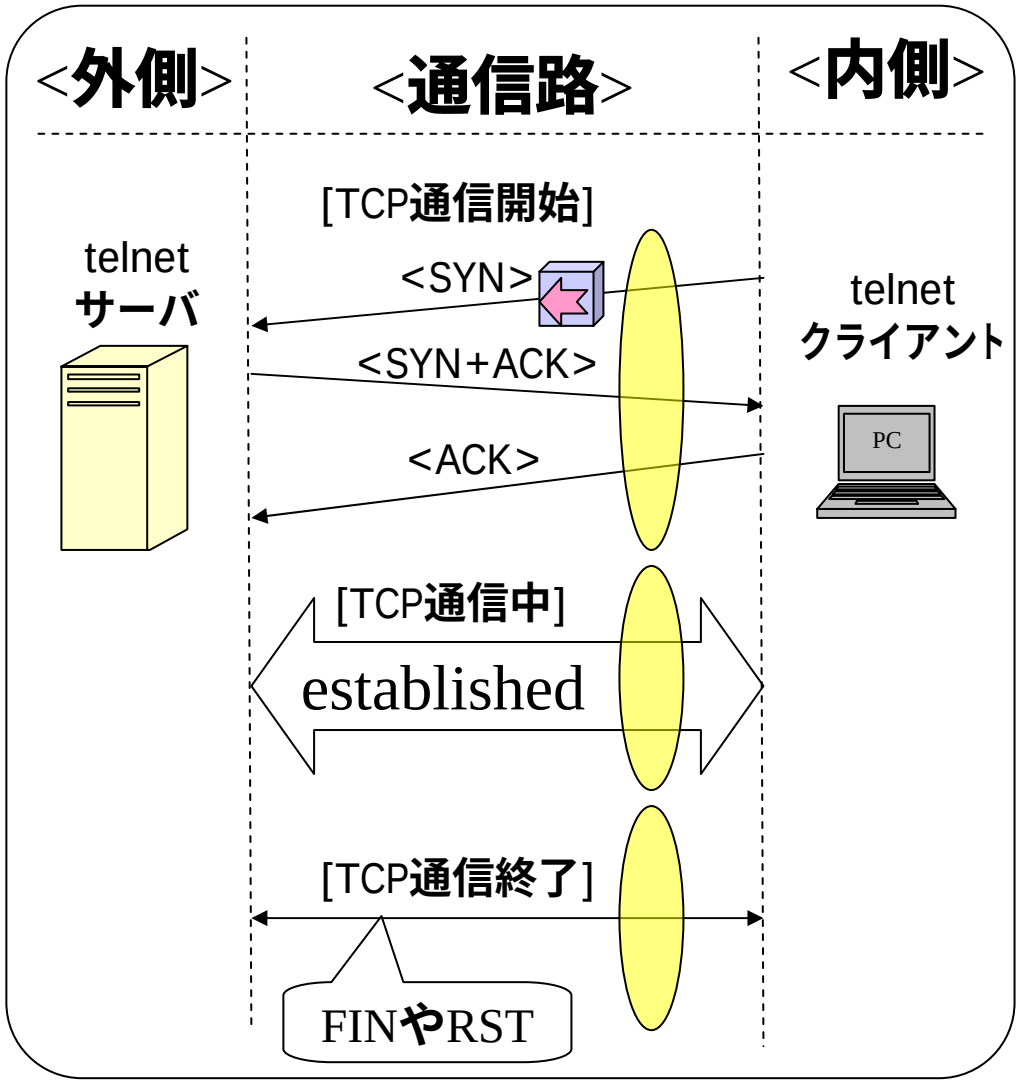


動的フィルタリングの処理対象

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



TCPの動的フィルタ (基本動作)

