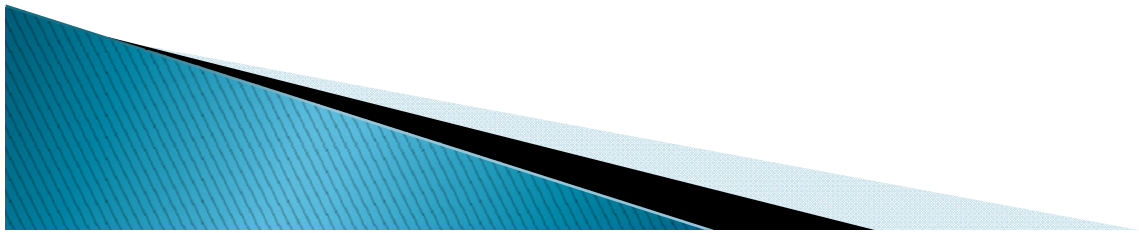
異なり数情報を使った ネットワーク管理の試み

正村雄介、松本智、佐藤聡
吉田健一、板野肯三

筑波大学大学院
システム情報工学研究科

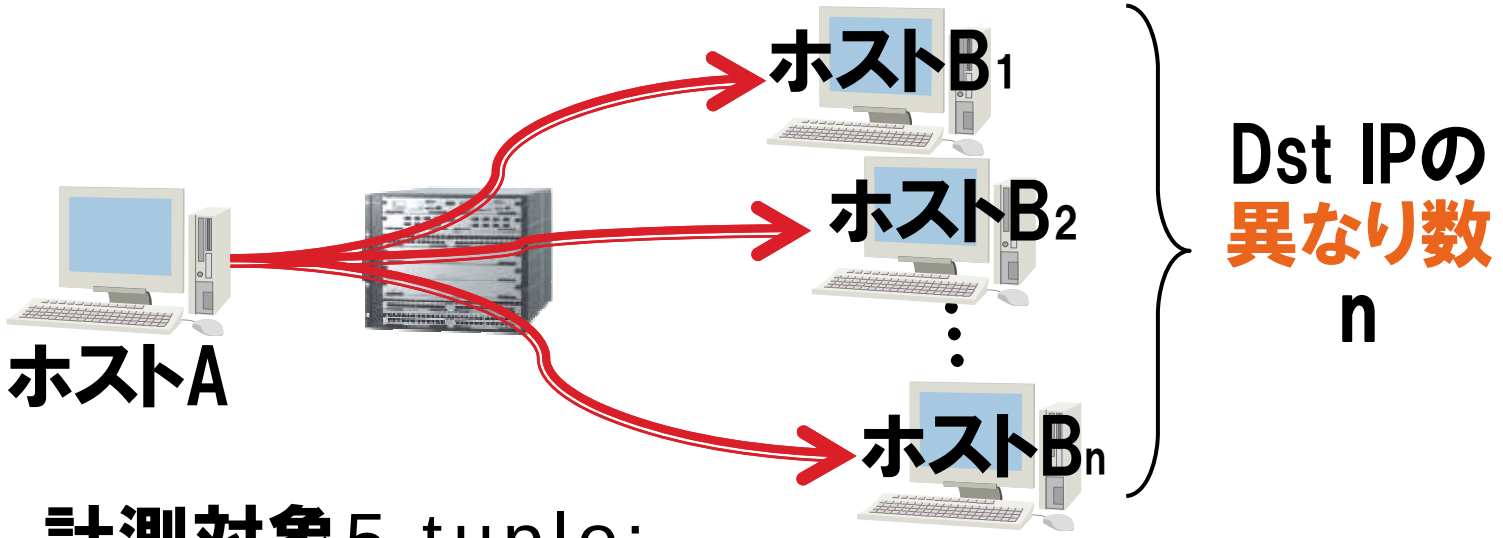
トラヒック管理の背景

- 高速回線に流れるトラヒックを可視化・制御
  - 悪意のある異常フローを排除
    - DDoS attack, Scan, Worm
  - ➢ネットワークの安全確保
  - 流量の多いフローを把握・管理
    - サーバトラヒック, P2Pトラヒック
  - ➢ネットワークの有効活用



