P2Pトラフィックコントロール手法

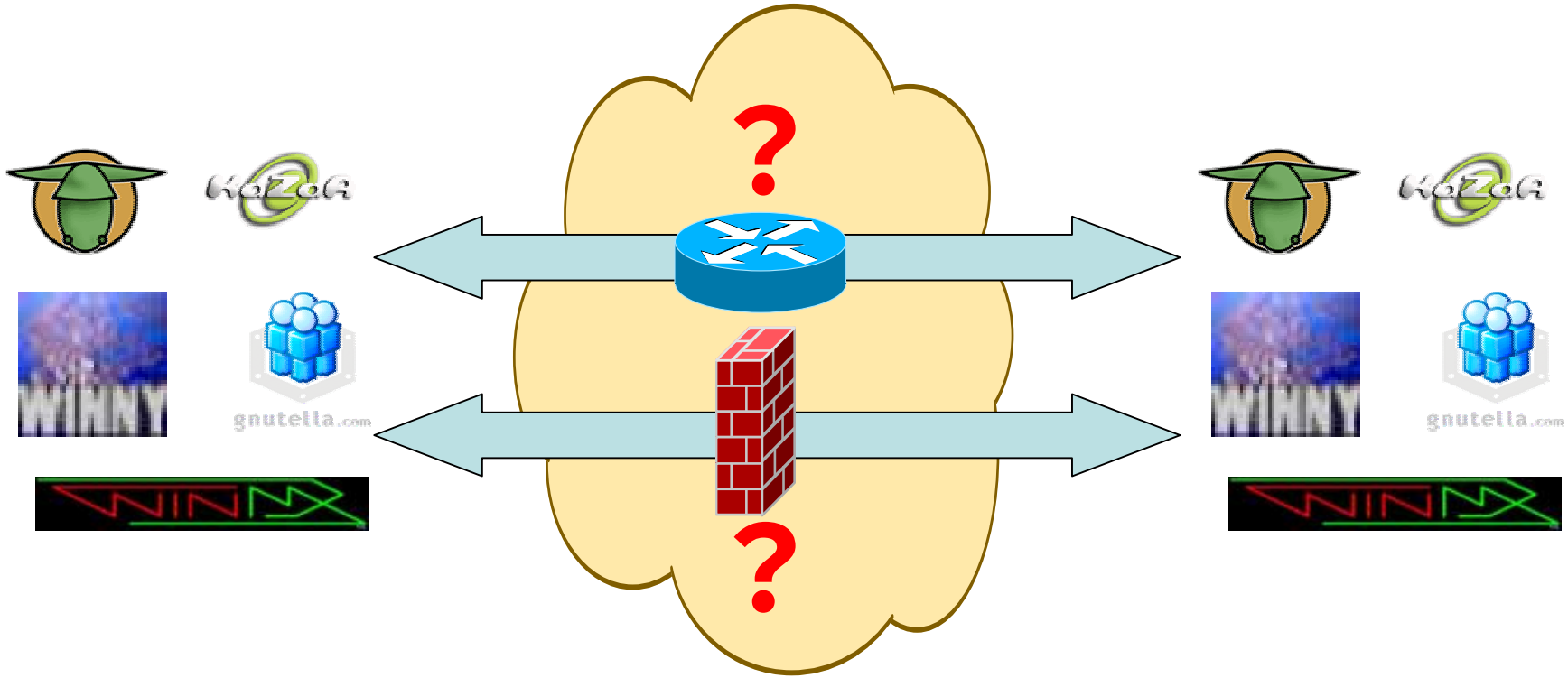
2004年1月30日

㈱ ネットワークバリューコンポネンツ
SEグループ　田山　信行

NETWORK VALUE COMPONENTS

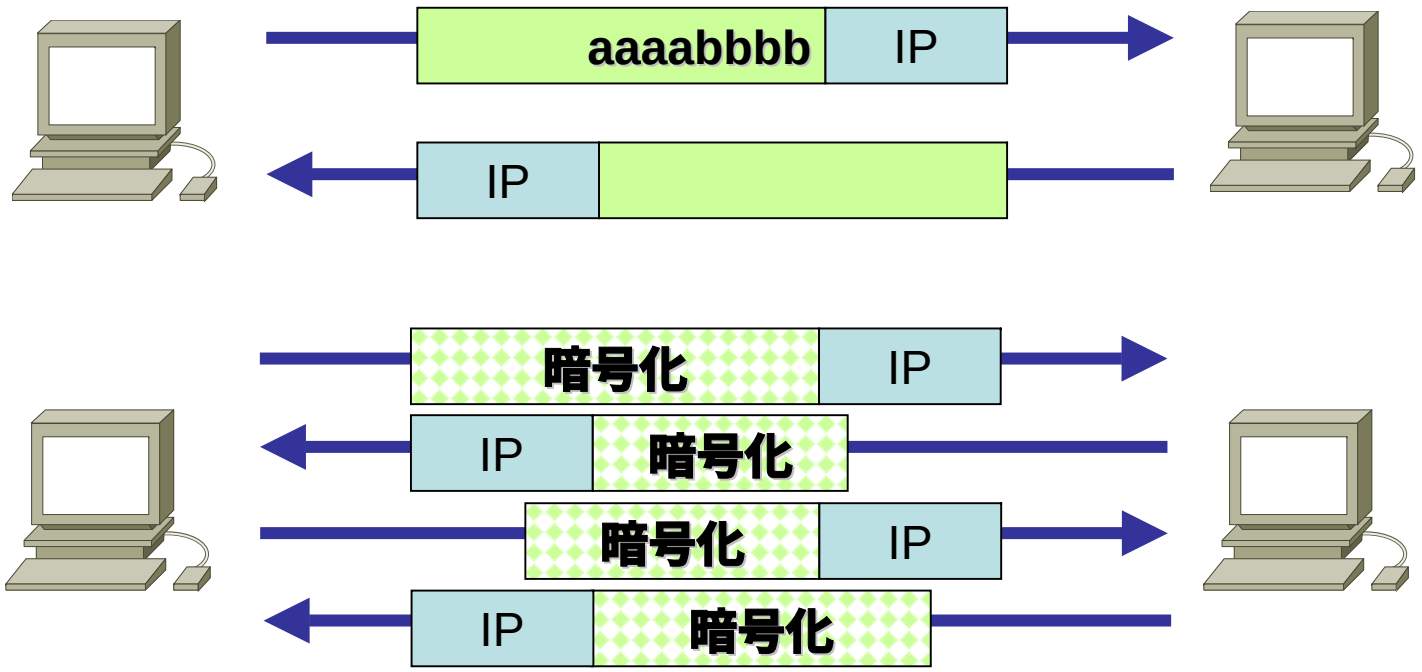
P2Pトラフィック

- Port Hopping
  - Peer間でPort番号を任意に変更して通信を行う
- 暗号化通信
- Router/Firewallでは検知できない



P2Pトラフィックの特徴

- **特定のデータパターン**
  - コントロールパケットに特定文字列 (HEX) が含まれる
- **特定のトラフィックパターン**
  - コントロールトラフィックが特定のトラフィックパターンを持っている