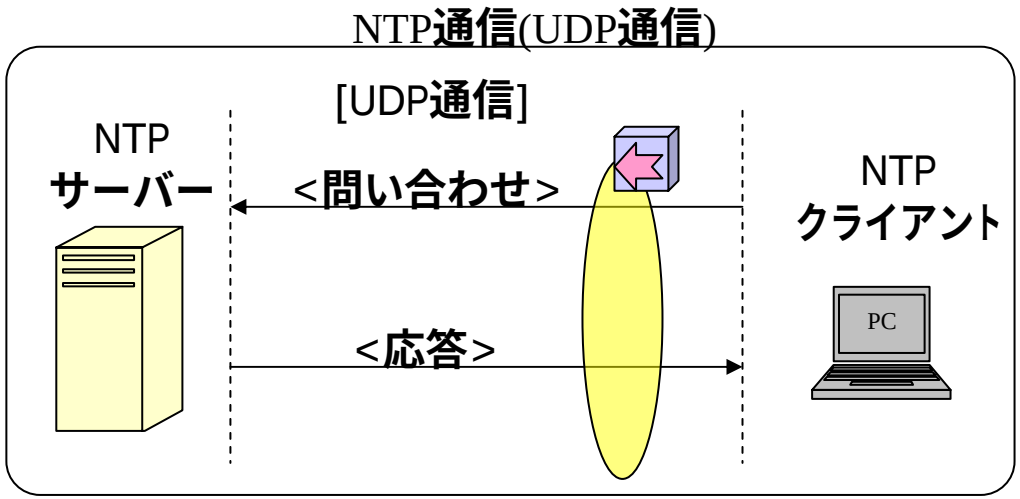


[開くトリガー]
- コネクションを開くSYN情報を持ったパケット

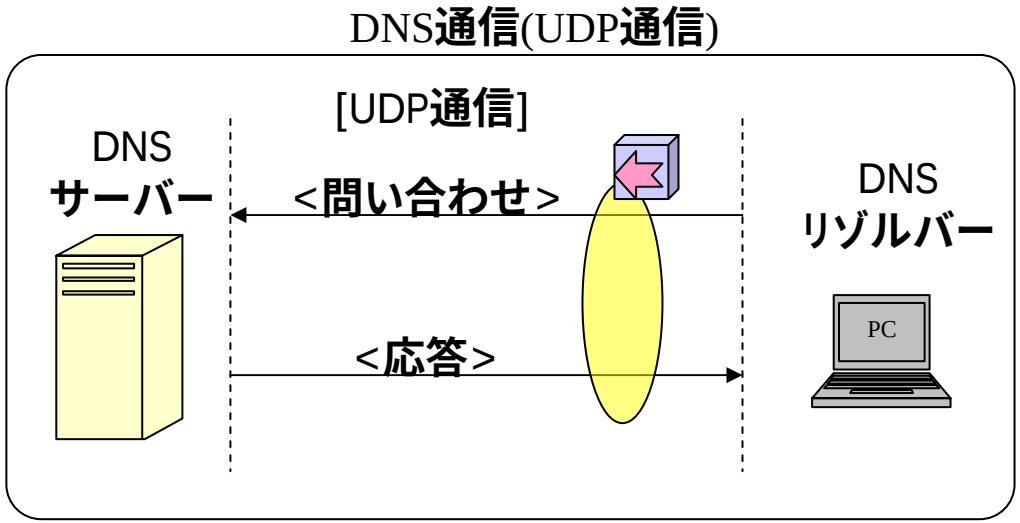
[確立の監視]
- TCPコネクションを開始するハンドシェイクの監視

[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