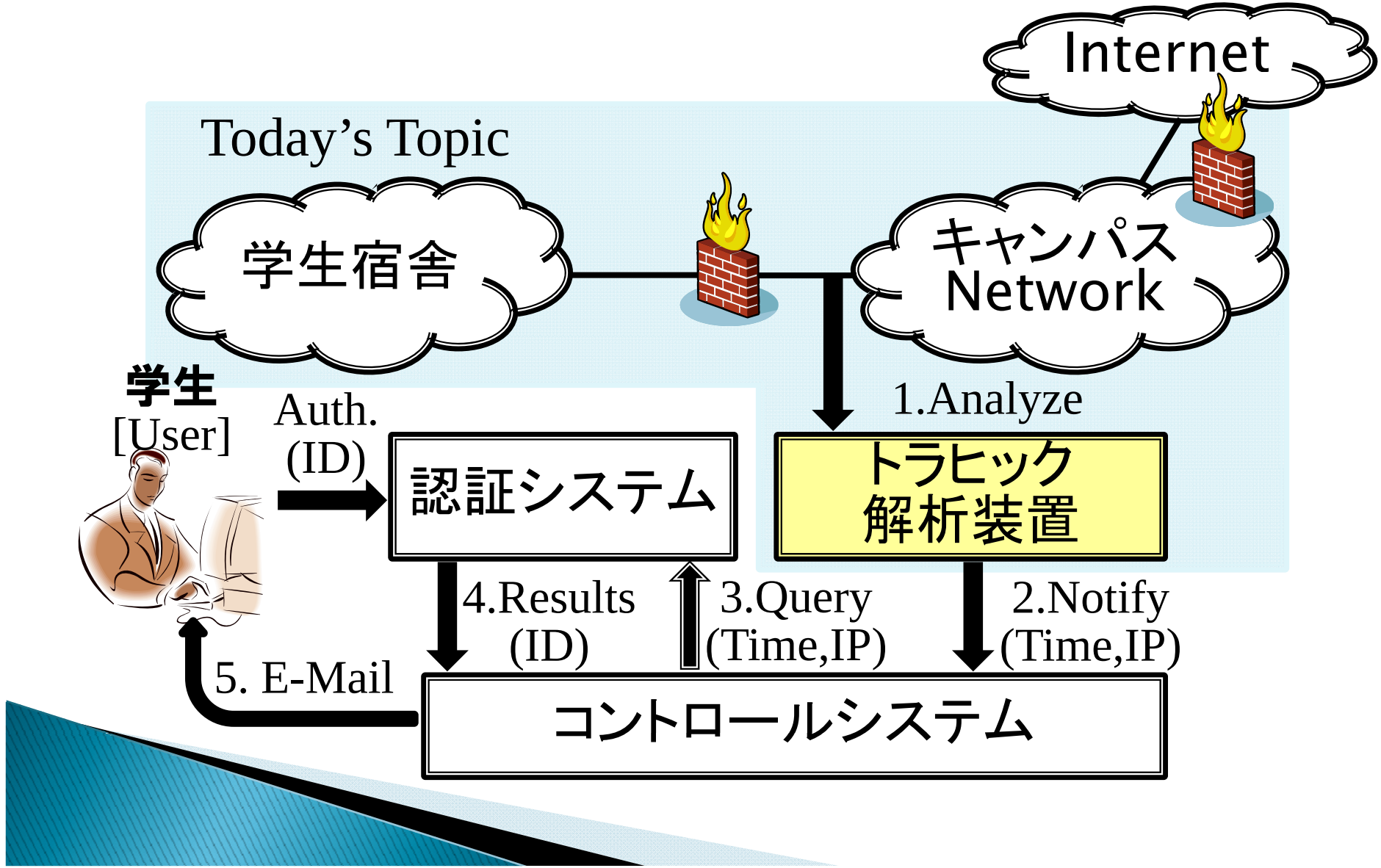
AFM ～「トラヒックの素性を知る」

- AFM(Aggregated Flow Mining)※
  - 集約フロー毎に流量を計測
  - 異なり数情報を計測
    - ホスト/フローの振る舞いを解析



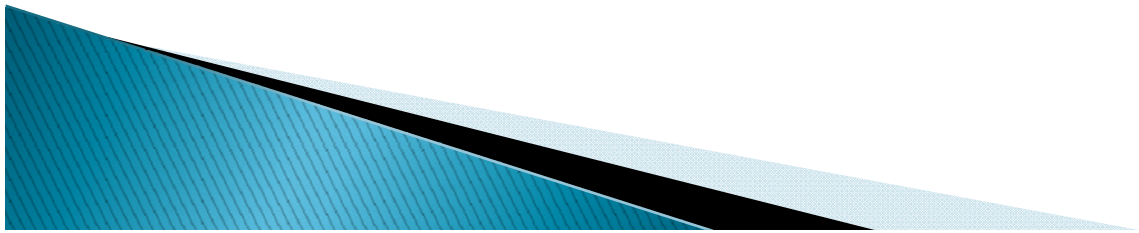
計測対象5-tuple:
(Src IP, Dst IP, Src PT, Dst PT , PRT)

システム構成


Internet
Today’s Topic
学生宿舎
キャンパス
Network
学生
[User]
Auth.
(ID)
認証システム
1.Analyze
トラヒック
解析装置
4.Results
(ID)
3.Query
(Time,IP)
2.Notify
(Time,IP)
5. E-Mail
コントロールシステム

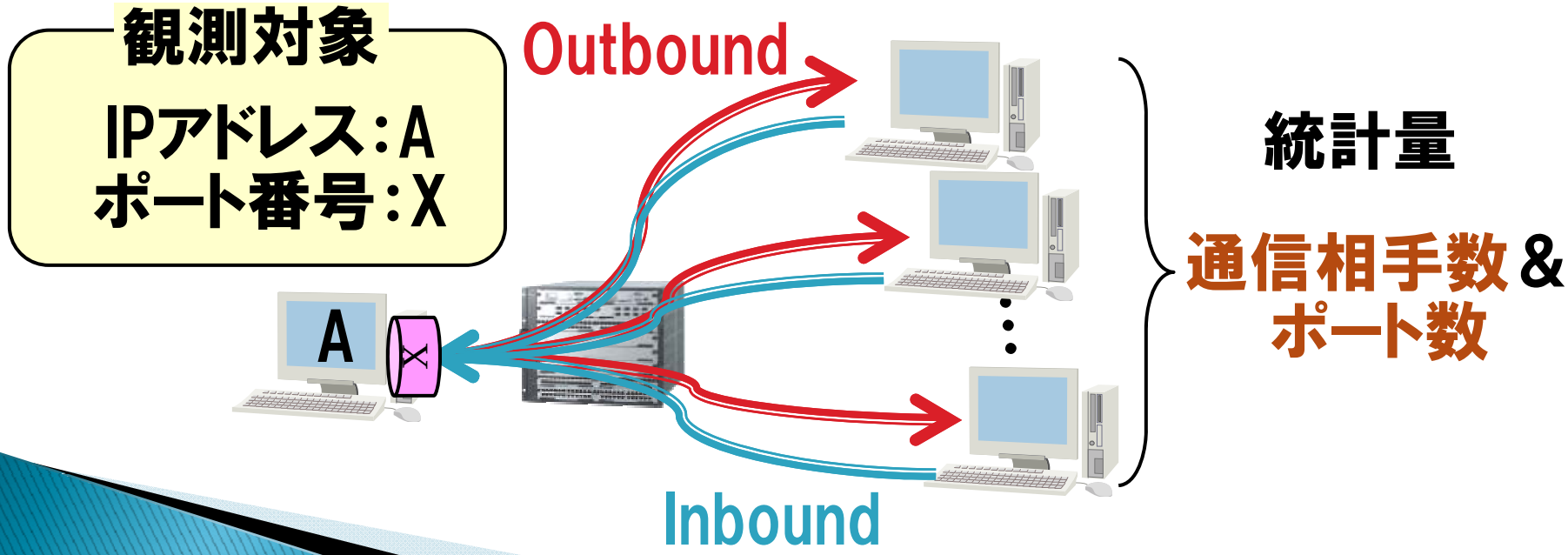
学生宿舎のネットワーク

- 4,000部屋に Ethernet port を設置
- 認証システムを使い各自のPCを接続
- グローバルIPv4アドレスを割り当て
- 海外留学生や新入生が多数在籍



