

フィルタリングルール最適化問題の解法

神奈川大学理学部情報科学科
田中研究室

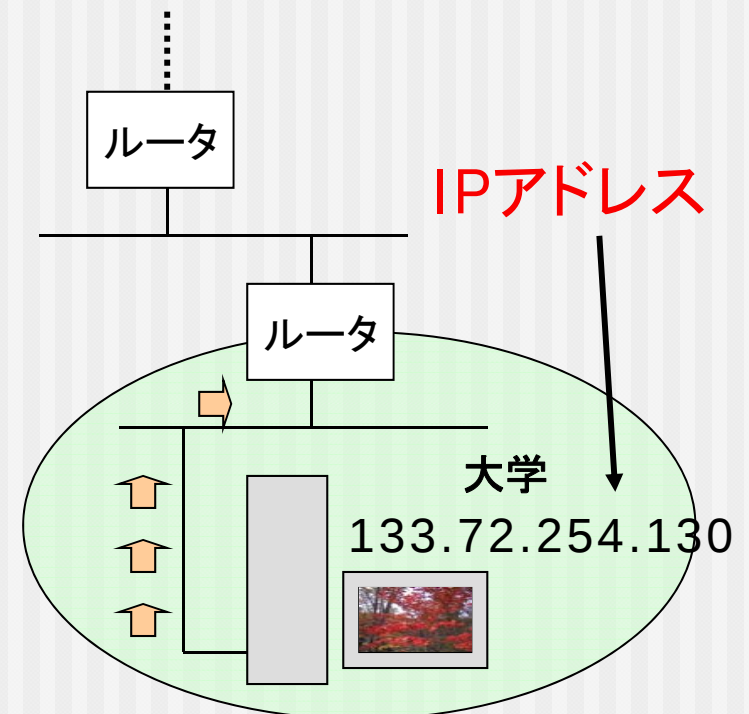
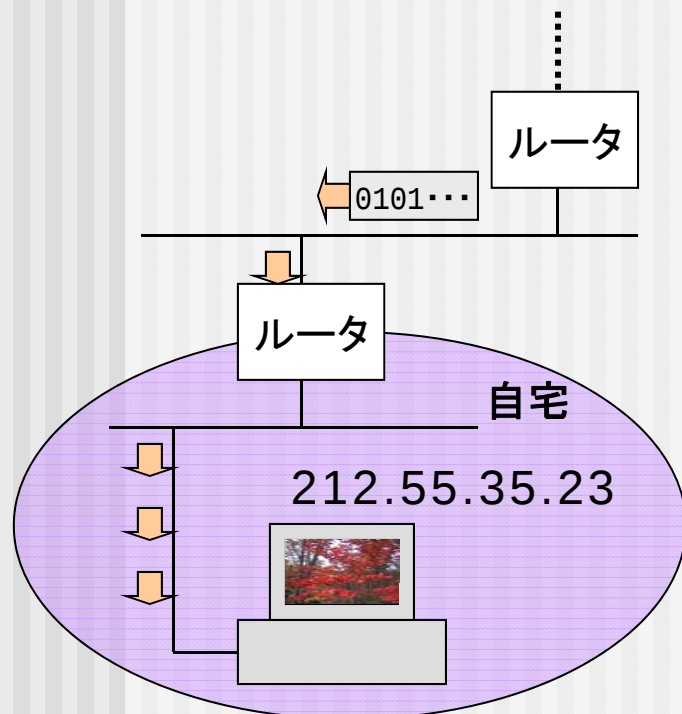
インターネットの仕組み - IPアドレス -

パケット

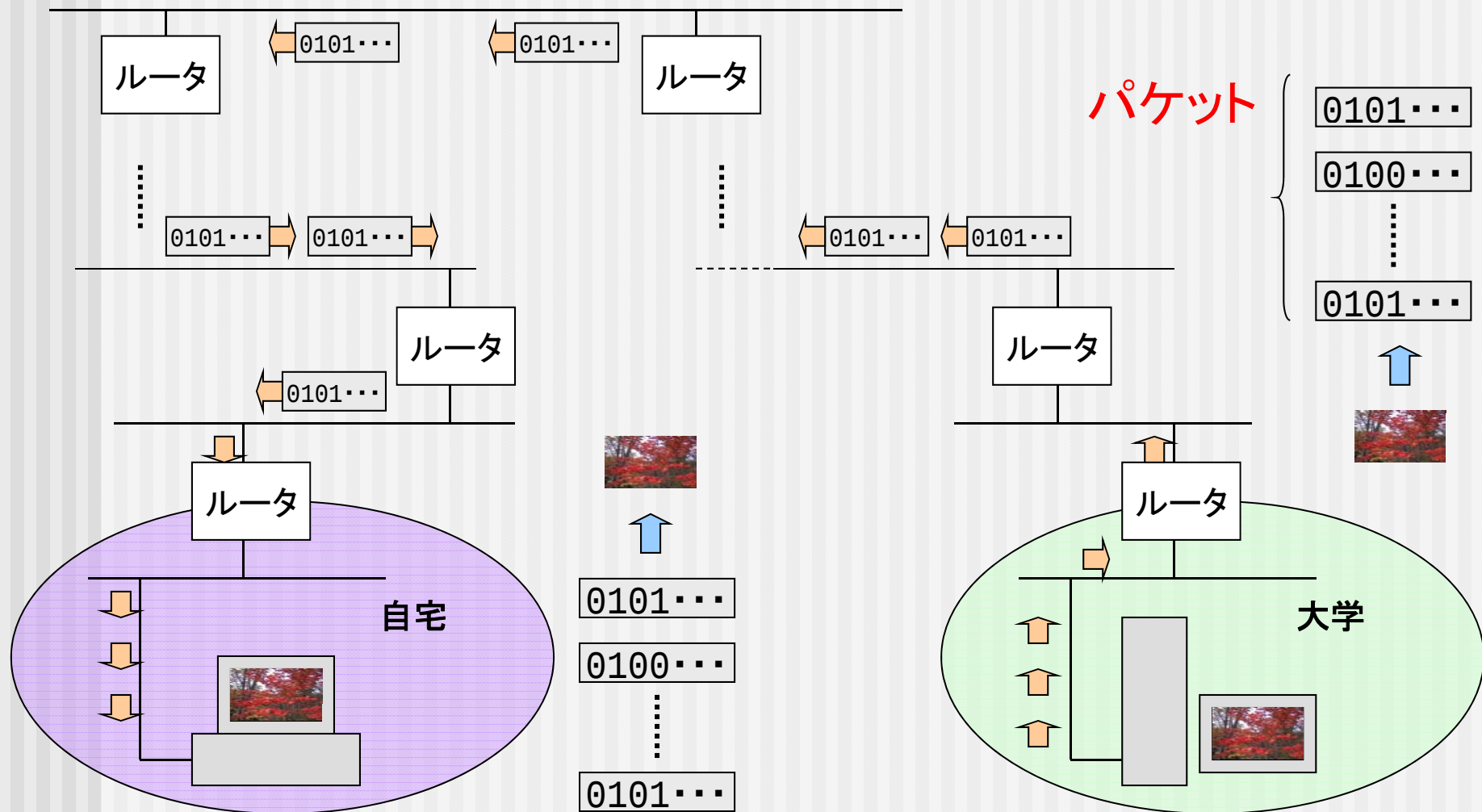
0101...