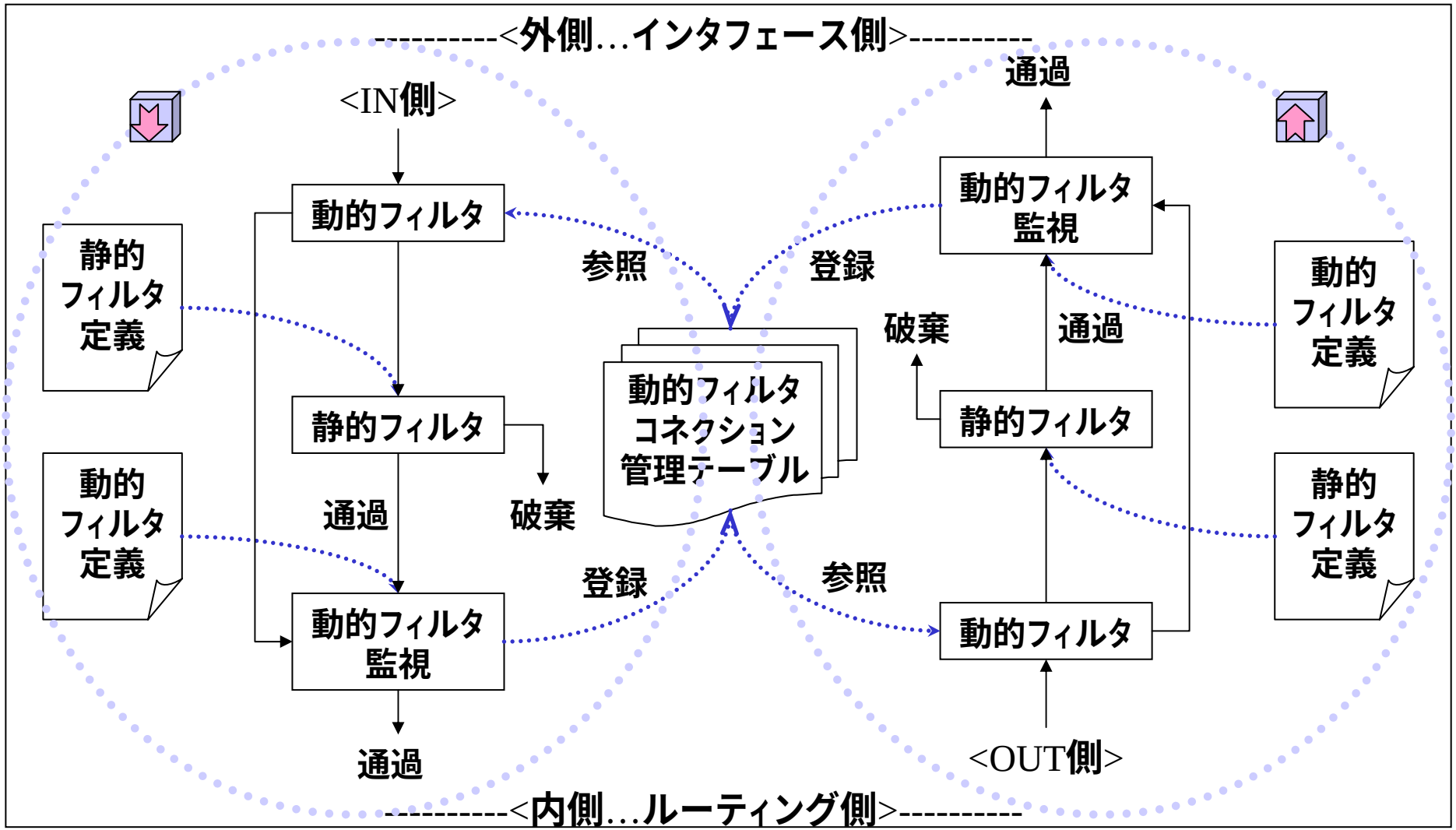
[DNSの処理]
・問い合わせパケットに対して、必ず、応答パケットがある。
→タイマー管理に加えて、応答パケットの到着で閉じる。

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)