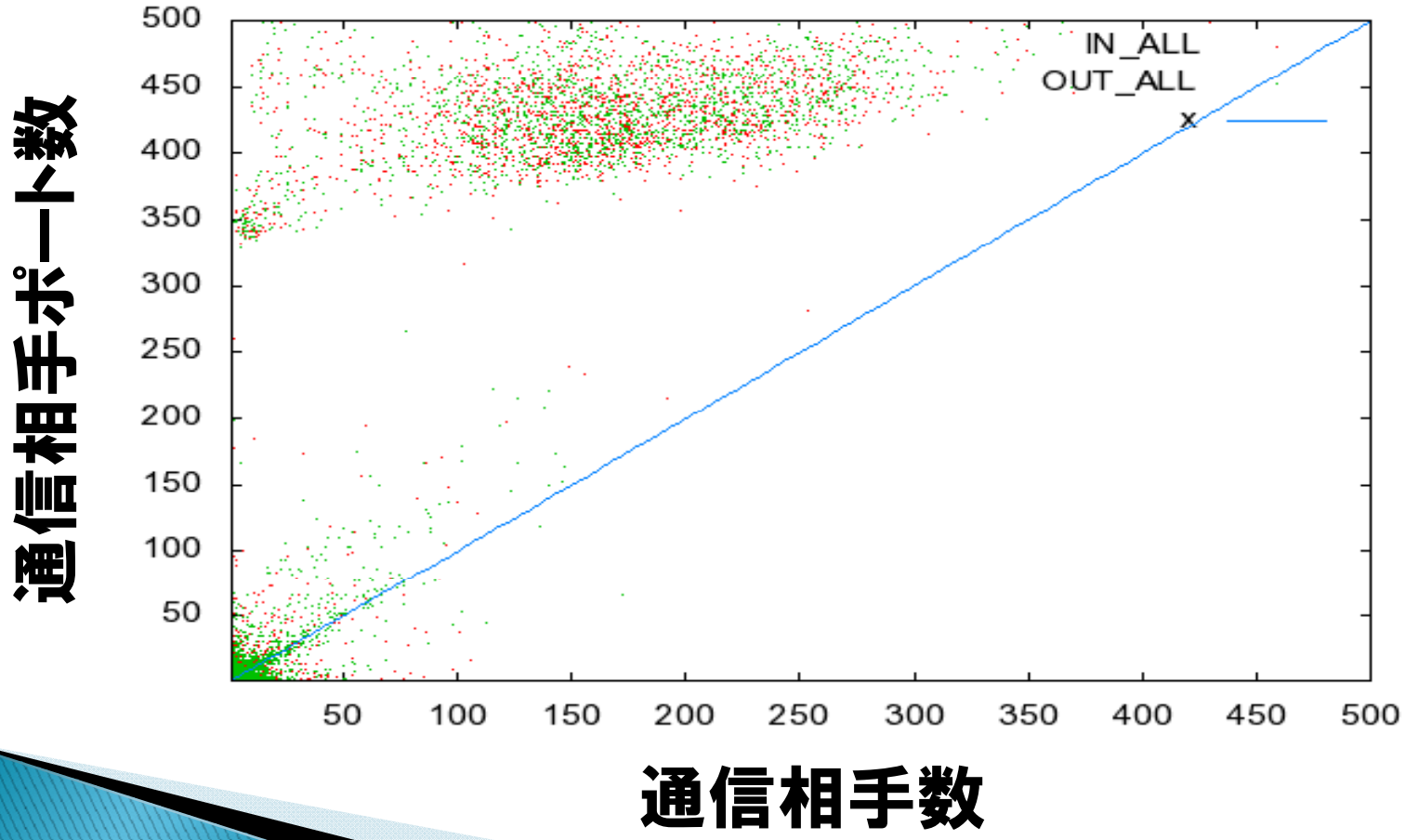
解析事例（Ⅰ）

- Server Flow
  - Outbound　3-tuple : Src_IP, Src_PT, PRT
  - Inbound　　3-tuple : Dst_IP, Dst_PT, PRT



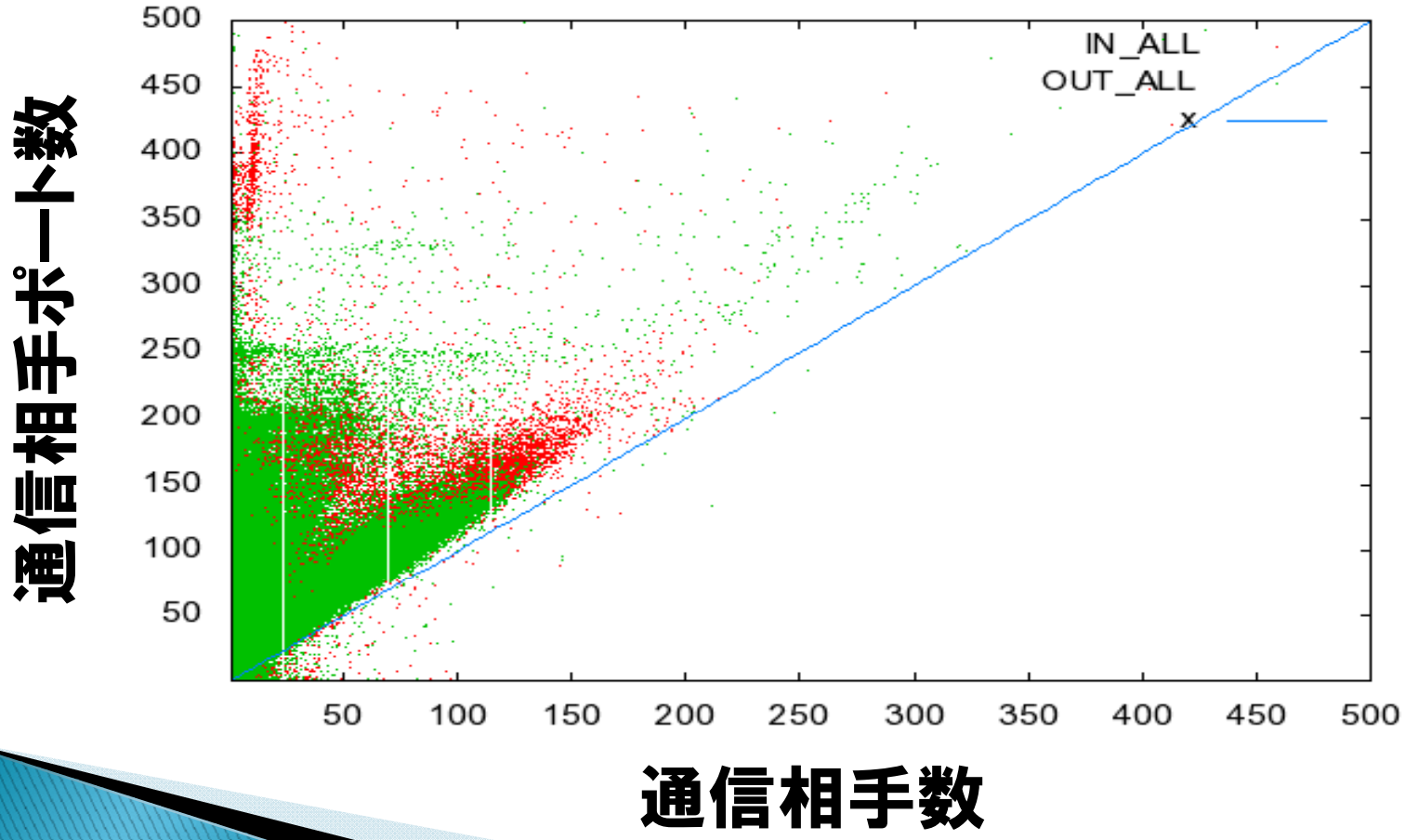
事例Ⅰ -TCP traffic (1/3)