送り先IPアドレス
発信元IPアドレス
を含む

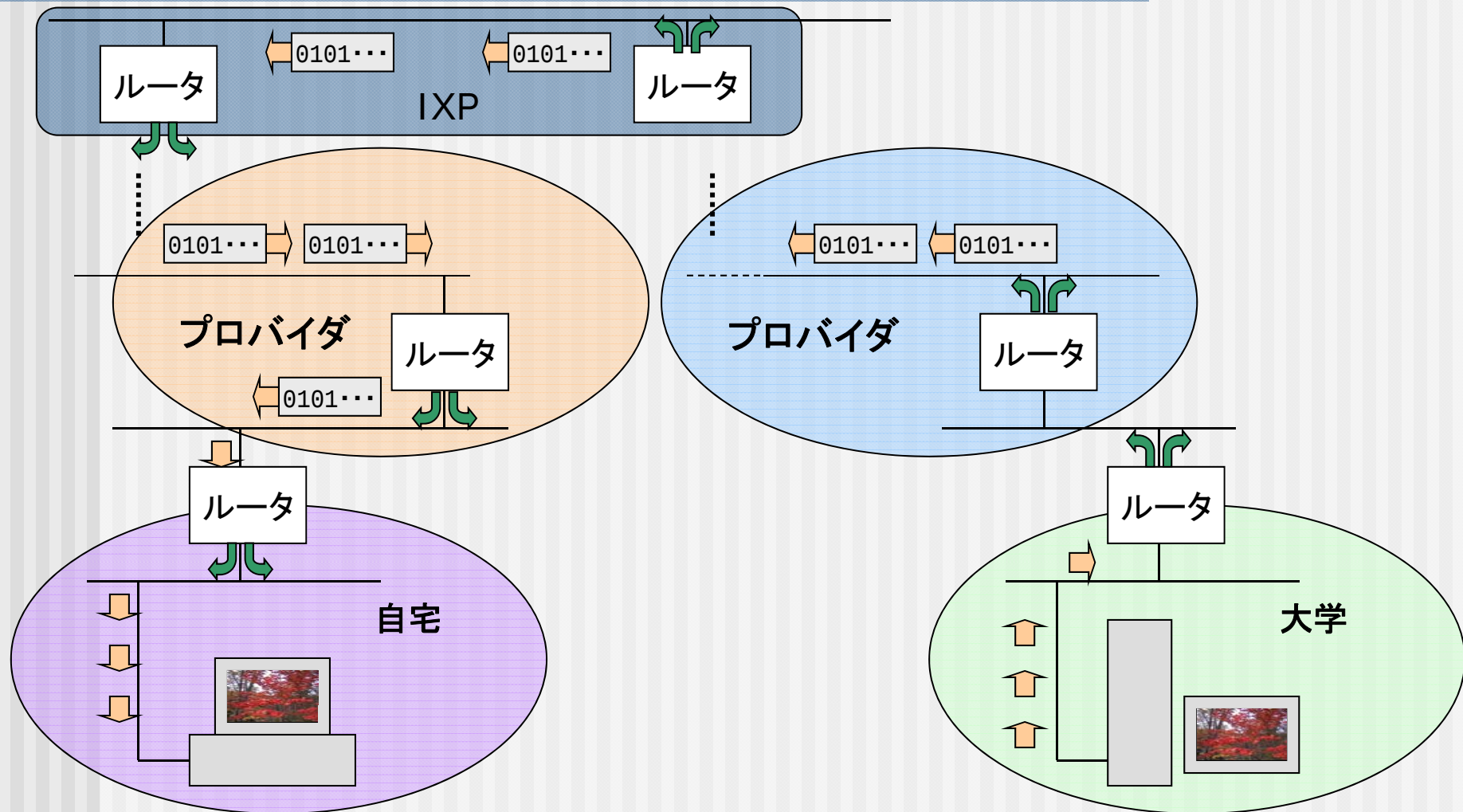
※確実に
相手に届く



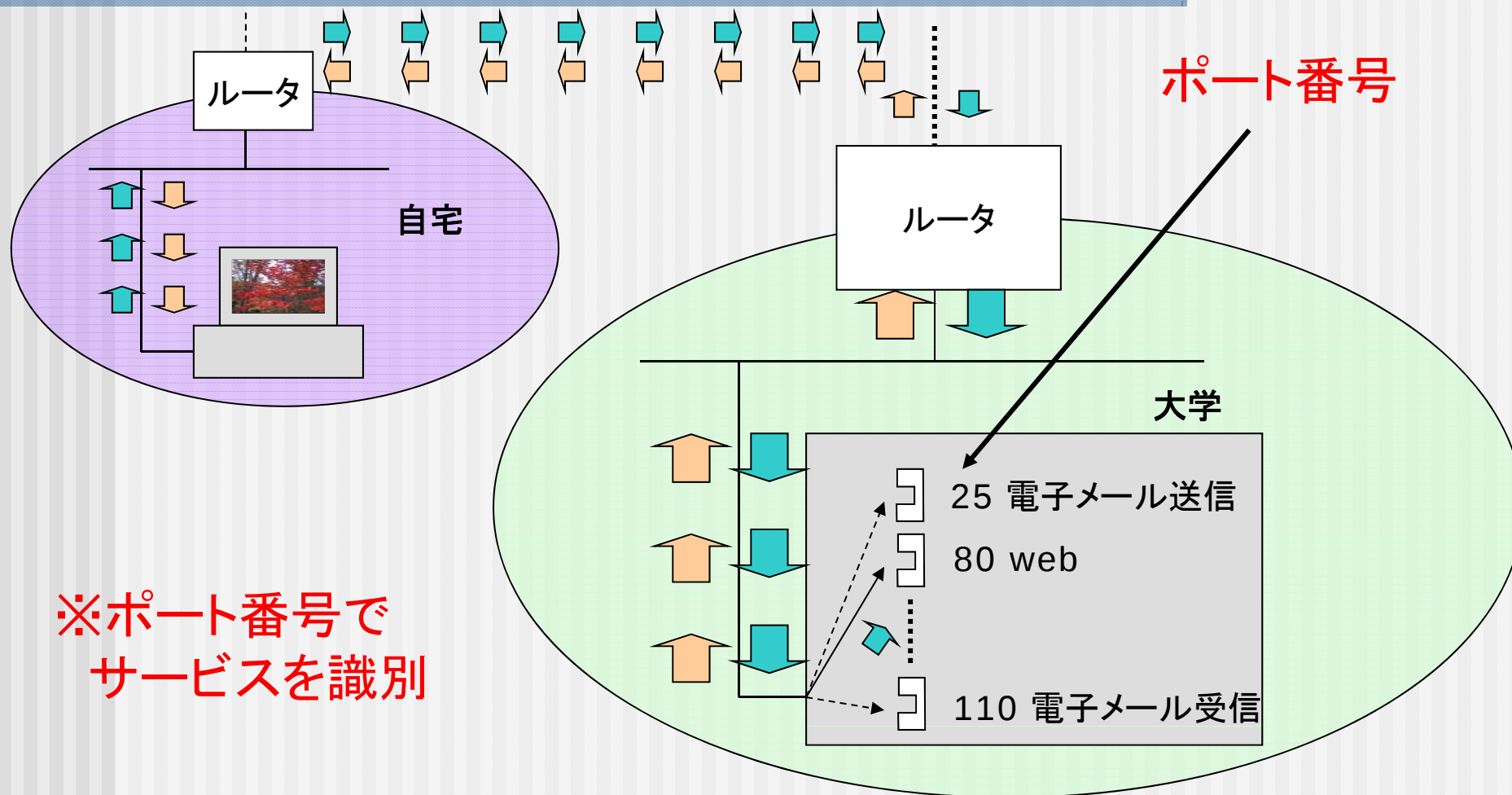
インターネットの仕組み - パケット -