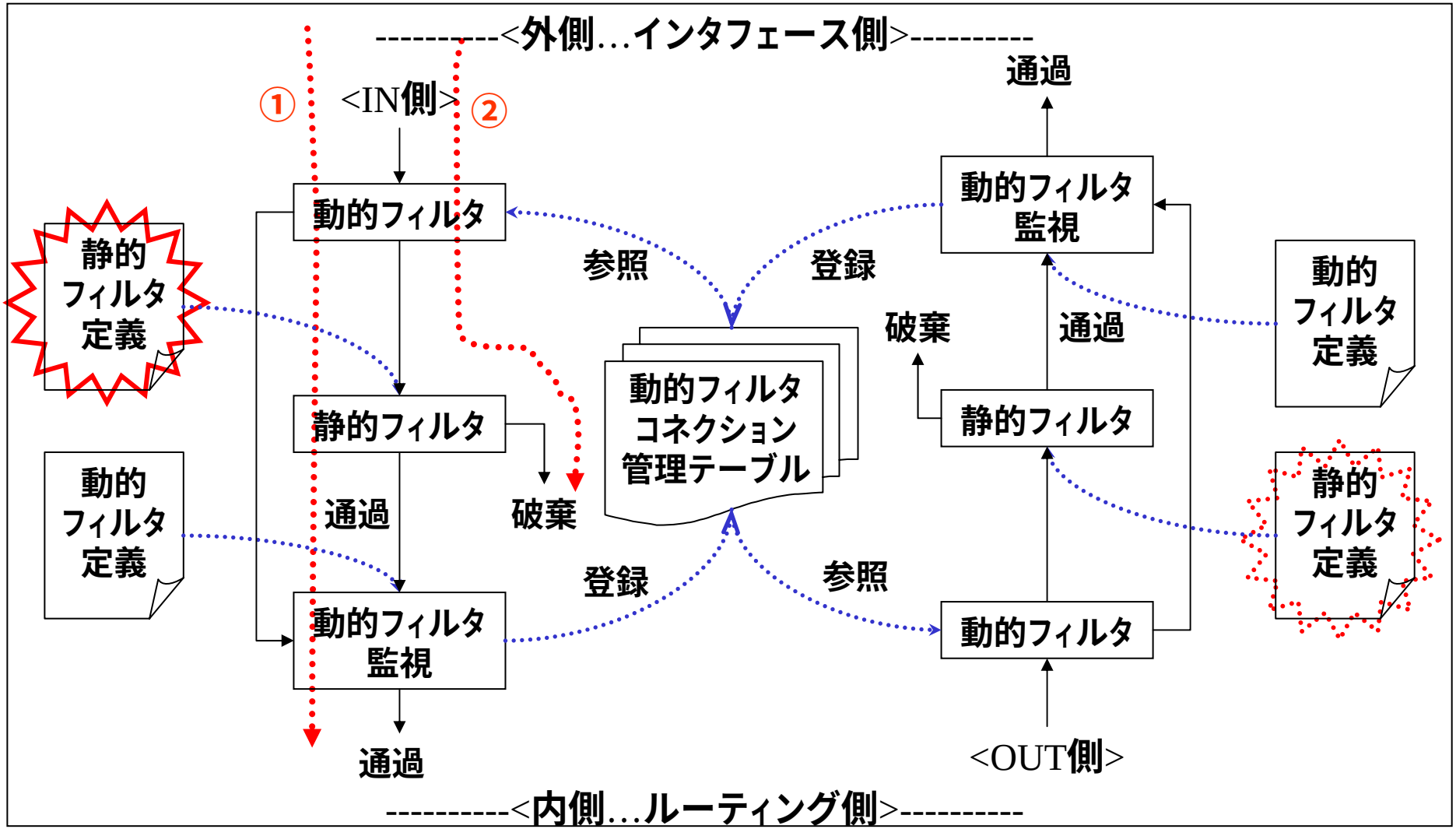
セキュリティ・レベル	1	2	3	4	5	6	7
予期しない発呼を防ぐフィルタ	○	○	○	○	○	○	○
NetBIOS等を塞ぐフィルタ (ポート番号:135,137,138,139,445)		○	○	○	○	○	○
プライベートアドレスのままの通信を禁止するフィルタ			○		○		○
静的セキュリティ・フィルタ (従来のセキュリティフィルタ)				◎	◎		
動的セキュリティ・フィルタ (強固なセキュリティ・フィルタ)						☆	☆