- 観測対象:学生宿舎の IPアドレス



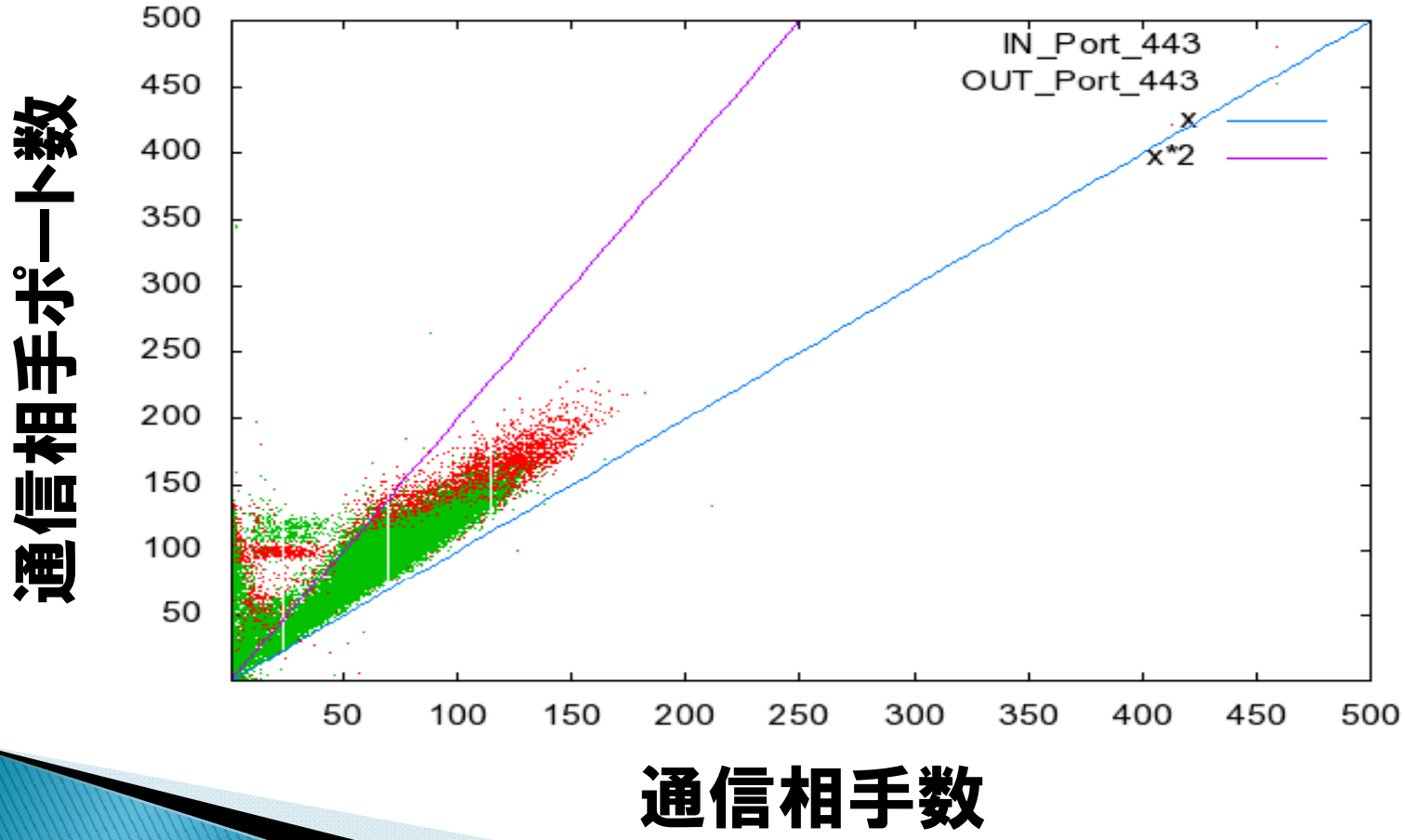
事例Ⅰ –TCP traffic (2/3)

- 観測対象：外部のIPアドレス



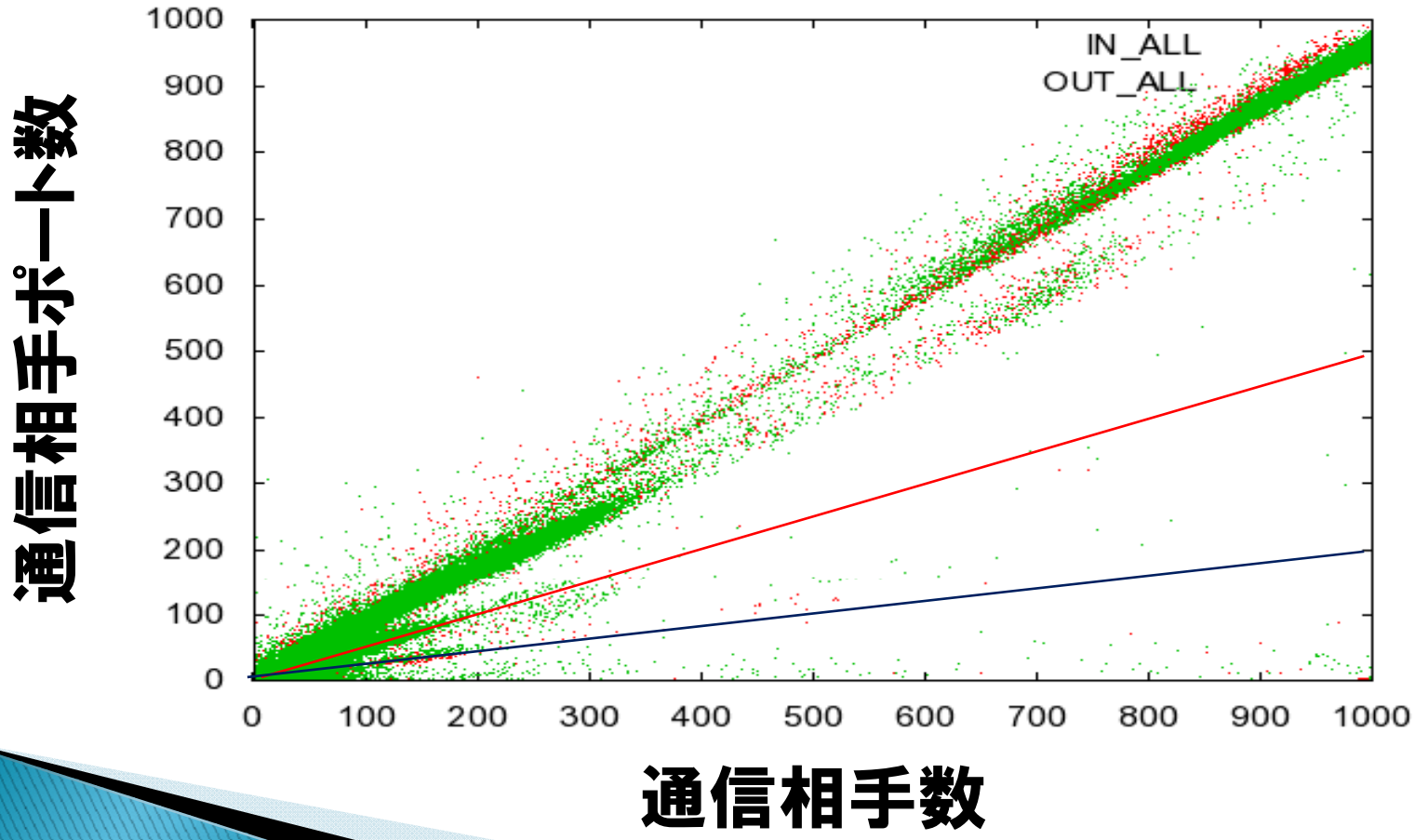
事例Ⅰ –TCP traffic (3/3)

