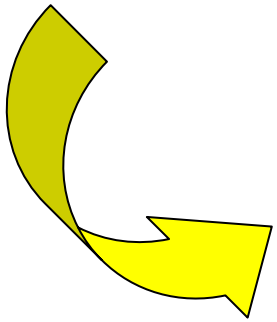
ヤマハ ルーター
ファイアウォール機能
～説明資料～

ヤマハ株式会社
AV･IT事業本部
マーケティング室
2002年3月

目次

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

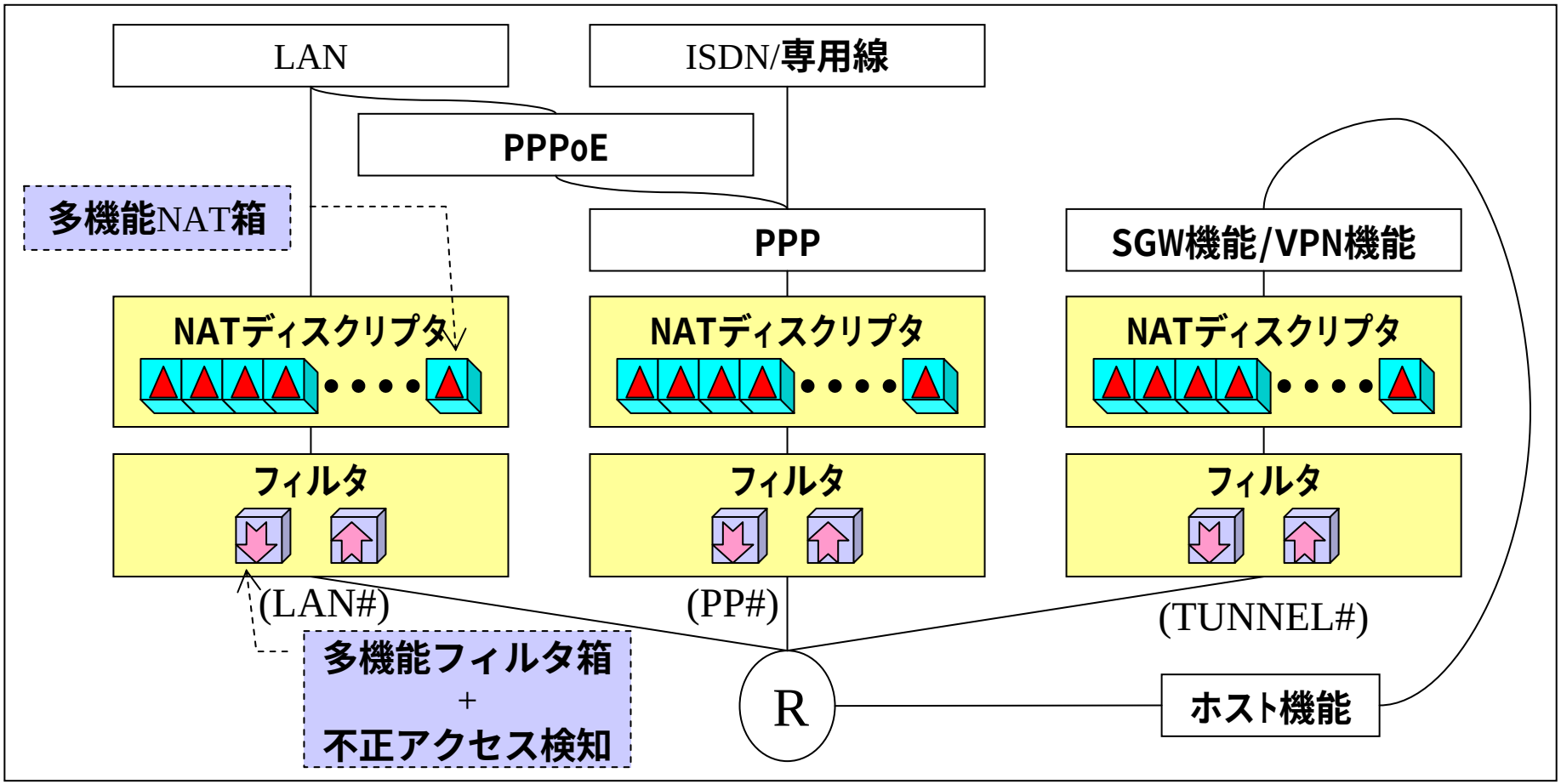
  侵入(Intrusion)や攻撃(attack)を目的とするパケットを受信したときに、それを検出してユーザに通知(ログ、ブザー、メール)

- **フレキシビリティ**

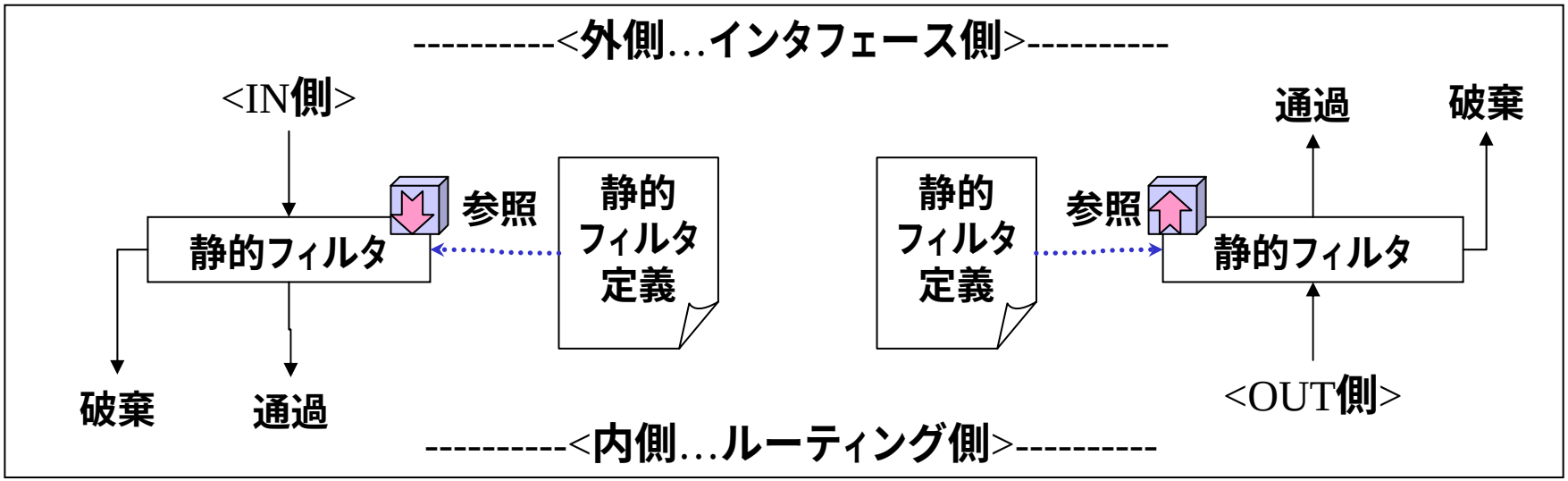
  a) フィルタ定義数の制限緩和(メモリの許す限り)