ファイアウォールの構造

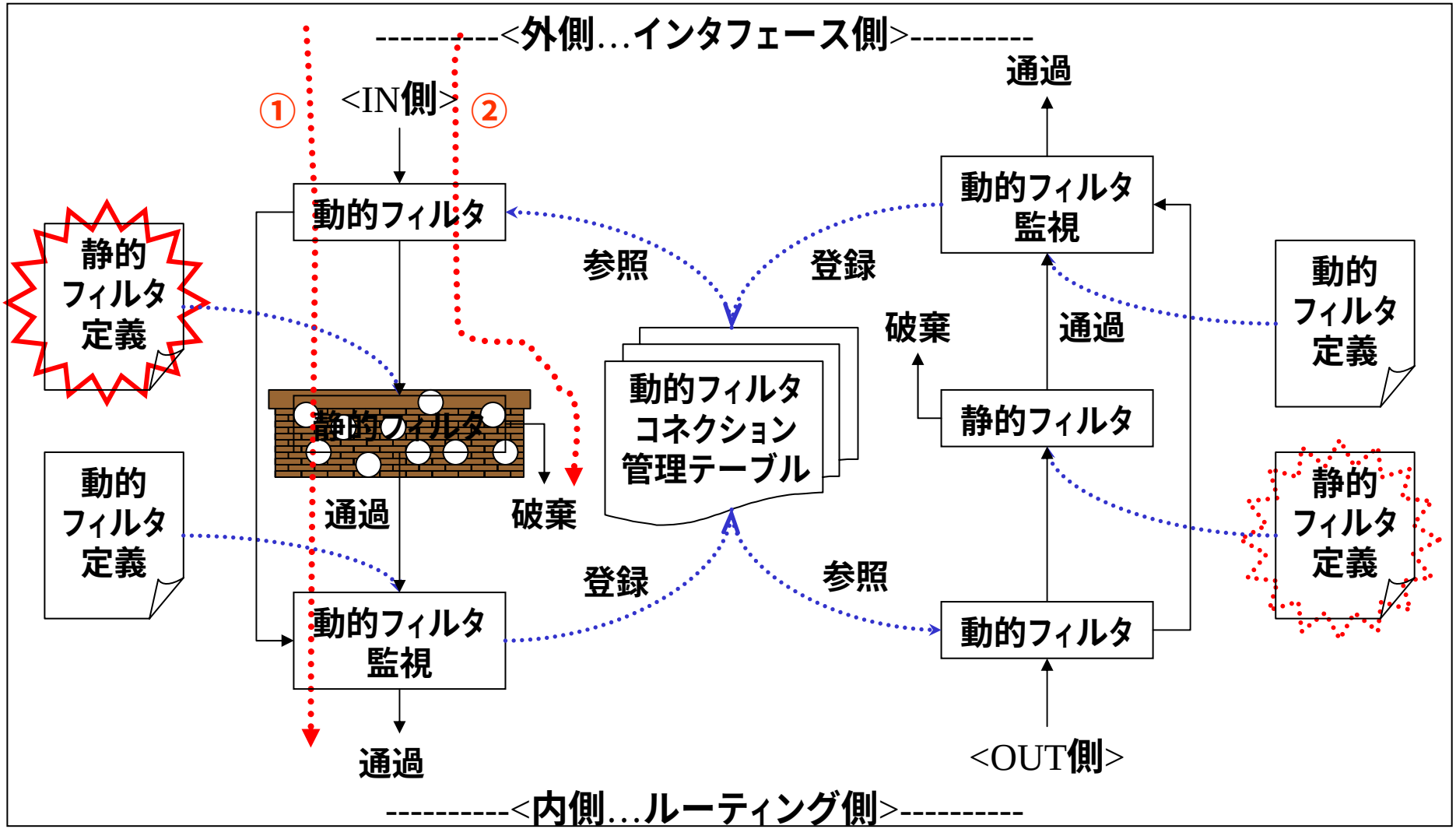


http://www.rtpro.yamaha.co.jp/RT/docs/firewall/index.html

一部の通信路を塞ぐ


----------<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
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



設定例#1

(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 * * * * *

[条件]

