Non-Sampling Flow Inspection を支える技術

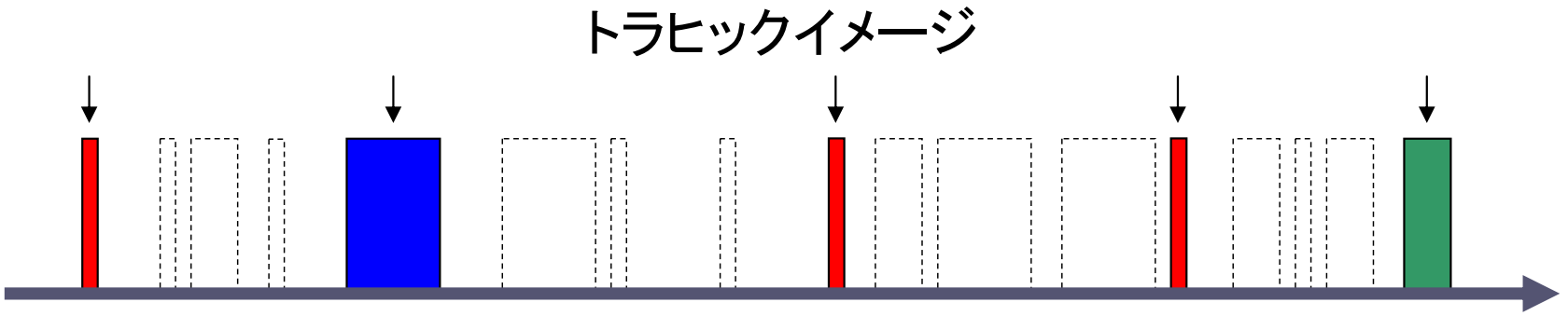
ユーテン・ネットワークス株式会
新籾 晶

アジェンダ

- Non-Sampling Flow Inspection を支える技術
  - 背景のおさらい
  - トラヒック解析の問題点（Non-Sampling観点）
  - 解決策
  - ハードウェア 作っちゃいました!!
  - 本当に Non-Sampling は実現できたのか?
    - 性能比較による検証
  - まとめ

背景

- 従来は Sampling でのトラヒック解析のみ



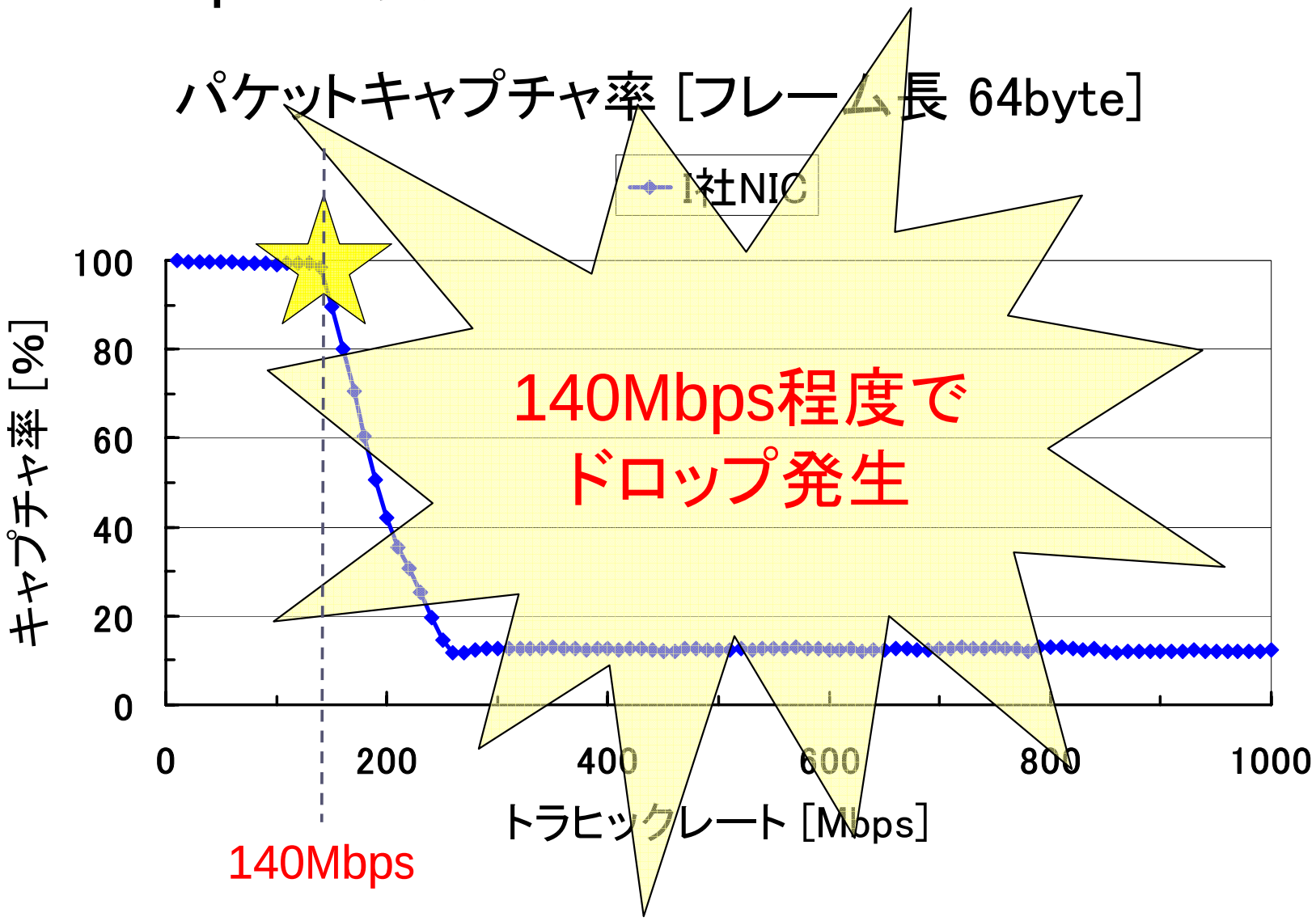
例えば 1/4 Sampling すると ...