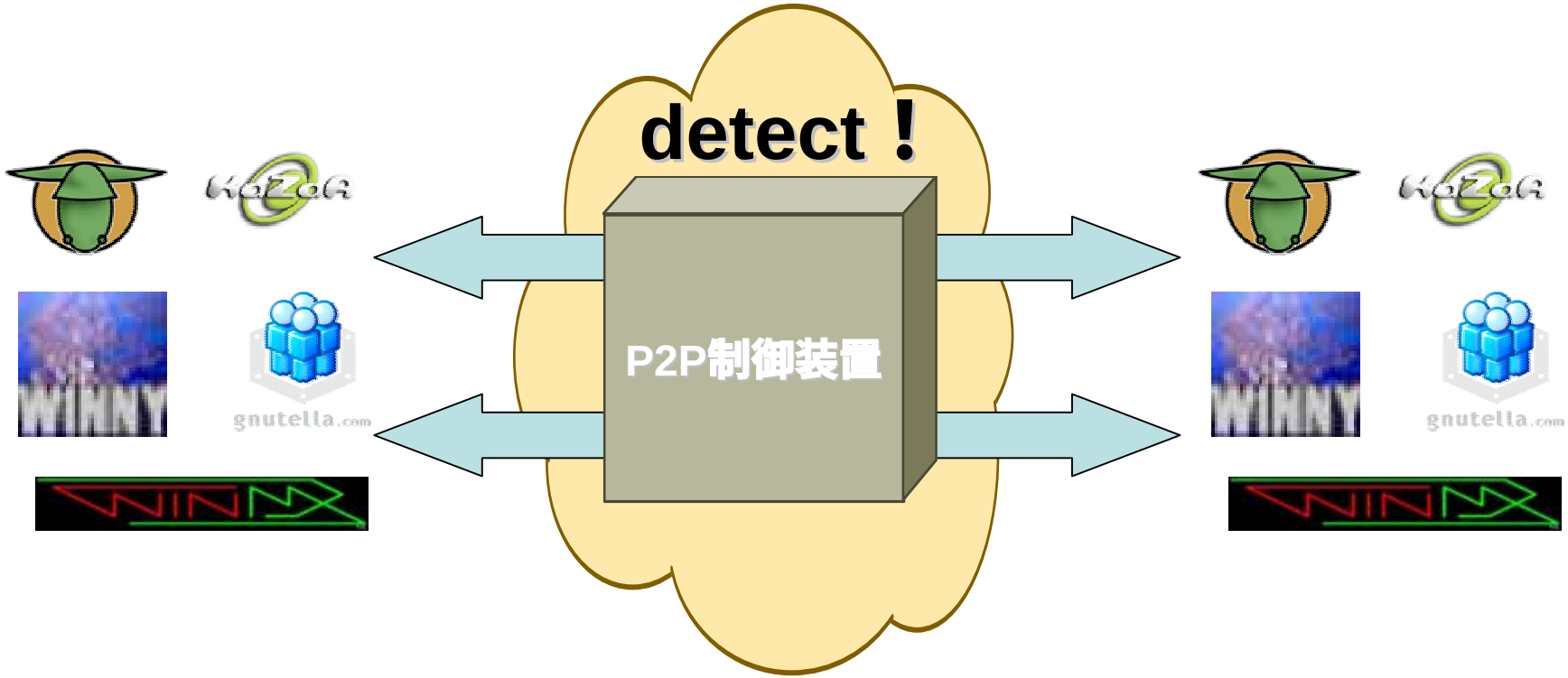


P2Pトラフィック検知方法

- Signature Pattern matching
  - ペイロード部分までLookupして、特定データパターンとマッチング
- Traffic Pattern matching
  - 特定のPacket長での連続したやり取りをLookupして、トラフィックパターンをマッチング
- Proving
  - Endユーザに対して、P2P lookupをかける