- 観測対象：外部のIPアドレス



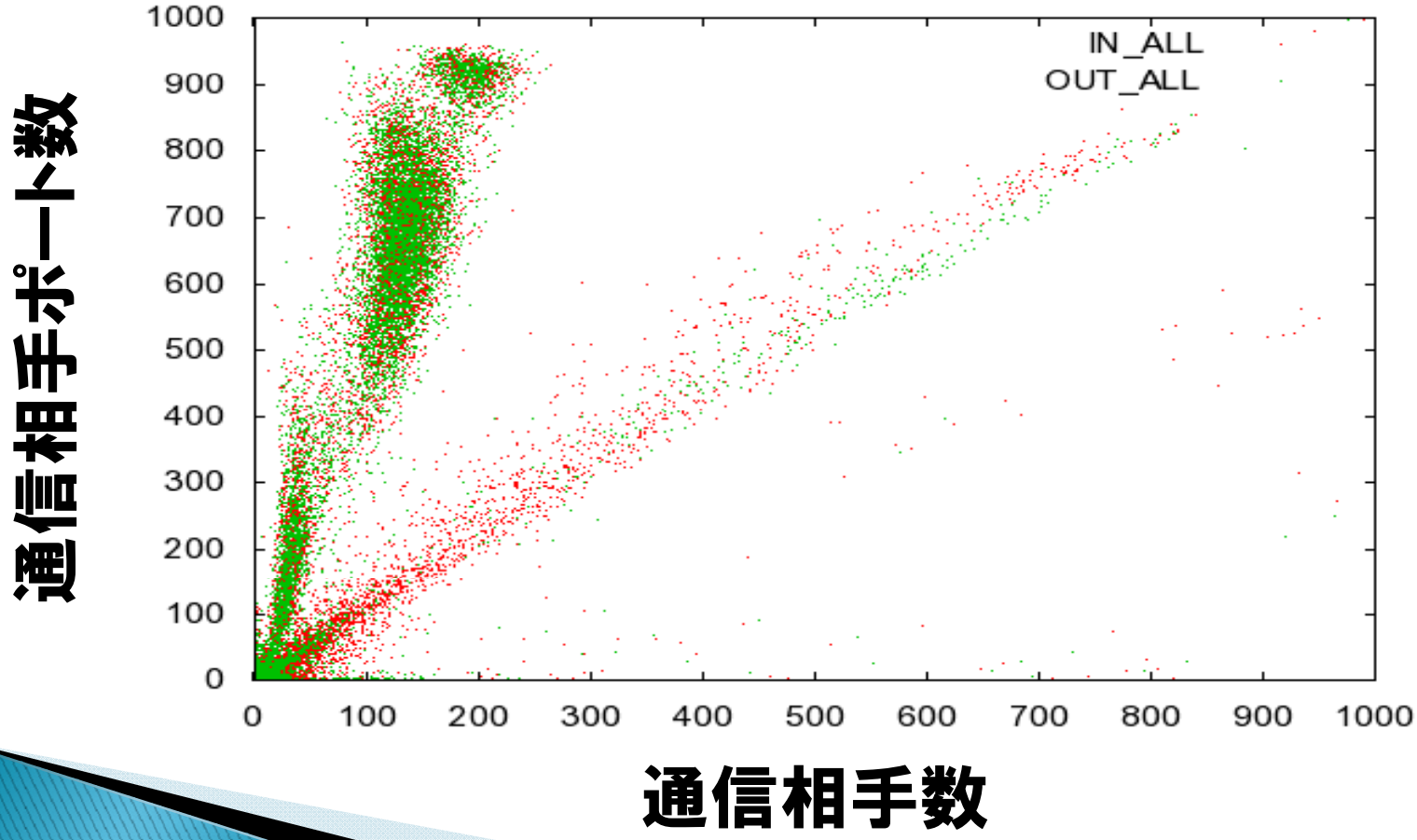
事例Ⅰ –UDP traffic (1 /2)

- 観測対象:学生宿舎の IPアドレス



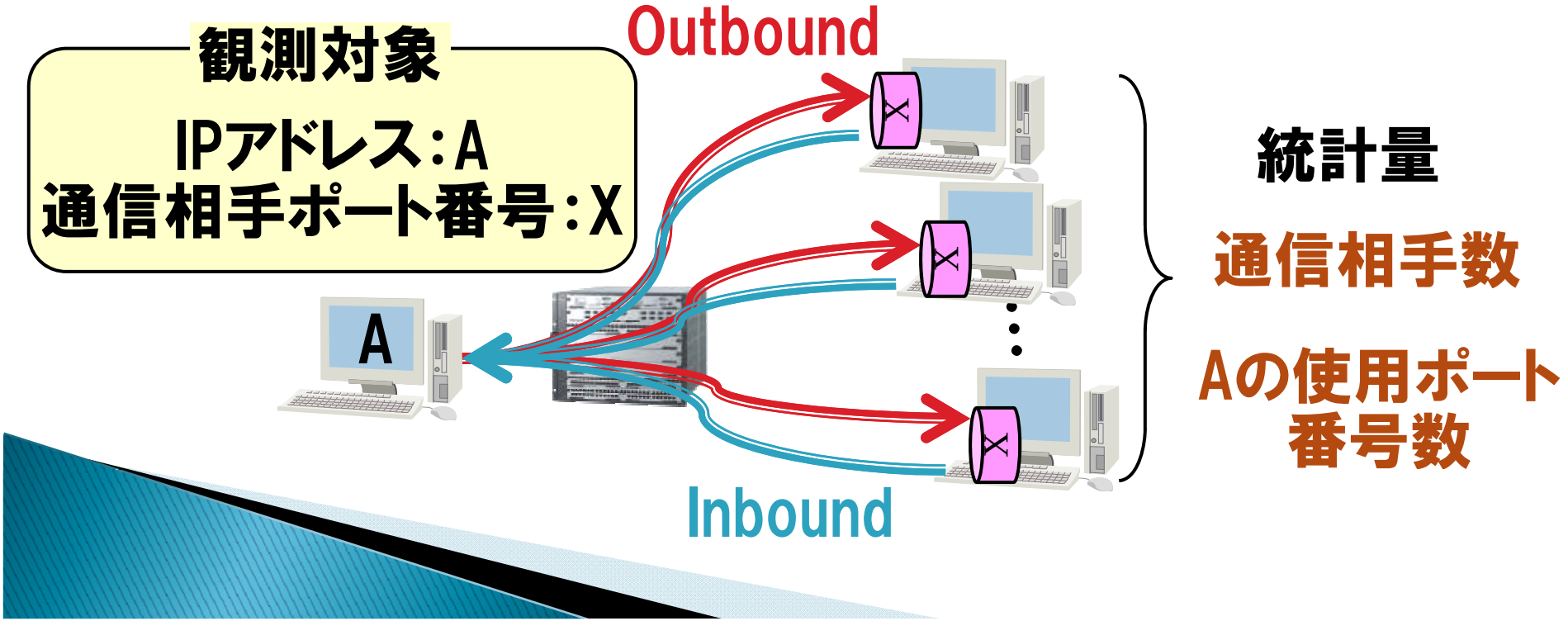
事例Ⅰ –UDP traffic (2/2)