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。

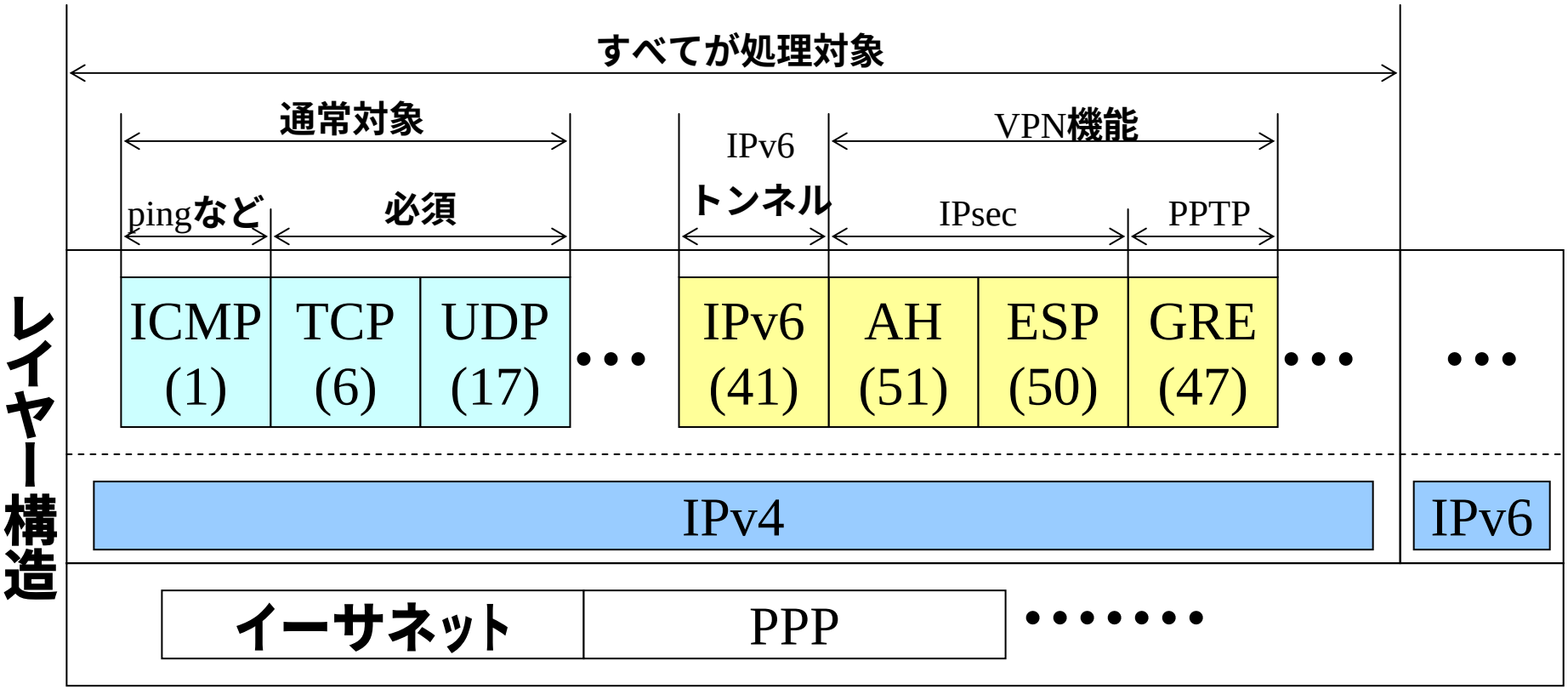
b) フィルタに何か適用されていいる場合、パケット単位で、

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。

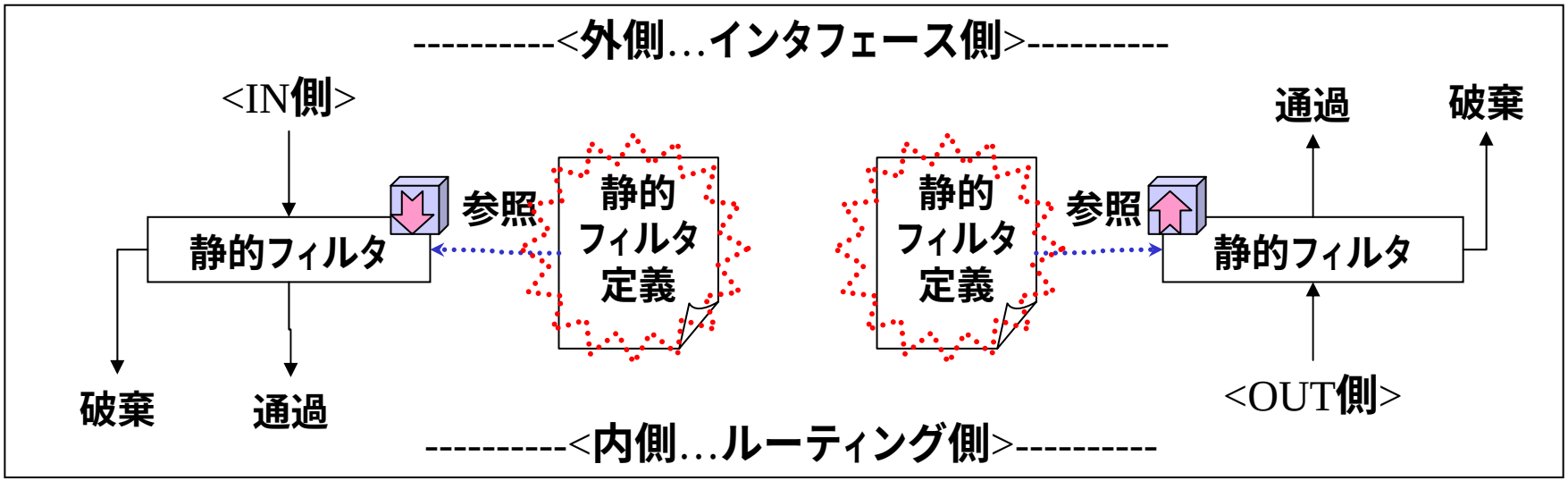
b2) すべてのパターンにマッチングしなければ、破棄される。

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。