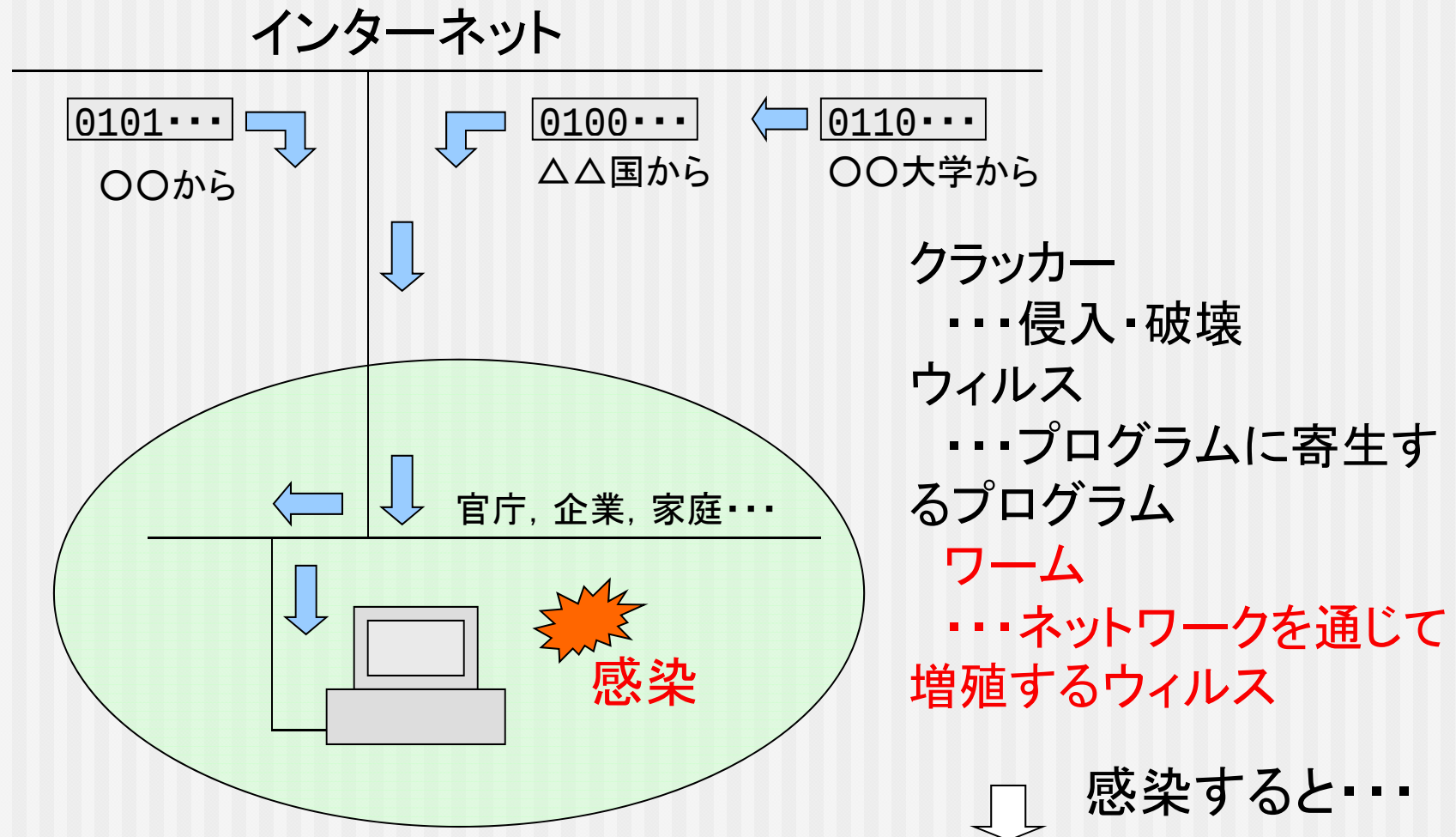
インターネットの仕組み - ルータ -



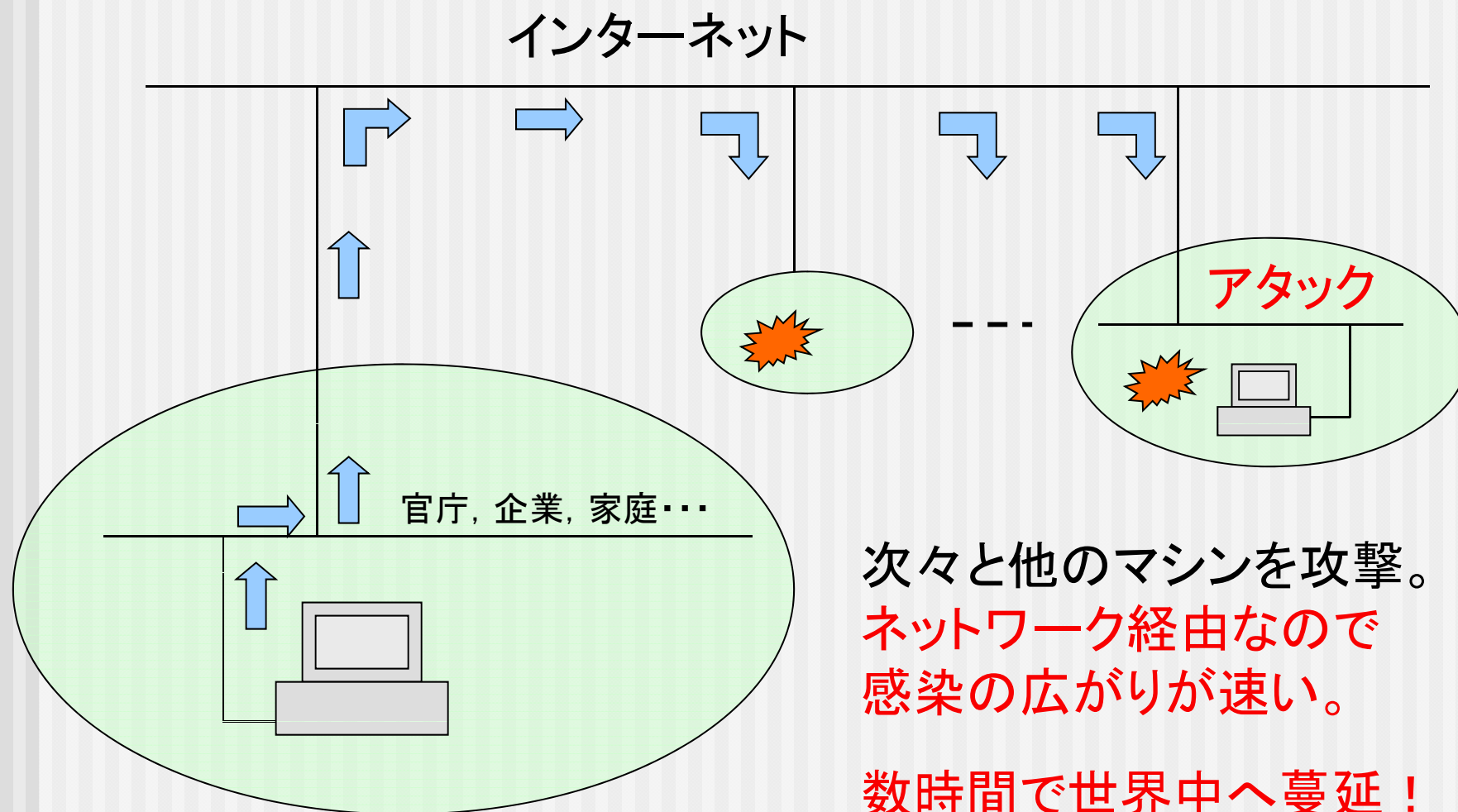
インターネットの仕組み - ポート -



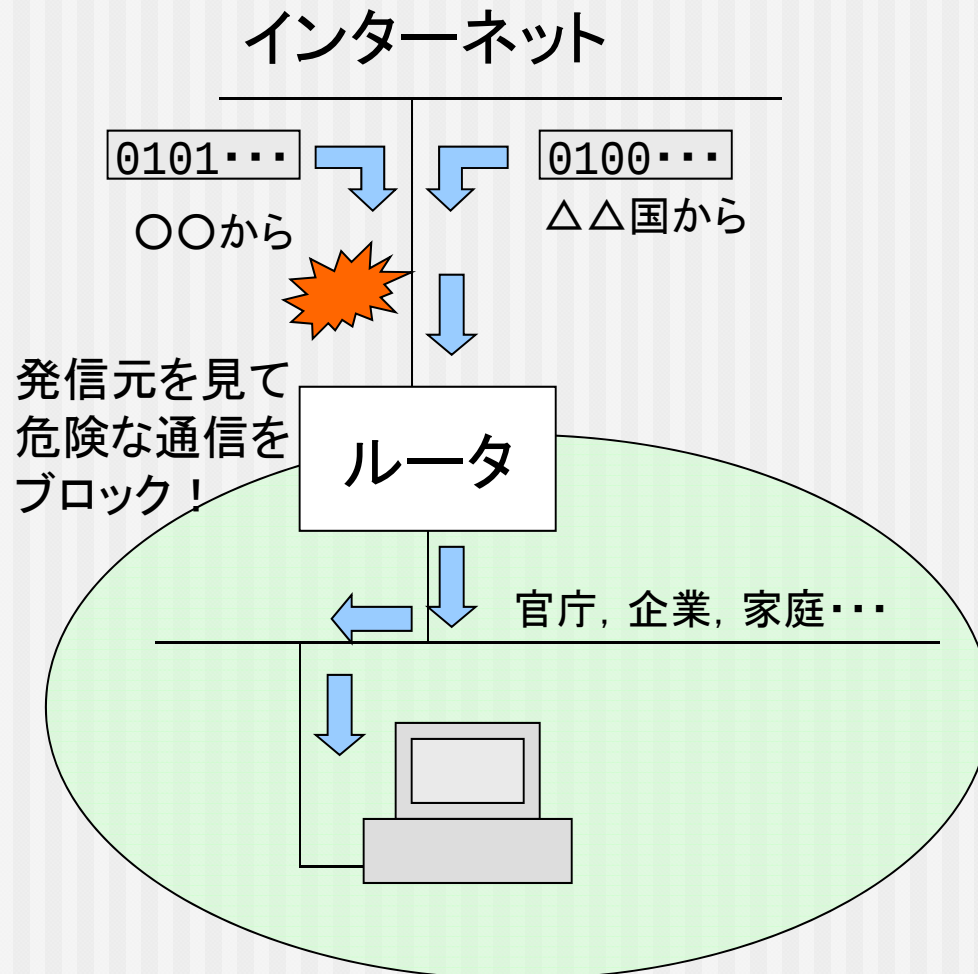
インターネットは危険！