P2Pトラフィック制御装置

- P2Pトラフィック制御装置により、P2Pを検知して制御を行う

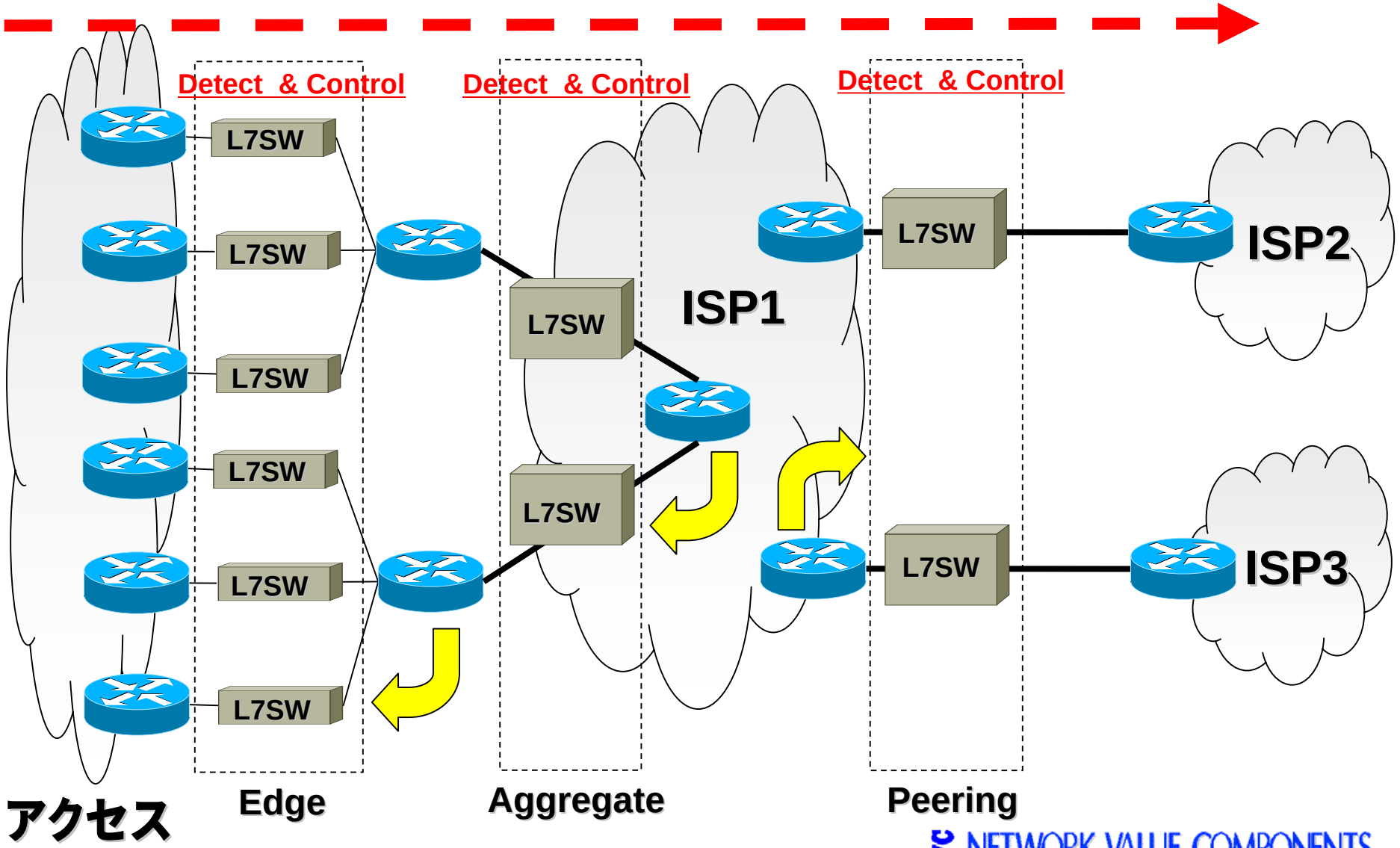


インライン型P2P検知装置

- **L7SW**
  - H/W
  - **ベンダ**
    - Ellacoya、P-Cube、Allot、・・・・
  - **インライン型**
    - **トラフィックを検知**
      - Signature Pattern matching
      - Traffic Pattern matching
    - **制御**
      - Rate-Limit
  - Performance
    - H/W Capacity
    - **～2004年**：1Gbps
    - 2004**年末～**：10Gbps