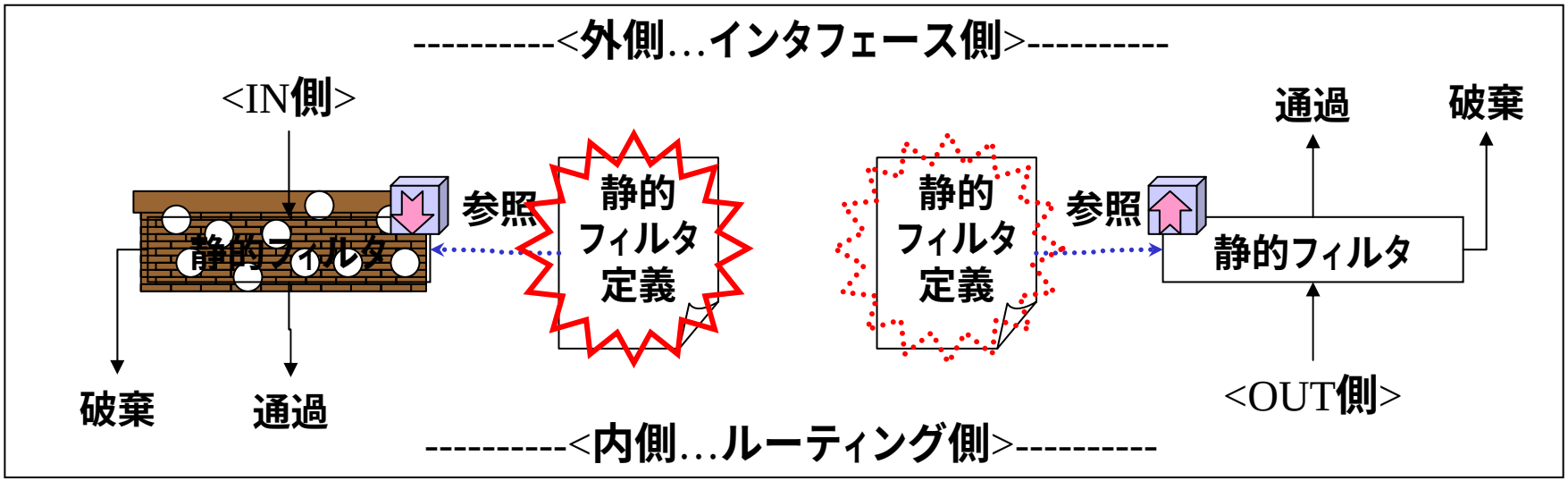


危険なポートを閉じるフィルタ



[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

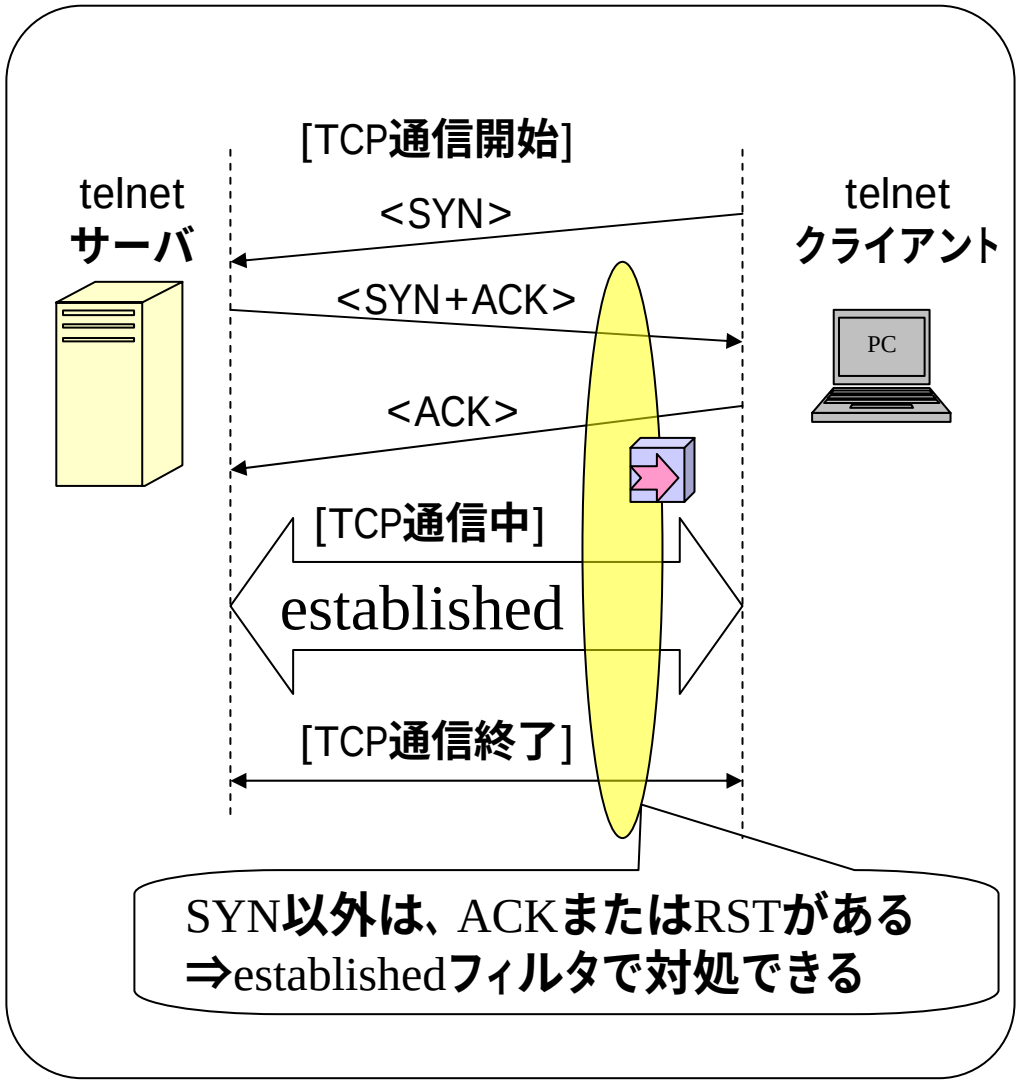


[ポリシー]
・基本的に全閉。使用する通信だけを通す。
[使用する通信]
・TCPは、establishedで確保される通信。
・UDPは必要最低限。
[悩み]
・「establishedフィルタで対処できないこと」、「ftpのアクティブ転送」、
「常に開けておくUDP」など