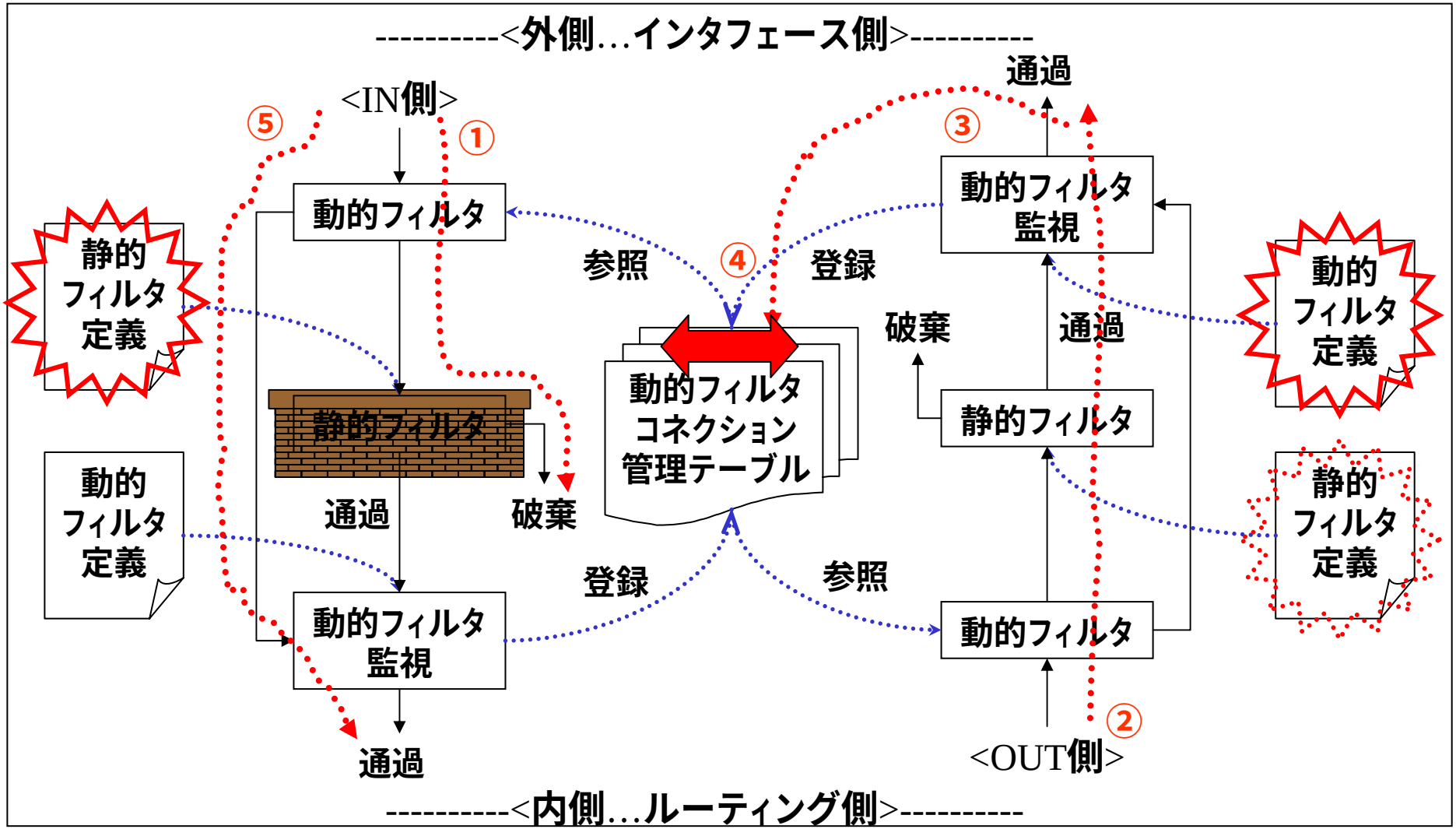
- ネットボランチ RTA54i
- プロバイダ接続設定の
  セキュリティ・レベル5

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
```


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

フィルタ関係の付録資料

- 静的フィルタのタイプ
- 動的フィルタのアプリケーション名
- 不正アクセス検知の内容

静的フィルタのタイプ

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

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

動的フィルタ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

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

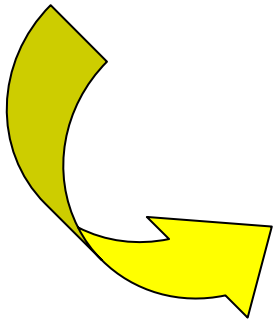
種別	名称	判定条件	
UDP	UDP short header	UDPのlengthフィールドの値が8よりも小さいとき	▲
	UDP bomb	UDPヘッダのlengthフィールドの値が大きすぎるとき	
	UDP port scan	ポートスキャンを受けたとき	△
TCP	TCP queue overflow	TCPのパケットキューが長くなったとき	★
	TCP no bits set	フラグに何もセットされていないとき	
	TCP SYN and FIN	SYNとFINが同時にセットされているとき	
	TCP FIN and no ACK	ACKのないFINを受信したとき	
	TCP port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

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、最初にパスワードを設定してもらう。

- **常時接続を想定した高度なフィルタリング機能**

  a) 動的フィルタリング

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

  b) 不正アクセス検知

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

- **フレキシビリティ**

  a) フィルタ定義数の制限緩和(メモリの許す限り)