際限ない増殖

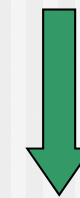


フィルタリングルール最適化問題



ルータ上のフィルタ規則

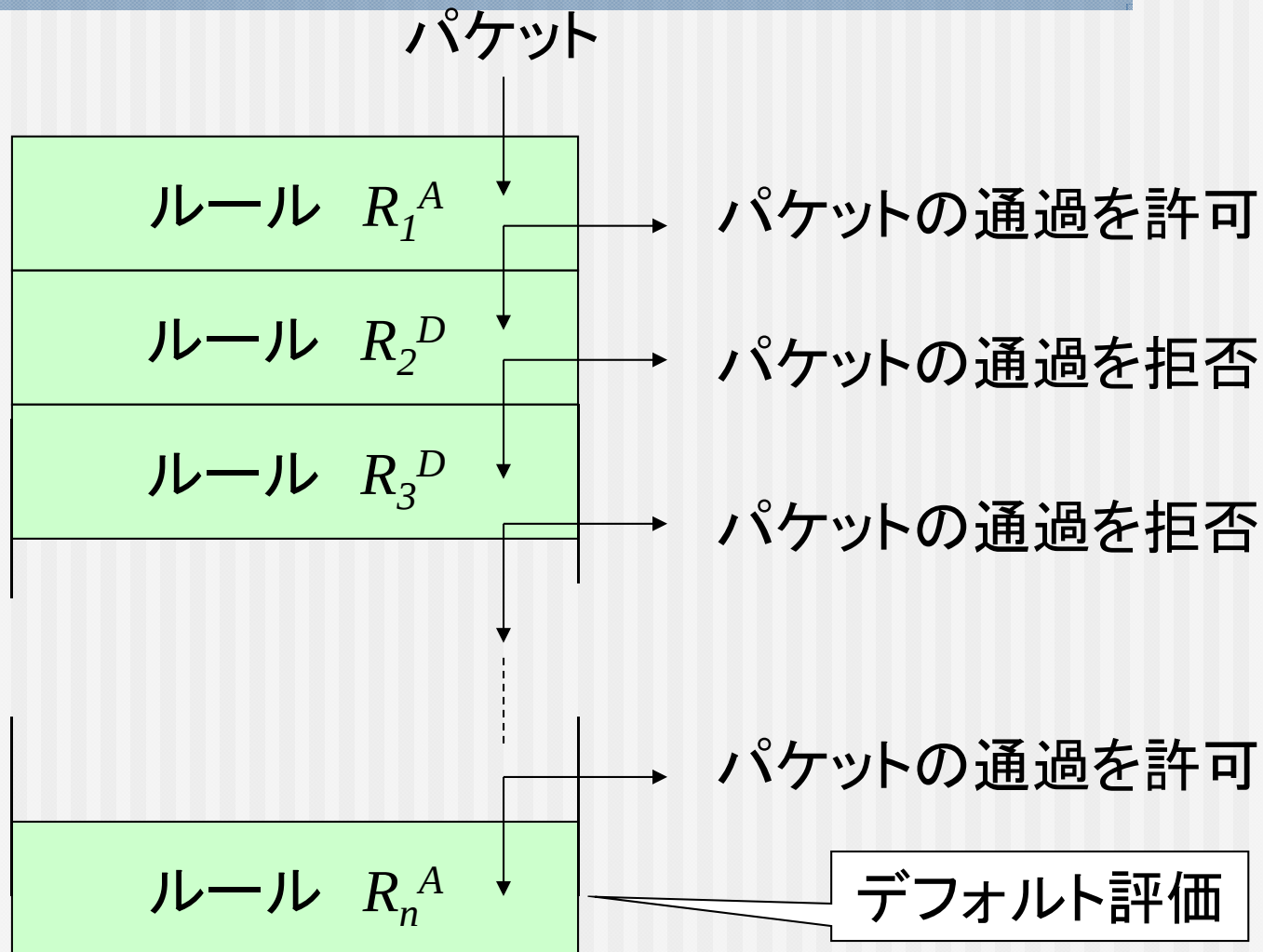
〇〇大学から : 許可
△△会社から : 拒否
◇◇国から : 拒否
....