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
```

TCPのestablishedフィルタ



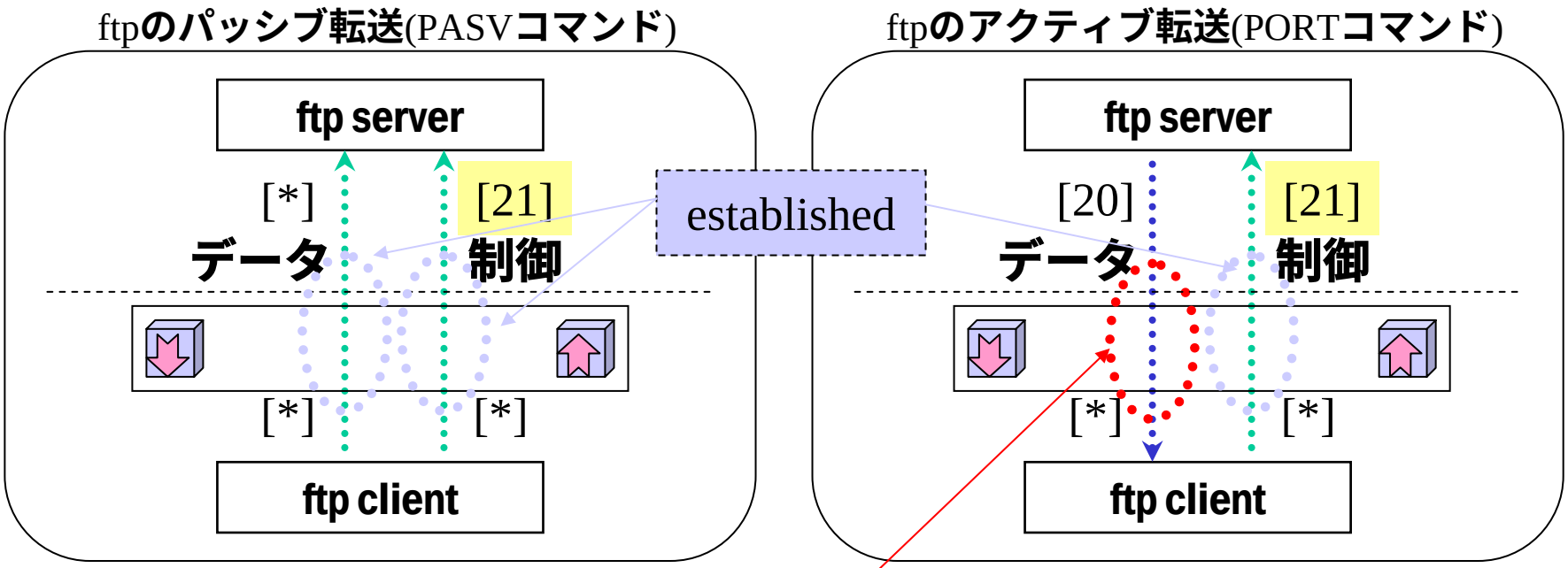
[目的]
- 静的フィルタリングにより外部からの不必要なTCP接続要求を破棄する。

[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。

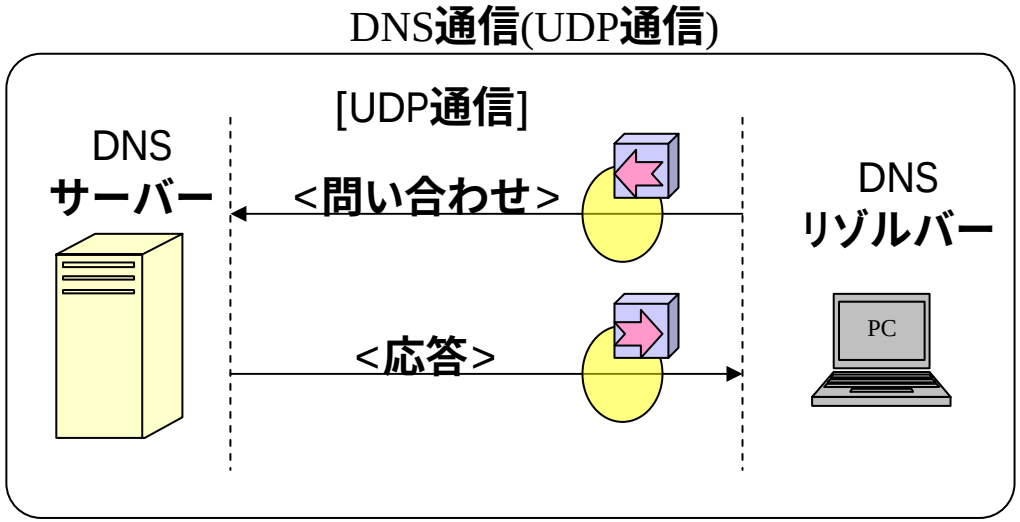
[解決策]

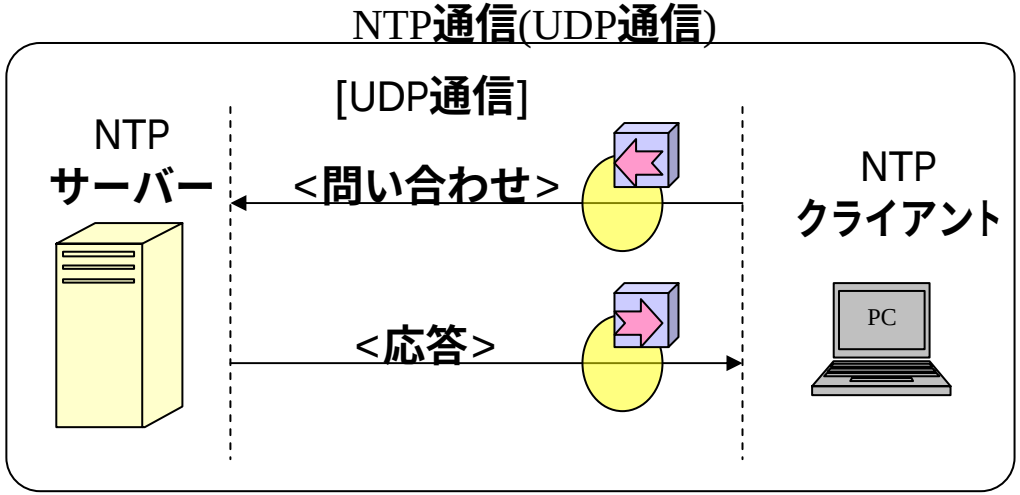
・動的フィルタリング