- 観測対象：外部のIPアドレス



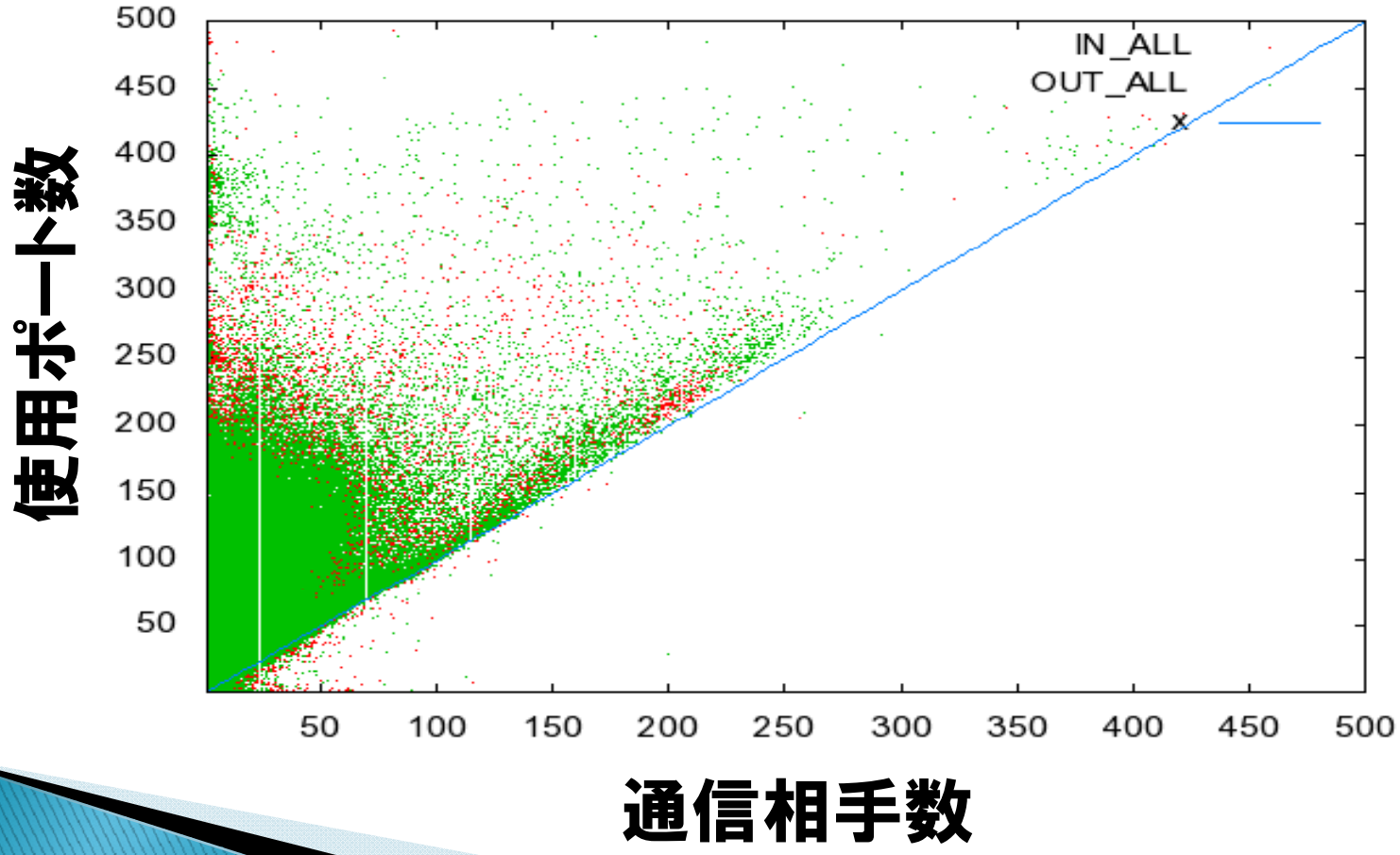
解析事例（Ⅱ）

- Client Flow
  - Outbound 3-tuple : Src_IP, Dst_PT, PRT
  - Inbound　3-tuple : Dst_IP, Src_PT, PRT



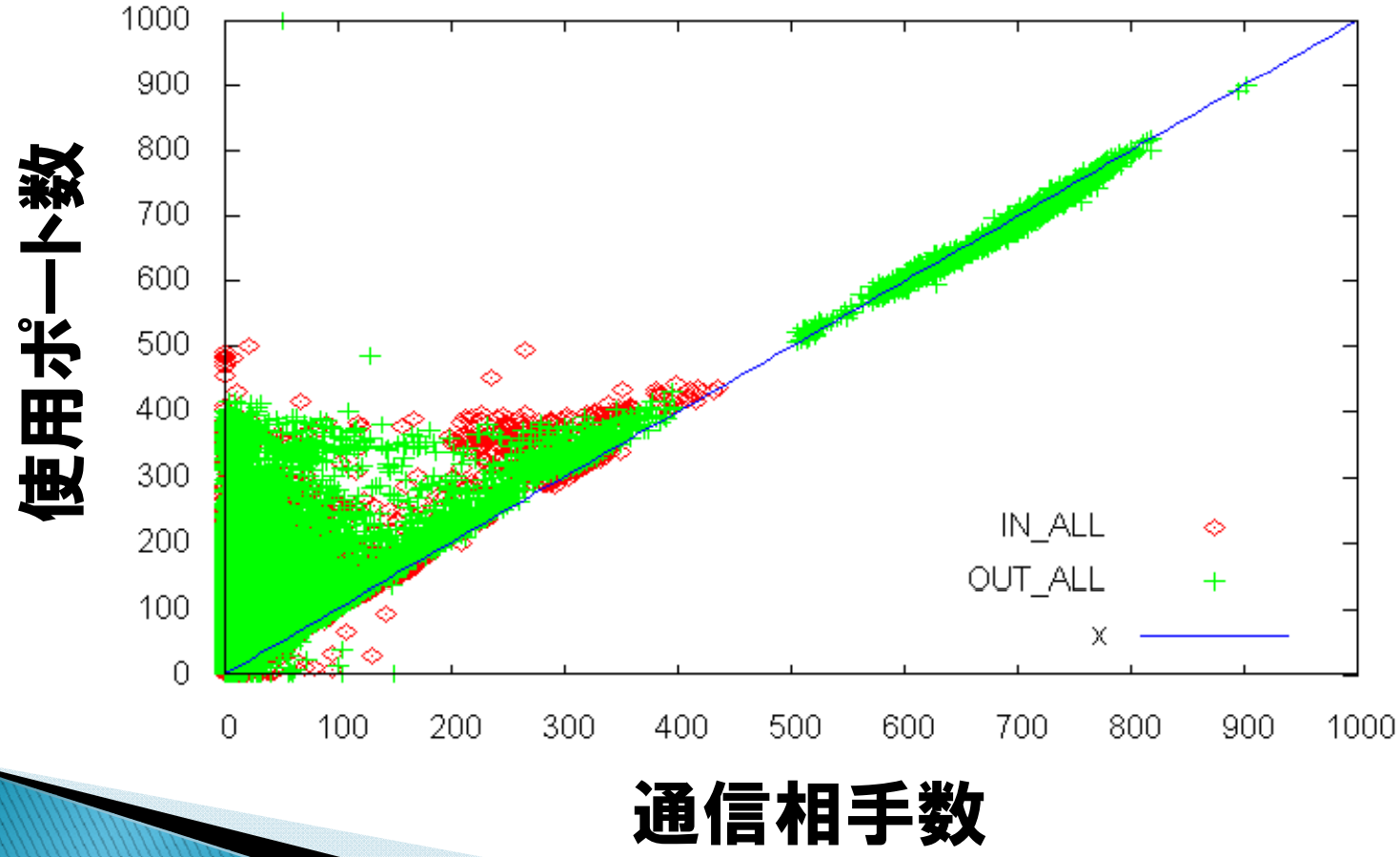
事例Ⅱ –TCP traffic (1/3)