規則が多いと遅延が発生
回線速度アップでは対応
できない

問題！
遅延を最小にするルール
の書き方は？

パケットフィルタリングのモデル



フィルタリングルールの形式

i番目のルール:

$$R_i^v = \underbrace{b_0 b_1 \cdots b_m}_{\text{ビット列}} \quad (b_i \in \{0, 1, -\} v \in \{A, D\})$$

ビット列:

送信元のIPアドレス
送り先のIPアドレス
ポート番号
プロトコル
...

例)

133.72.259.130
192.218.241.4
80
TCP
...

11000000.11011010.
11110001.00000100

例)

許可

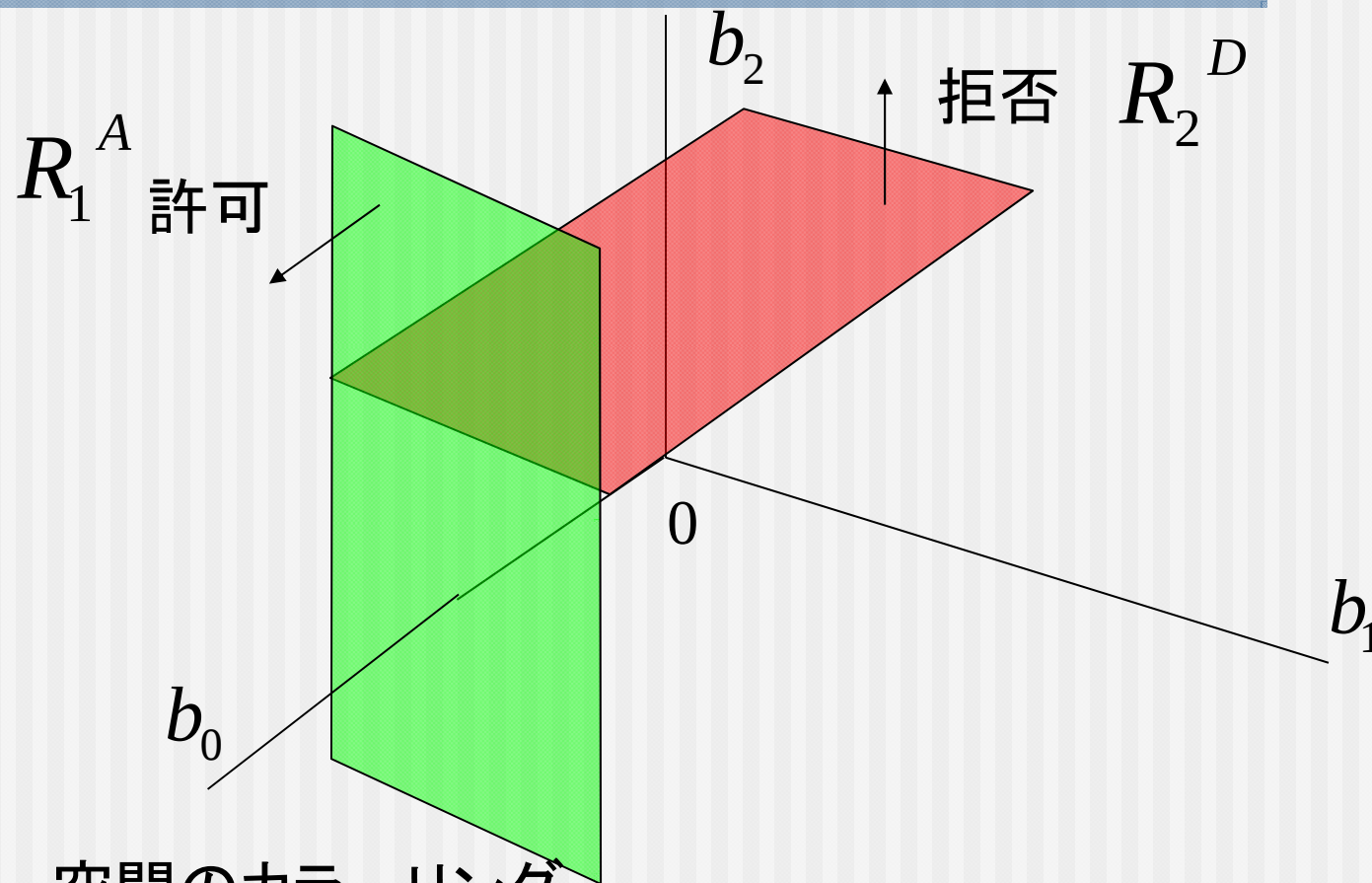
$R_3^A = 1000010110000101-----$

発信元は神奈川大学

1000000110110101111000100000100

送信先は〇〇大学

パケットフィルタリングのイメージ



- ・空間のカラーリング
- ・許可(拒否)の裏側が常に拒否(許可)になるわけではない

ルールの適用の順序

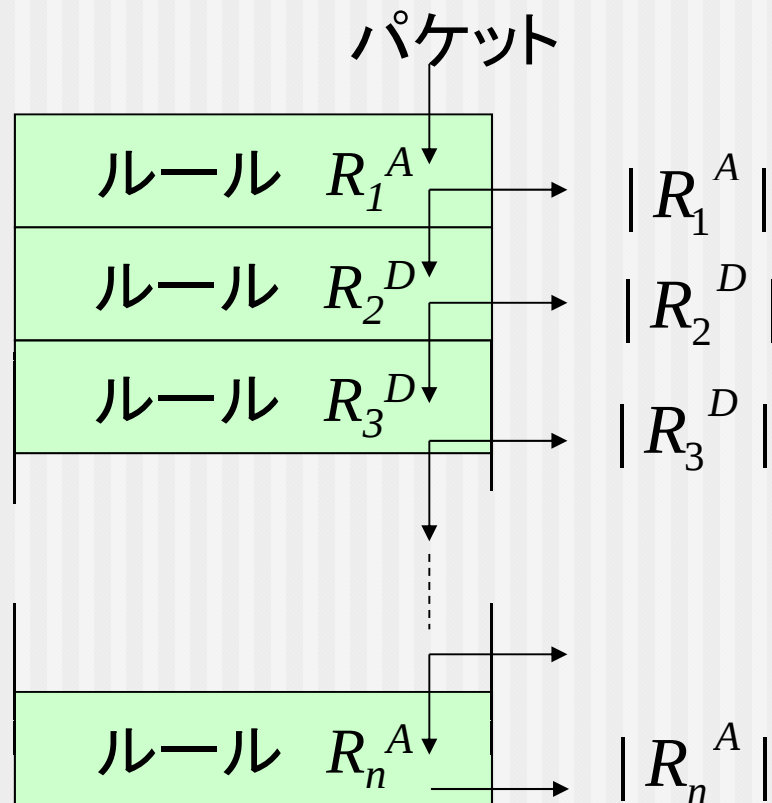
注意:

各々のルールに置いては、直前のルールまでに
評価が決まらなかったパケットのみが評価の対象に



- ・ **順序を考慮**しながらルールを決める必要あり
- ・ 単純な論理式の組み合わせの問題の問題にはならない

評価パケット数

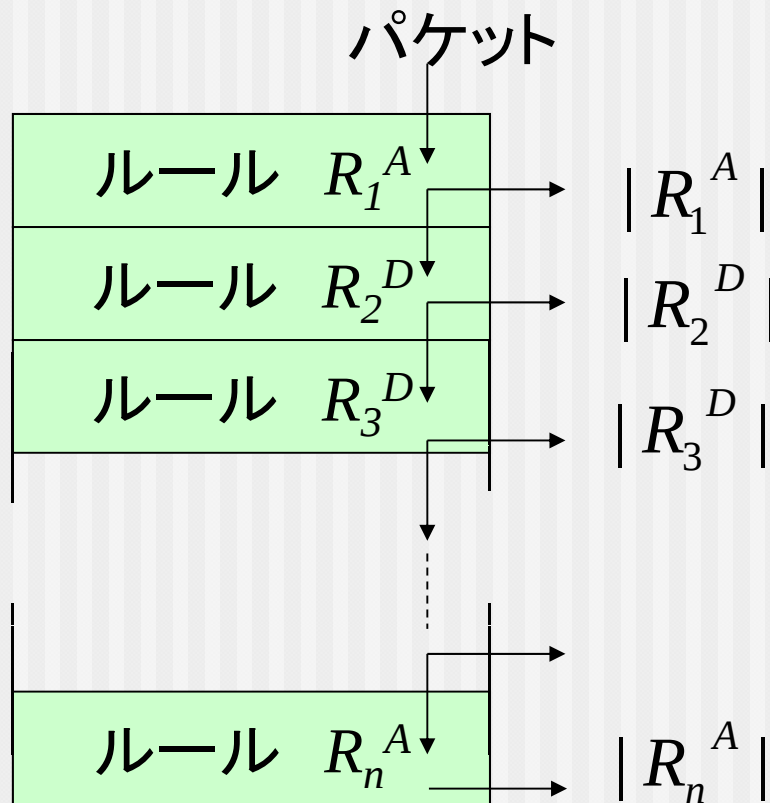


定義(評価パケット数 $|R_i^v|$)
ルール R_i によって評価が
決まるパケット数

$$\text{総パケット数} = \sum_i |R_i^v|$$

$|R_i|$ は到着パケットの
頻度分布によって変化

ネットワーク機器の遅延



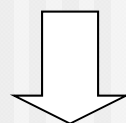
i番目のルールによって
評価が決まるパケットは
i回の評価を受けている



1回の評価を遅延1考え
ネットワーク機器への遅延を
定義

$$L(R) = \sum_i^n i |R_i^v|$$

遅延はルールセットRの
関数である点に注意

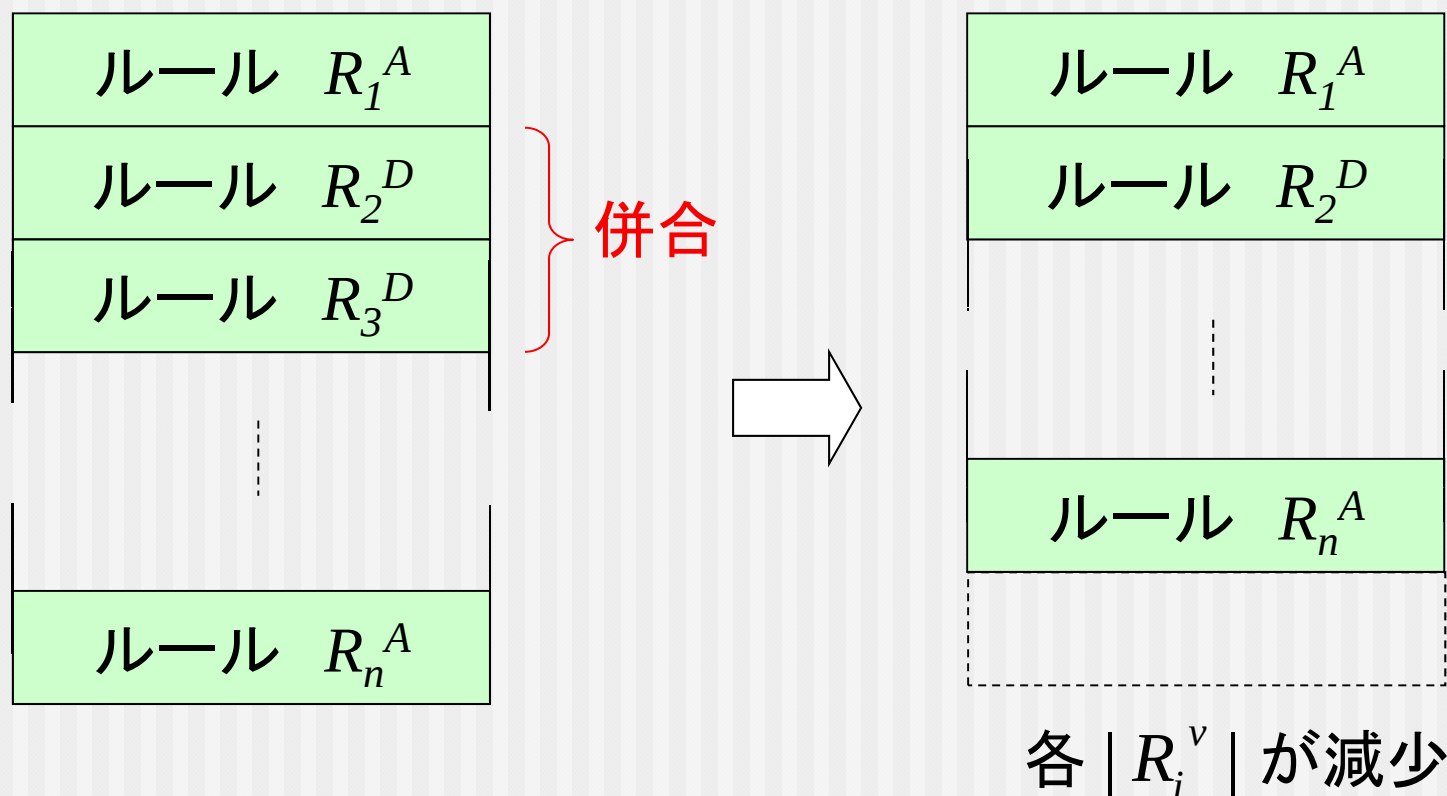


$L(R)$ を最小にするような R を求めよ！

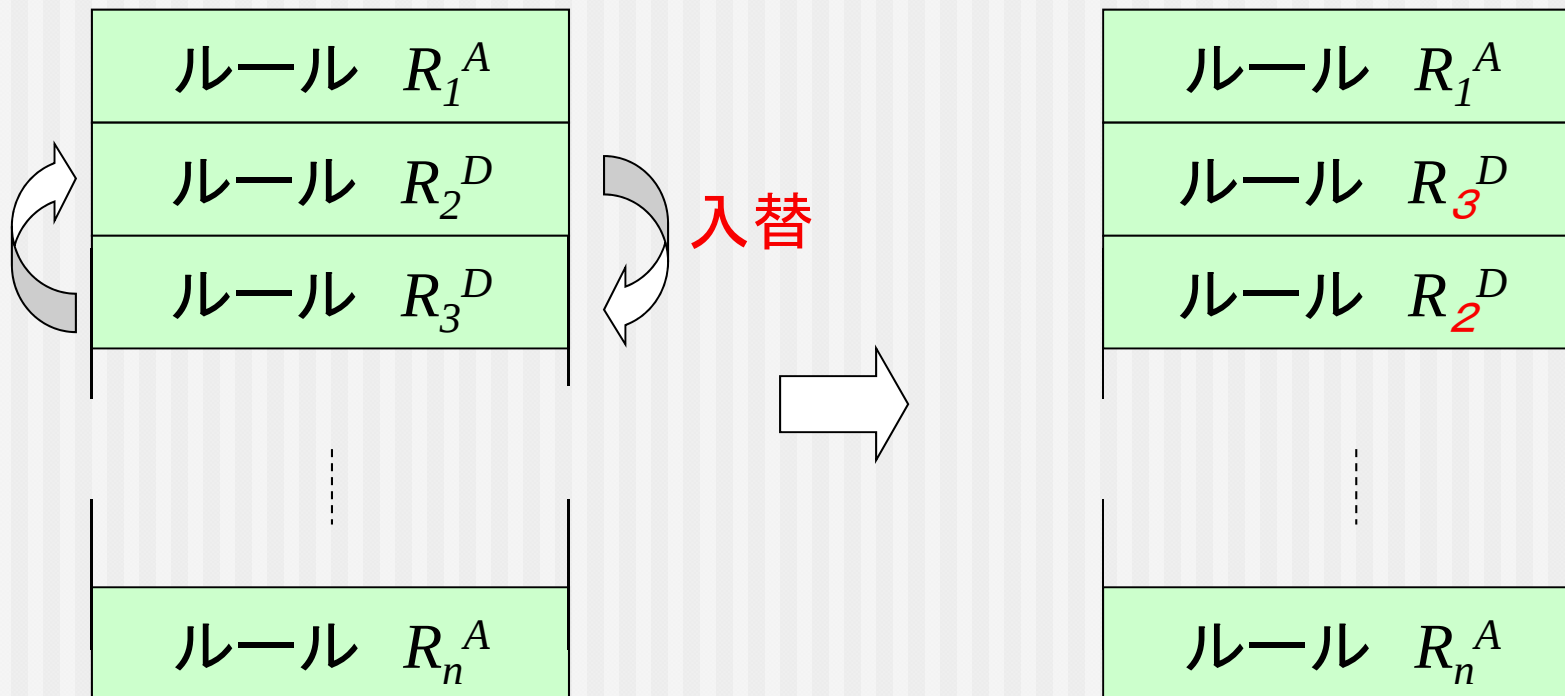
最適フィルタリングルール構成問題

最適化の方針

1) 複数のルールを1つにまとめる(併合)



2) ルールを入れ替える(入替)



上位のルールで評価が決まるパケットが増加し $\sum_i |R_i^v|$ が減少

ルールの併合法

評価が同じで連続するルールを併合

例)

$$\begin{array}{l} R_3^A = 133.72.259.- \\ R_4^A = 133.72.-.- \end{array} \Rightarrow R_3^A = 133.35.-.-$$

論理関数の簡単化の問題に帰着

……カルノー図、クワイン・マクラスキー法など

クワイン・マクラスキー法

論理関数の積和標準形からその最簡形を求める手法

1) 関数の積和標準形を求める

例)

$$\begin{array}{l} R_1^A = 00 - \\ R_2^A = 011 \\ R_3^A = 100 \end{array} \Longrightarrow \left\{ \begin{array}{l} R_1^A = 000 \\ R_2^A = 001 \end{array} \right.$$

個々のビットの積(最小項)として展開

全てのルールについて最小項を求める

2) 最小項を2進数の順に整列

例)