・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。

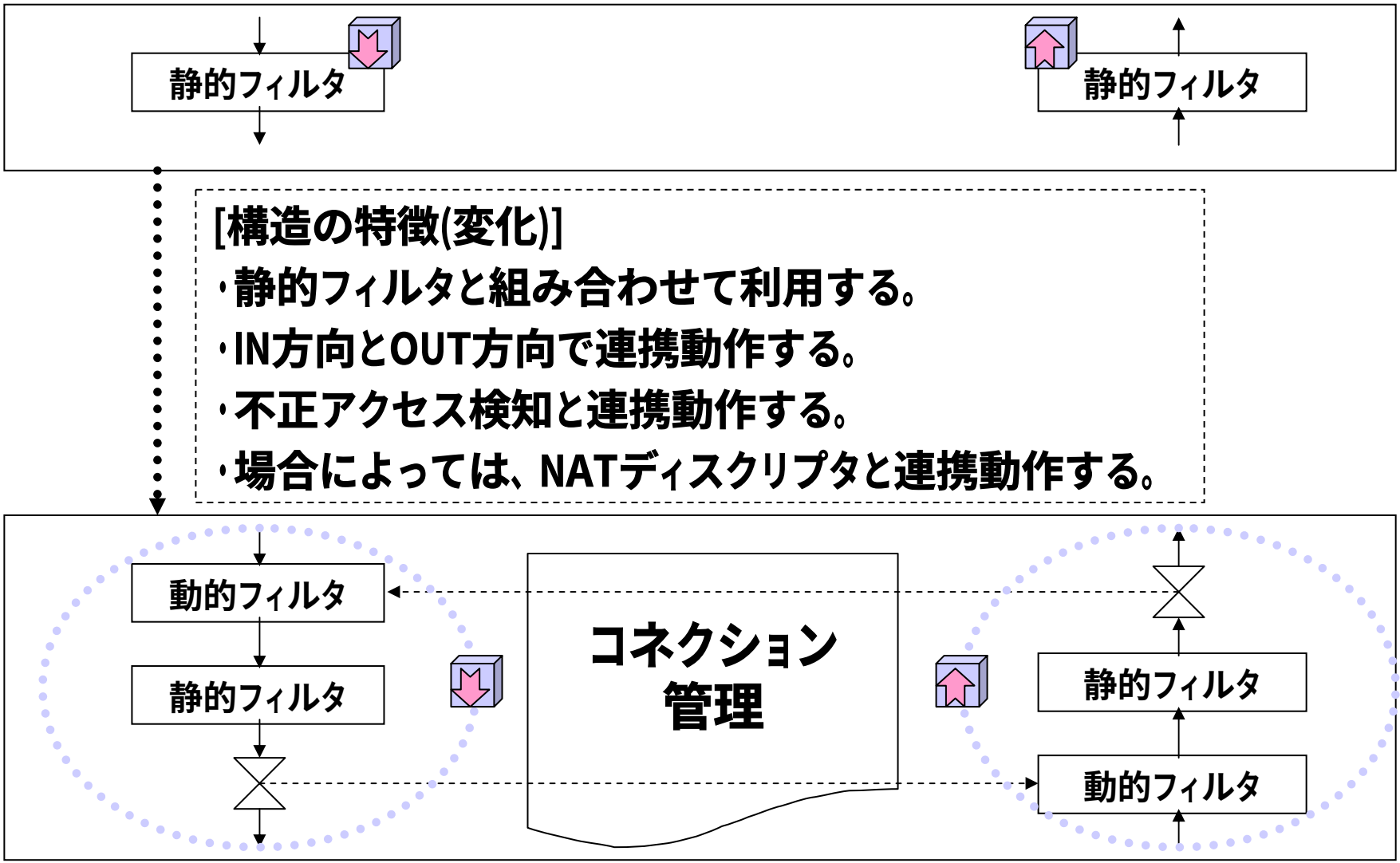
・不正アクセスが明らかであれば、該当パケットを破棄させることも可能です。

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。

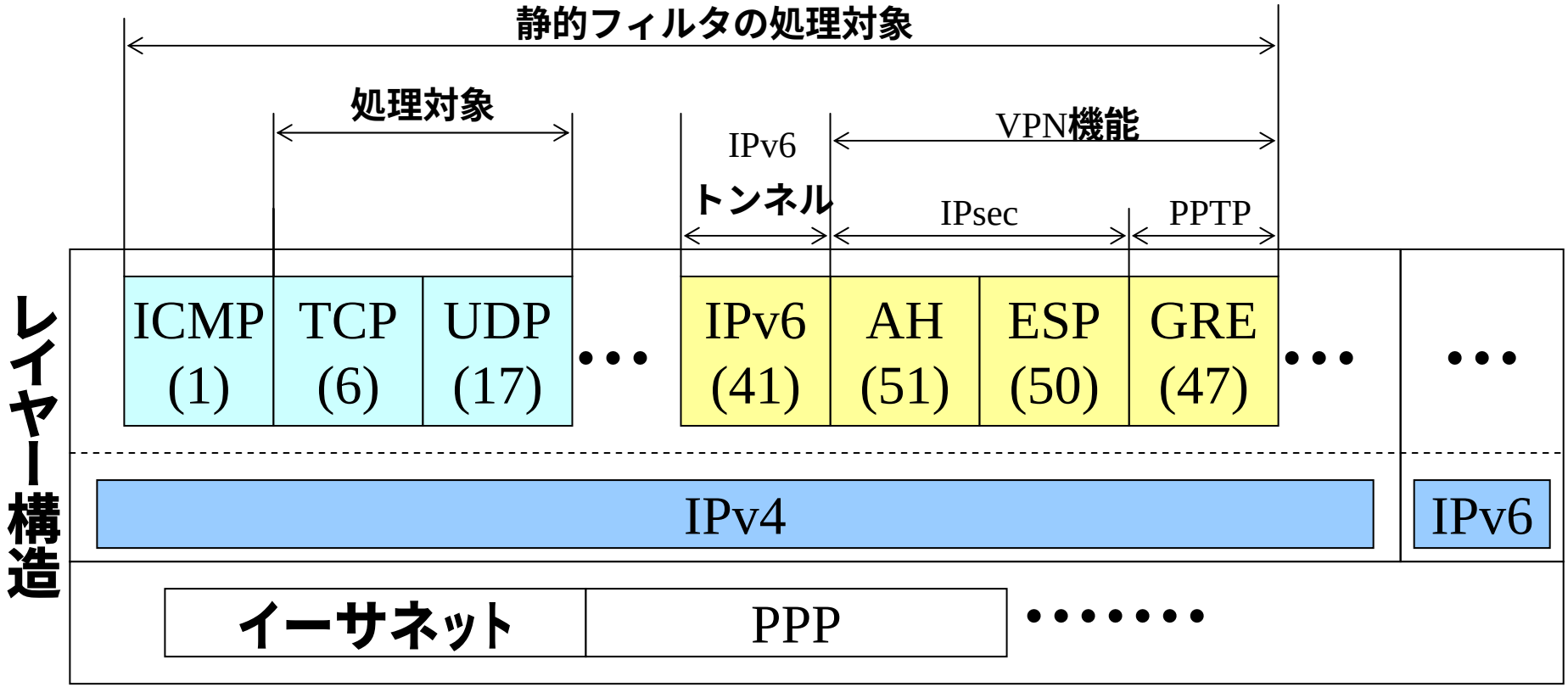
[静的フィルタリングの弱点]
・安全性と安定性を確保した十分なフィルタリングを行うためには、
高度な知識が求められる。
・ftp通信のフィルタリングにおける安全性
・UDP通信のためのフィルタの安全性