- 観測対象:学生宿舎の IPアドレス



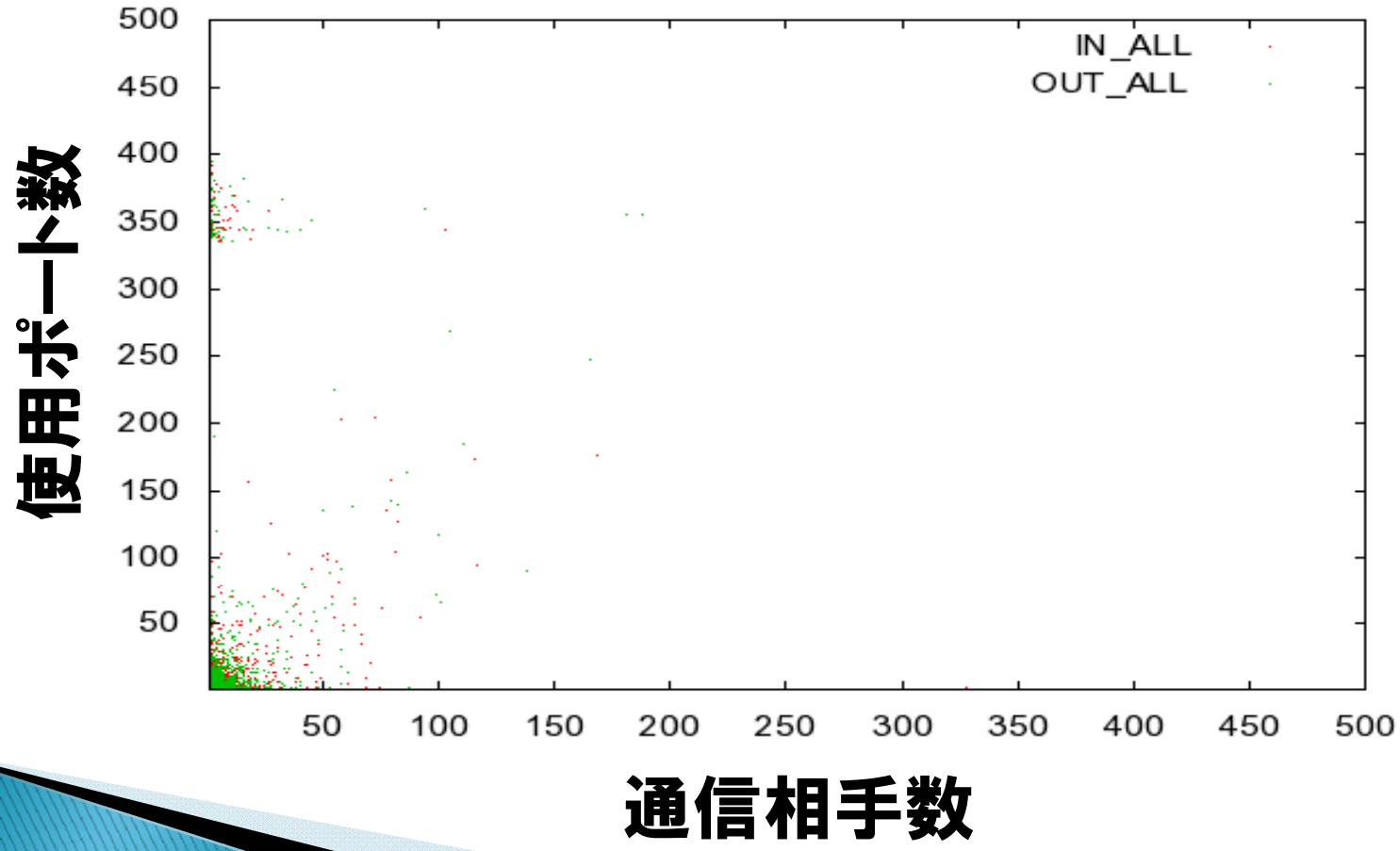
事例Ⅱ –TCP traffic (2/3)