$$R_1^A = 000 \quad \boxed{0}$$

$$R_2^A = 001 \quad \boxed{1}$$

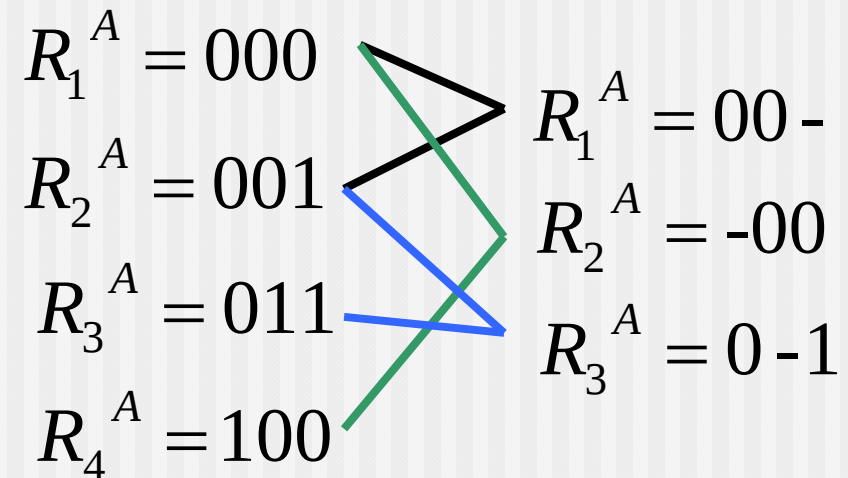
$$R_3^A = 011 \quad \boxed{3}$$

$$R_4^A = 100 \quad \boxed{4}$$

⋮

3) 各項を比較して対応するビットが1ビットだけ異なる
項を選び圧縮

例)



4) 残った項(主項) × 最小項なる表を作成し、
 主項が最小項を含むなら○を記入
 例)

		最小項			
		$R_1^A = 000$	$R_2^A = 001$	$R_3^A = 011$	$R_4^A = 100$
主項	$R_1^A = 00-$	○	○		
	$R_2^A = -00$	○			○
	$R_3^A = 0-1$		○	○	

5) 全ての最小項が少なくとも1つの○を含む
 ような主項の組み合わせを求める

最小項

例)

		$R_1^A = 000$	$R_2^A = 001$	$R_3^A = 011$	$R_4^A = 100$
主項	$R_1^A = 00-$	○	○		
	$R_2^A = -00$	○			○
	$R_3^A = 0-1$		○	○	

1つだけの○を含む最小項に注目

6) 選んだ主項の和が最簡形となる

最小項

例)

	$R_1^A = 000$	$R_2^A = 001$	$R_3^A = 011$	$R_4^A = 100$
$R_1^A = 00 -$	○	○		
$R_2^A = -00$	○			○
$R_3^A = 0-1$		○	○	

主項

の部分は に含まれ、 は を含む

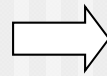
2つの主項で4つの最小項と同等

併合結果

$$R_1^A = 00 -$$

$$R_2^A = 011$$

$$R_3^A = 100$$



$$R_2^A = -00$$

$$R_3^A = 0 - 1$$

$$\begin{aligned} L(R) &= 1 \cdot 2 + 2 \cdot 1 + 3 \cdot 1 \\ &= 7 \end{aligned}$$

$$\begin{aligned} L(R) &= 1 \cdot 2 + 2 \cdot 2 \\ &= 6 \end{aligned}$$

遅延は86%程度に

ルールの入替法

併合の場合・・・評価が同じで連続するルールを併合

入替の場合・・・**評価が異なる連続するルール**をどう扱うか？

例)