・TCP通信のためのestablishedフィルタの安全性

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。

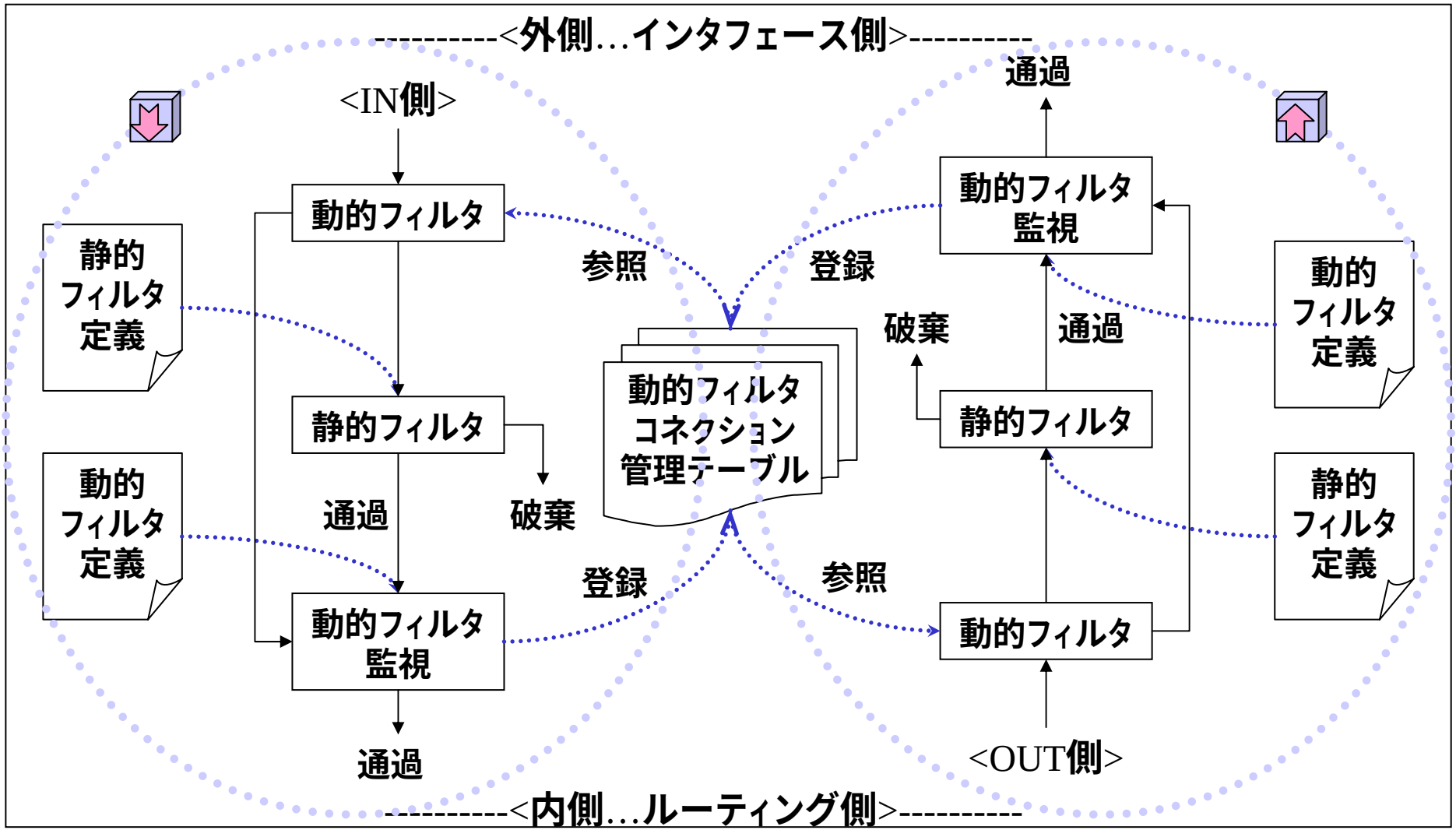


セキュリティ・レベル

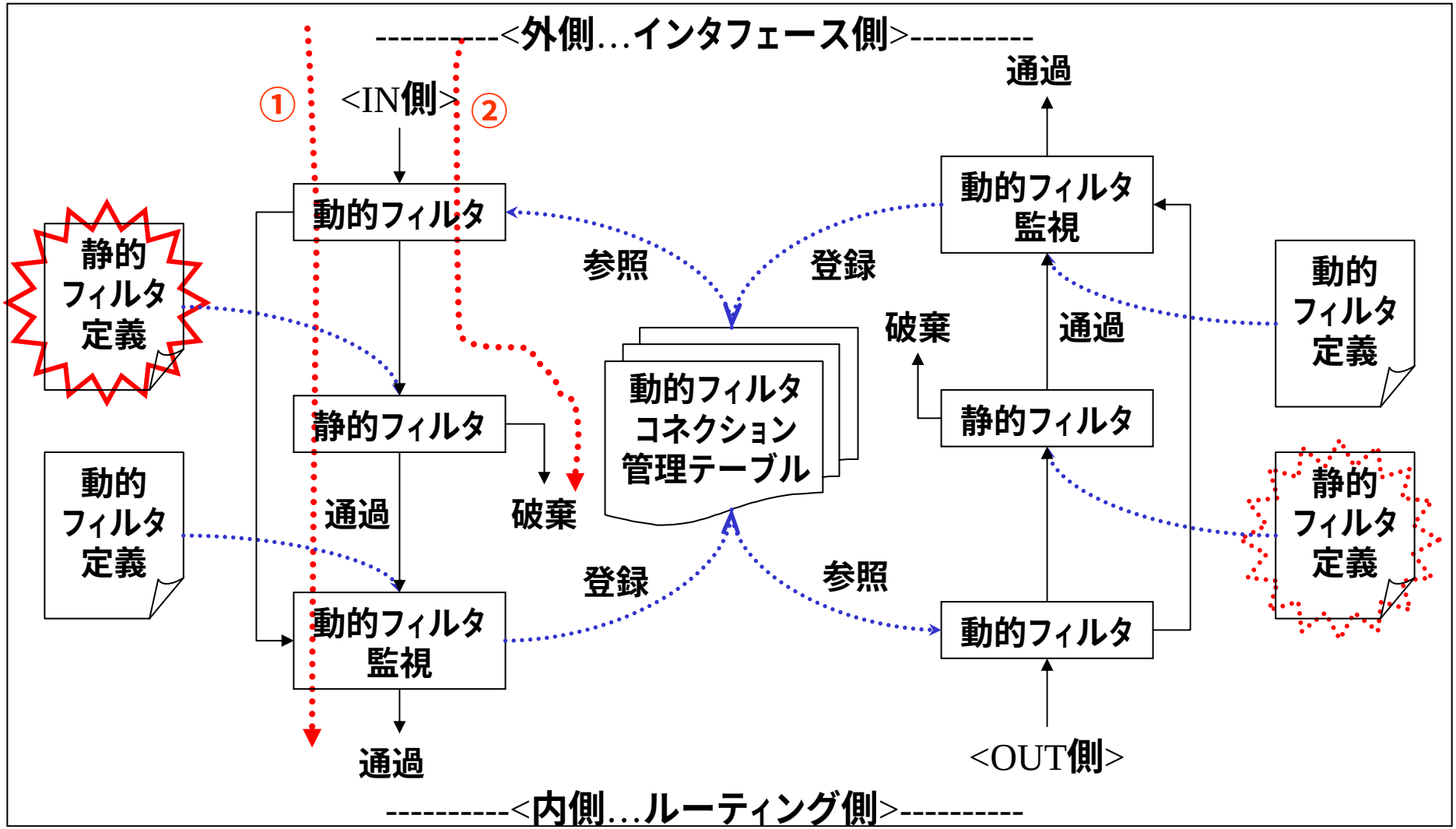
(ネットボランチのセキュリティ強度の選択機能)

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

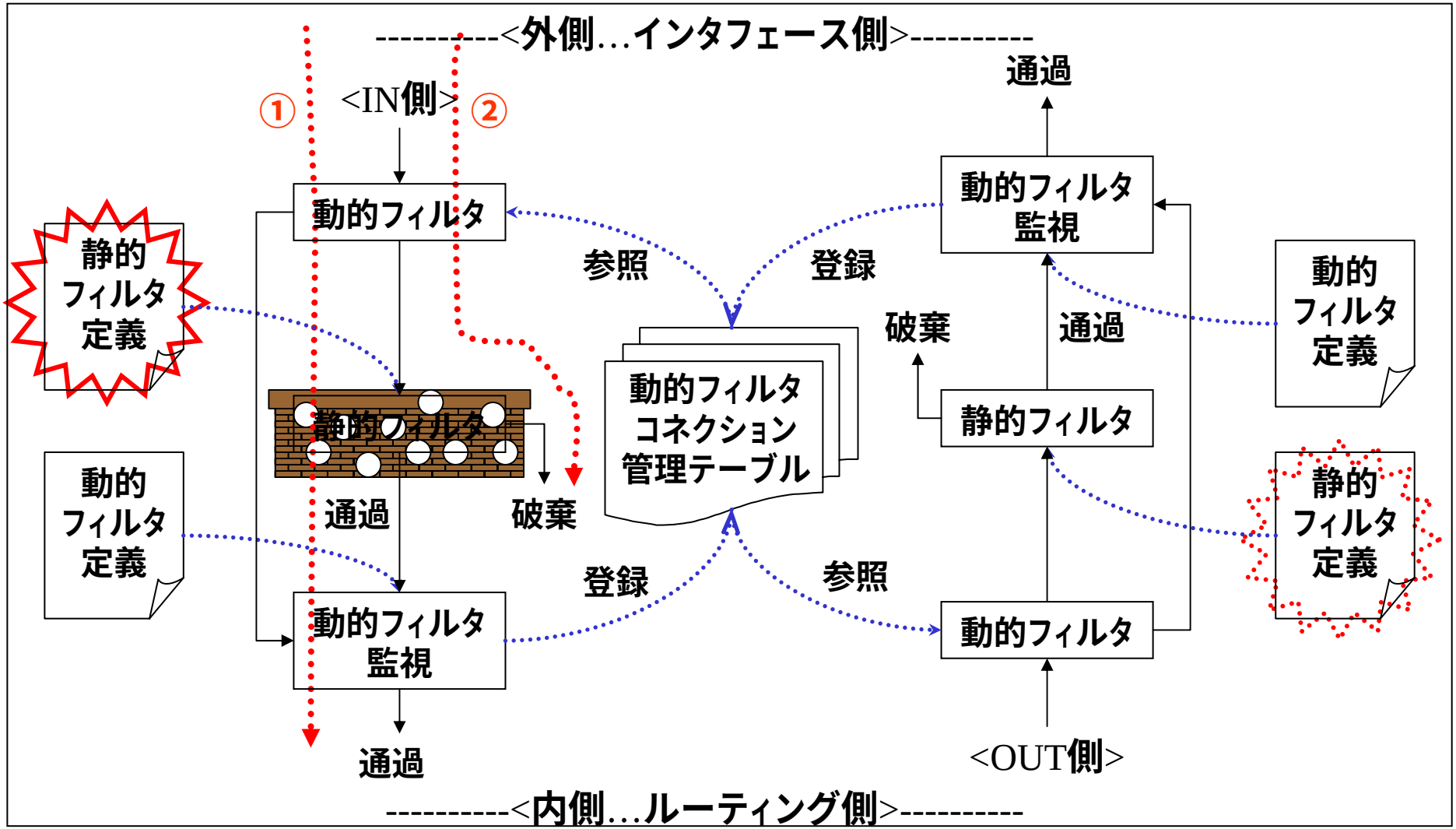
ファイアウォールの構造



一部の通信路を塞ぐ