- 観測対象:学生宿舎の IPアドレス



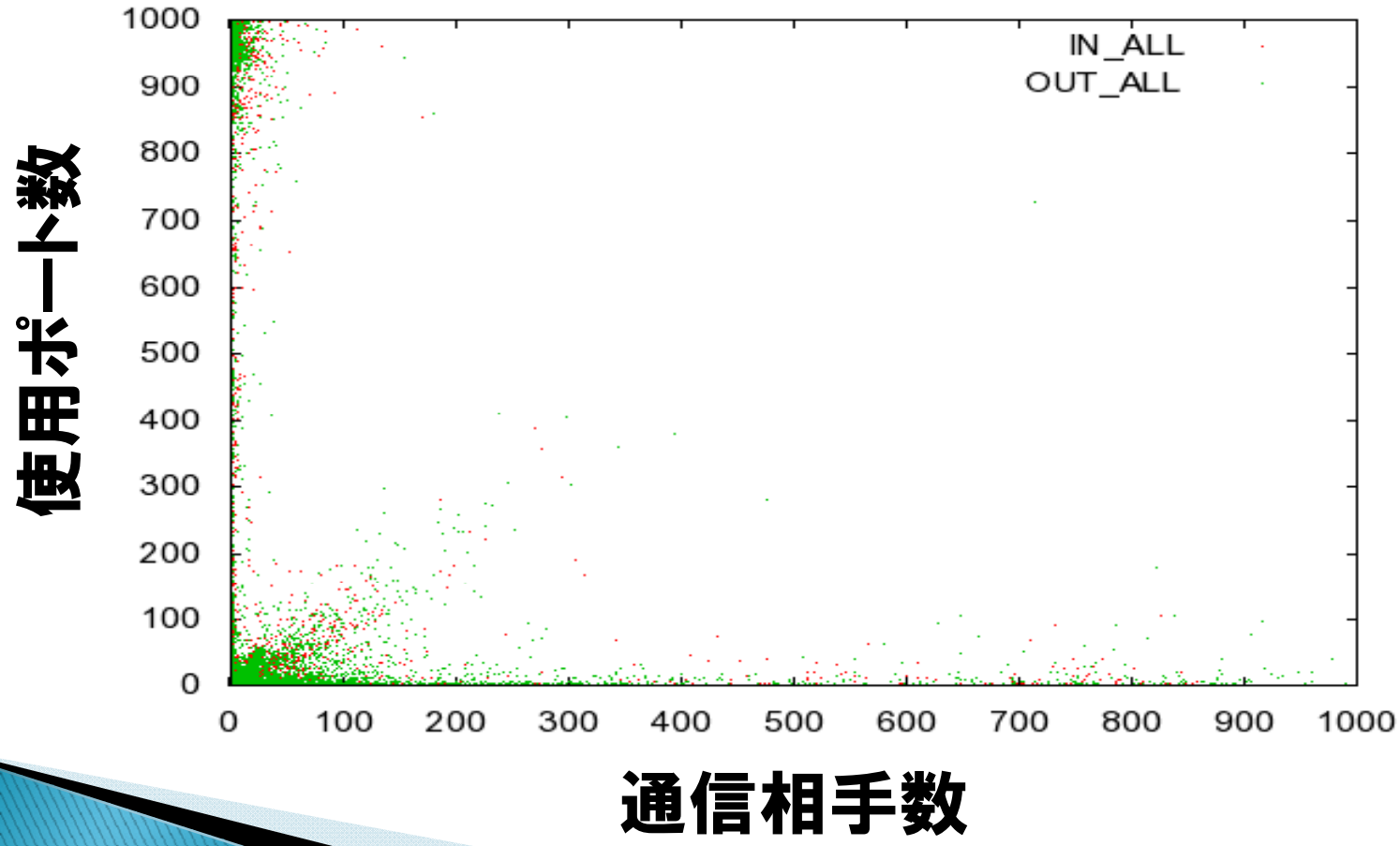
事例Ⅱ –TCP traffic (3/3)

- 観測対象：外部のIPアドレス



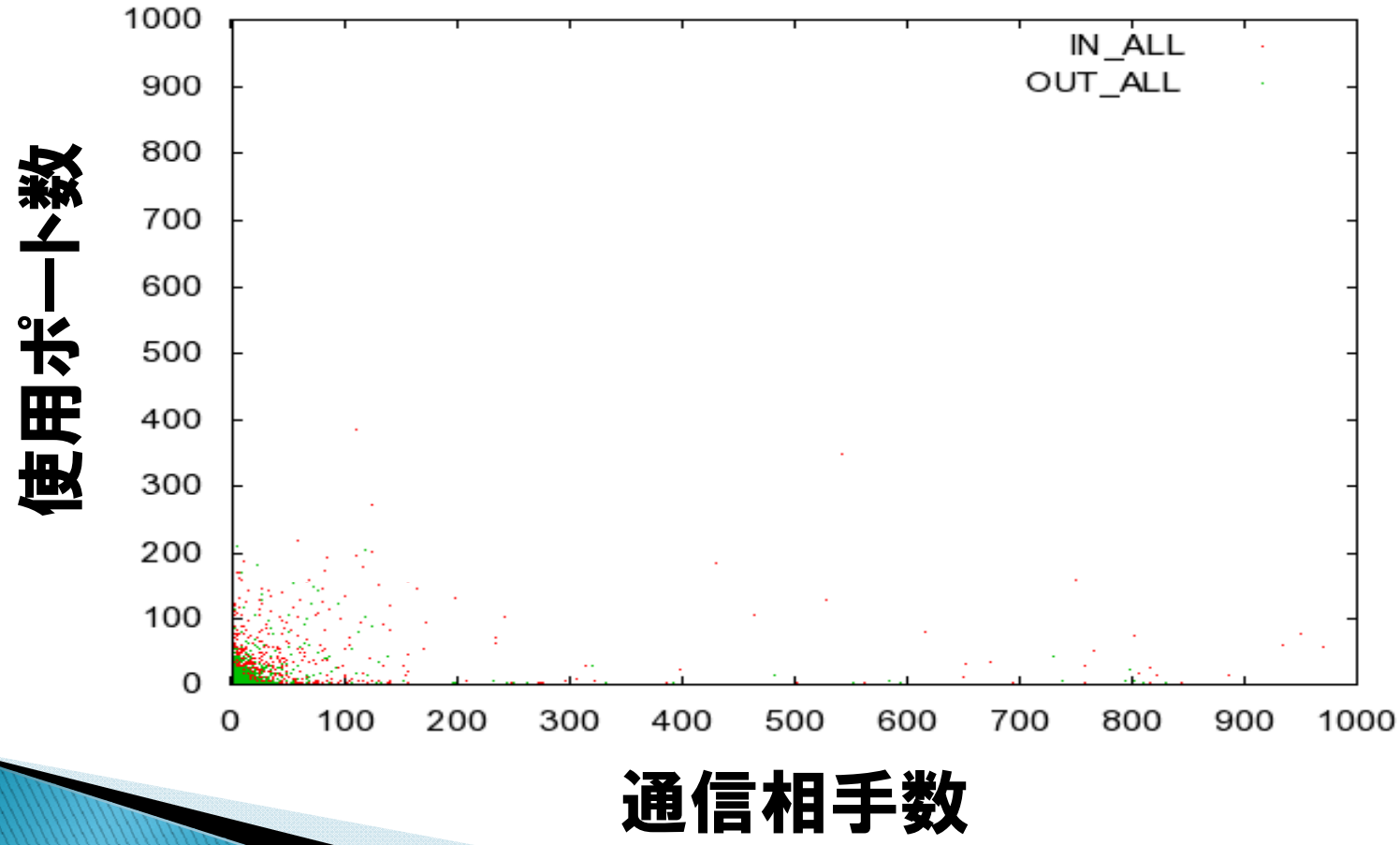
事例Ⅱ –UDP traffic (1 /2)

- 観測対象:学生宿舎の IPアドレス



事例Ⅱ –UDP traffic (2/2)

- 観測対象：外部のIPアドレス



結論

- 異なり数解析装置（AFM※）を筑波大学キャンパスNWに設置し運用
  - ノンサンプリングでのトラヒック監視
  - 端末認証システムとの連携
- 異常トラヒックの検出が可能なことを検証
  - Scanを実施しているホストの検出

（※）Y. Shomura et.al, “Analyzing the Number of Varieties in Frequently Found Flow,” IEICE Trans. Commun., vol.E91-B, no.6, pp.1896-1905, Jun.2008.