$$R_2^A = 001$$

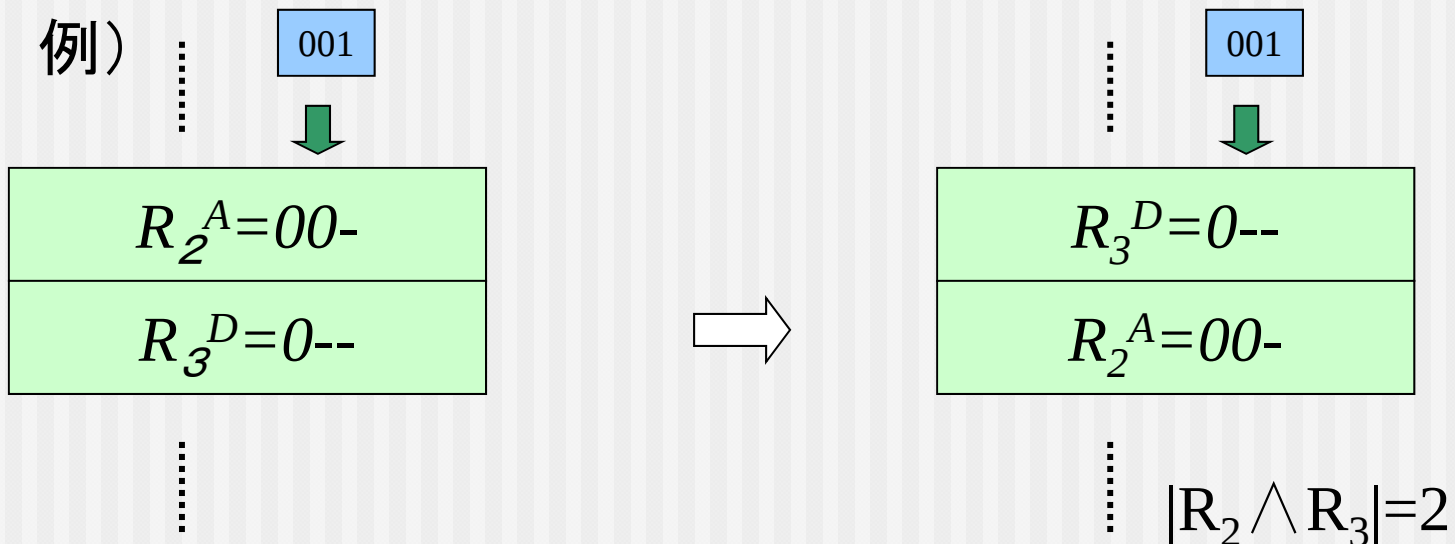
$$R_3^D = 0--$$

$|R_2| < |R_3|$ なので入れ替えたいが、
入れ替えると評価が変わってしまう

どんな場合に入替が可能かつ有効か？

定義: 重複

R_i で評価が決まり、 R_{i+1} を R_i の手前に移動したとき
 R_{i+1} で評価が決まるようなパケットが存在するとき
 R_i 、 R_{i+1} は重複しているといい、重複しているパケット
の数を $|R_i \wedge R_{i+1}|$ で表す。



入替の条件

命題1:

評価が等しい連続する2つのルール R_i 、 R_{i+1} を入れ替えて
 $L(R)$ が減少するための必要十分条件は、

$|R_i| < |R_{i+1}| + |R_i \wedge R_{i+1}|$
である。

命題2:

評価が異なる連続する2つのルール R_i 、 R_{i+1} を入れ替えて
 $L(R)$ が減少するための必要十分条件は、

$|R_i \wedge R_{i+1}| = 0$ かつ $|R_i| < |R_{i+1}|$
である。

最適化手順

併合と入替を交互に適用してL(R)を減少

重複がないか、
評価型が同じ
なら入替可能

- 1, 評価の等しいフィルタリングルールが連続するようルールを**入替**。
- 2, クワイン・マクラスキー法によりルールを**併合**。
- 3, 1, 2, を繰り返し、ルール数を最小にする。
- 4, 上位のルールの評価パケット数が多くなるようルールを**入替**。

最適化の例

着目 $R_1^A = 0001$

$$R_2^D = 11-0$$

$$R_3^A = 0000$$

重複がないので入替

$$R_4^A = 11--$$

$$R_5^D = 10-1$$

$$R_6^D = 10-0$$

$$R_7^A = 1---$$

$$R_8^A = 1-1-$$

$$R_9^D = ----$$

$$L(R) = 92$$

最適化の例

着目 $R_3^A = 0000$

$R_1^A = 0001$

$R_2^D = 11-0$

$R_4^A = 11--$

重複し評価が異なるので入替せず

$R_5^D = 10-1$

$R_6^D = 10-0$

$R_7^A = 1---$

$R_8^A = 1-1-$

$R_9^D = ----$

$L(R) = 92$

最適化の例

着目 $R_3^A = 0000$

$R_1^A = 0001$

$R_2^D = 11-0$

$R_4^A = 11--$

$R_5^D = 10-1$

$R_6^D = 10-0$

$R_7^A = 1---$

$R_8^A = 1-1-$

$R_9^D = ----$

$L(R) = 92$

重複するので入替せず

最適化の例

着目 $R_3^A = 0000$

$R_1^A = 0001$

$R_2^D = 11-0$

$R_4^A = 11--$

$R_5^D = 10-1$

$R_6^D = 10-0$

$R_7^A = 1---$

$R_8^A = 1-1-$

$R_9^D = ----$

$L(R) = 92$

重複するので入替せず



最適化の例

着目

$$R_3^A = 0000$$

$$R_1^A = 0001$$

併合してリナンバ

$$R_2^D = 11-0$$

$$R_4^A = 11--$$

$$R_5^D = 10-1$$

$$R_6^D = 10-0$$

$$R_7^A = 1---$$

$$R_8^A = 1-1-$$

$$R_9^D = ----$$

$$L(R) = 92$$

最適化の例

$$R_1^A = 000 -$$

$$R_2^D = 11 - 0$$

$$R_3^A = 11 - -$$

$$R_4^D = 10 - 1$$

$$R_5^D = 10 - 0$$

$$R_6^A = 1 - - -$$

$$R_7^A = 1 - 1 -$$

$$R_8^D = - - - -$$

$$L(R) = 73$$

最適化の例

$$R_1^A = 000-$$

$$R_2^D = 11-0$$

$$R_3^A = 11--$$

$$R_4^D = 10-1$$

$$R_5^D = 10-0$$

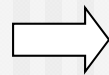
$$R_6^A = 1---$$

$$R_7^A = 1-1-$$

$$R_8^D = ----$$

$$L(R) = 73$$

上位のルールから
順に繰り返す



$$R_1^A = 000-$$

$$R_2^D = 10--$$

$$R_3^D = 11-0$$

$$R_4^A = 1---$$

$$R_5^D = ----$$

$$L(R) = 54$$

最適化の例

$$R_1^A = 000- \quad |R_1^A| = 2$$

$$R_2^D = 10-- \quad |R_2^D| = 4$$

$$R_3^D = 11-0 \quad |R_3^D| = 2$$

$$R_4^A = 1--- \quad |R_4^A| = 2$$

$$R_5^D = ---- \quad |R_5^D| = 6$$

$$L(R) = 54$$

最適化の例

$$R_1^A = 000- \quad |R_1^A| = 2$$

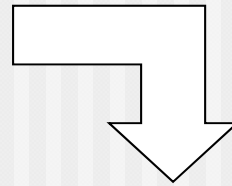
$$R_2^D = 10-- \quad |R_2^D| = 4$$

$$R_3^D = 11-0 \quad |R_3^D| = 2$$

$$R_4^A = 1--- \quad |R_4^A| = 2$$

$$R_5^D = ---- \quad |R_5^D| = 6$$

$$L(R) = 54$$



$|R_1^A \wedge R_2^D| = 0$ (重複なし)
かつ $|R_1^A| < |R_2^D|$ より入替

最適化の例

$$R_1^D = 10-- \quad |R_1^D| = 4$$

$$R_2^A = 000- \quad |R_2^A| = 2$$

$$R_3^D = 11-0 \quad |R_3^D| = 2$$

$$R_4^A = 1--- \quad |R_4^A| = 2$$

$$R_5^D = ---- \quad |R_5^D| = 6$$

$$L(R) = 52$$

その他のルールは入替の
条件を満たさないため終了

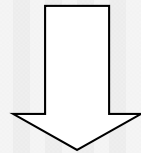
応用の可能性

- 論理式のリストによってフィルタリングする問題全般に適用可能

例) ブリッジ、スイッチの効率化

SPAMメールの選別

パターン分類



通信速度と安全性の両立に貢献

今後の展望

- ・クワイン・マクラスキー法は計算量的に膨大。
ルールが複雑になったときにどう対応するか？
- ・頻度の変化にどう対応するか？
頻度を観測して動的にルールを変更（適応型）