NETWORK VALUE COMPONENTS

L7SW



NETWORK VALUE COMPONENTS

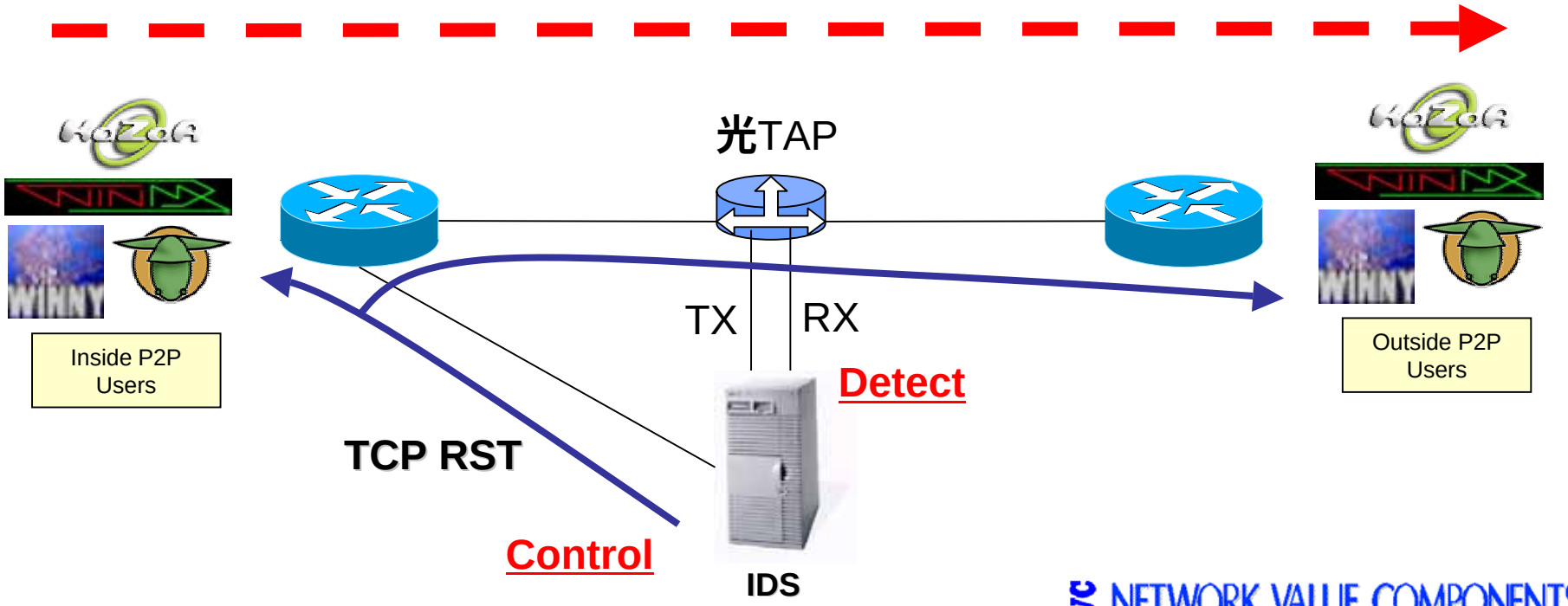
アウトライン型P2P検知装置

- IDS
  - アプライアンス
  - ベンダ
    - ARA Networks、・・・・
  - アウトライン型
    - トラフィック検知
      - Signature Pattern matching
      - Traffic Pattern matching
      - Proving
    - 制御
      - TCP RST
  - Performance
    - CPU capacity
    - 2004年～：over 1Gbps

NETWORK VALUE COMPONENTS

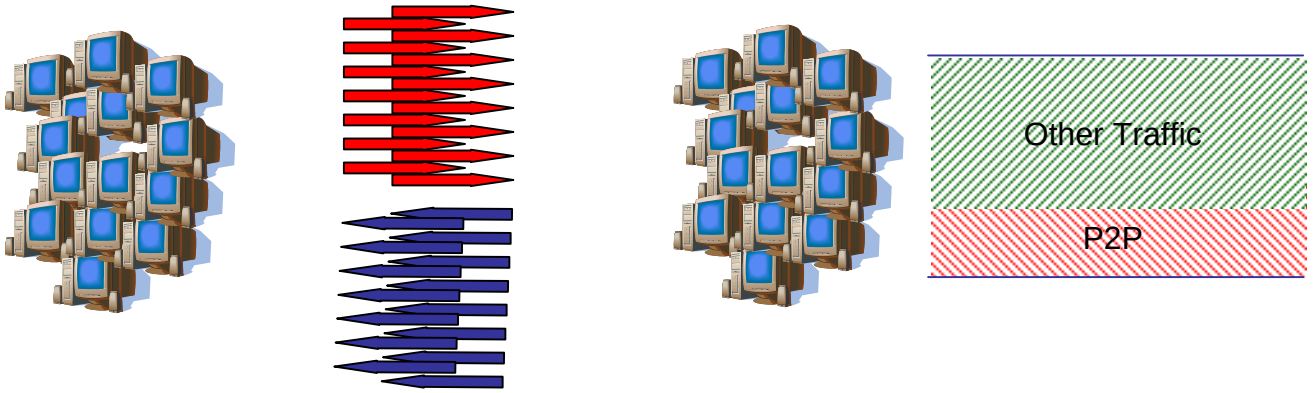
IDS

- **Detect**
  - **光**TAP**より**Monitor
- **Control**
  - **バックドアより**TCP RST

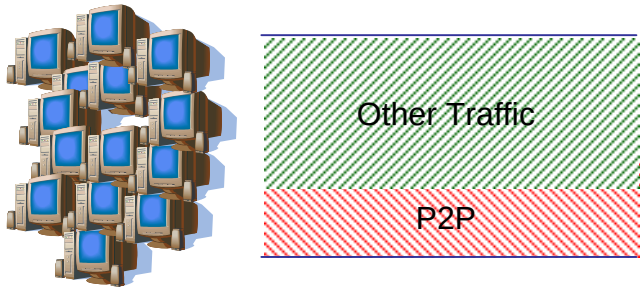


L7SWとIDSのトラフィック制御の違い

- Control
  - L7SW
    - ユーザ単位の制御が可能ユーザトラフィック公平化
    - 回線単位の制御が可能



  - IDS
    - 回線単位の制御が可能



NETWORK VALUE COMPONENTS

P2Pトラフィック制御レポート