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

静的セキュリティ・フィルタ



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

設定例#1

(静的セキュリティフィルタ)

[条件]

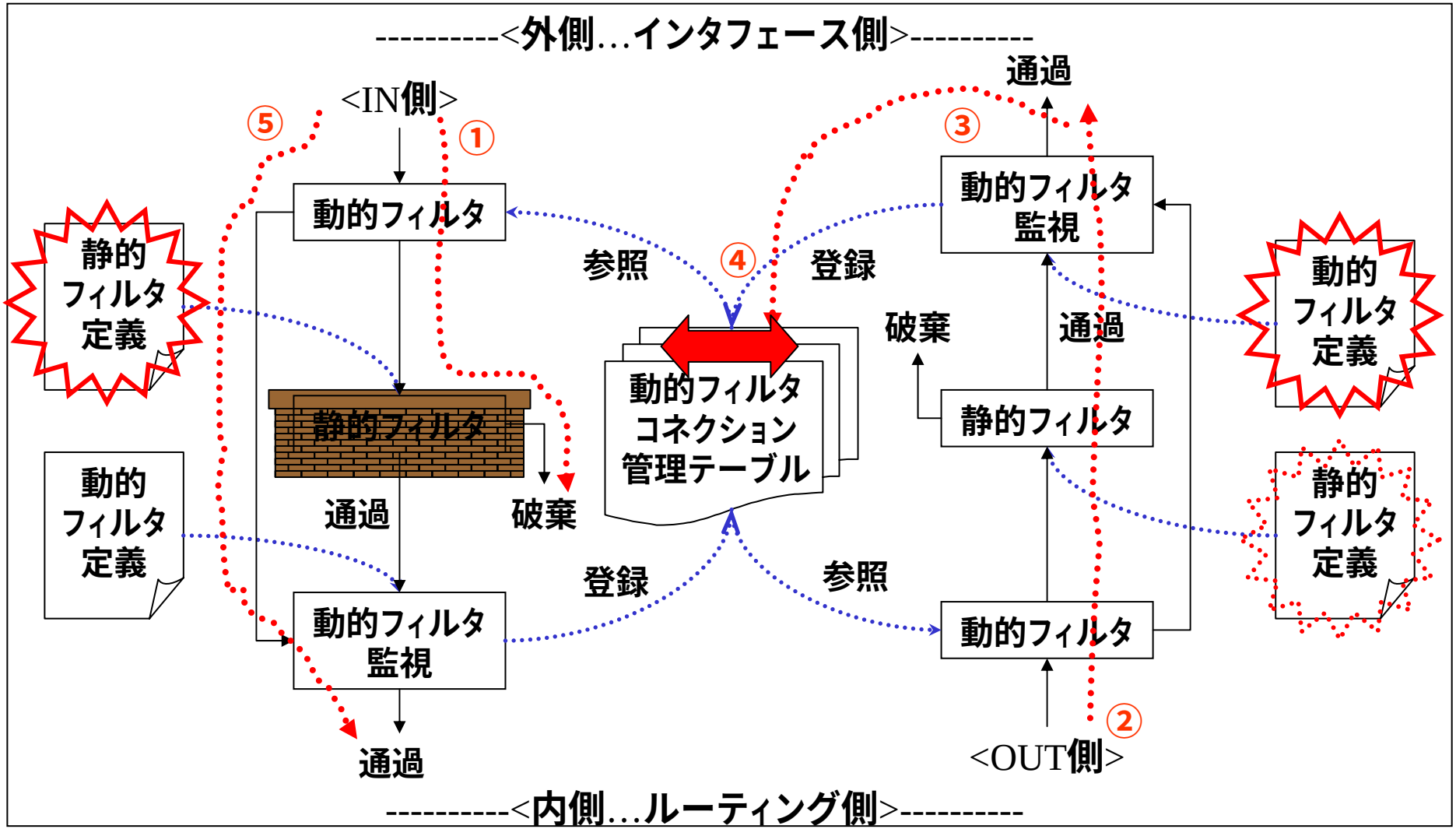
- ネットボランチ RTA54i
- プロバイダ接続設定の
  セキュリティ・レベル5

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

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


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

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
stmp	tcp	電子メール(送信)
pop3	tcp	電子メール(受信)
telnet	tcp	telnet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

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

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	★