トラヒック解析結果に誤差

しかし Non-Sampling は難しい...

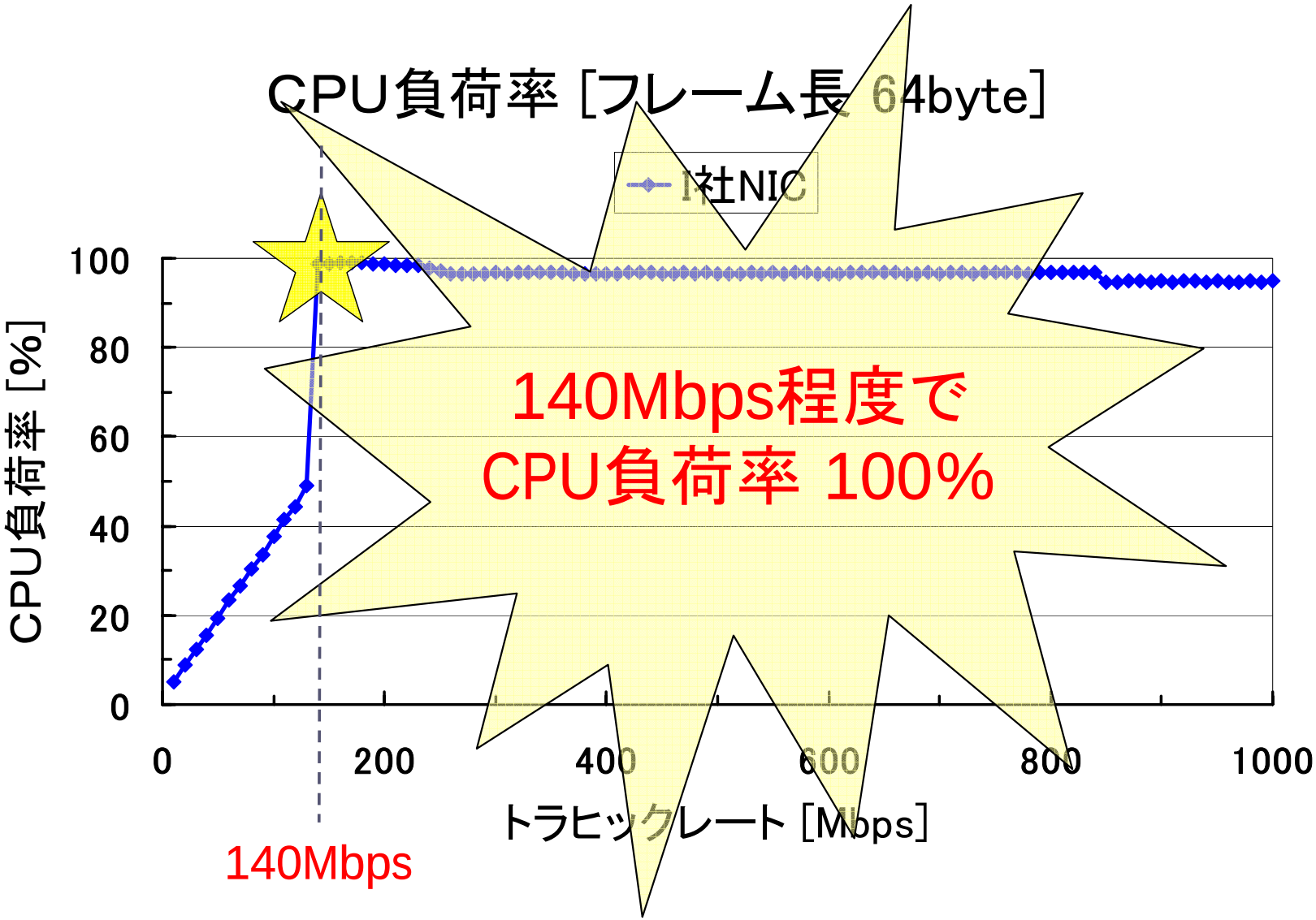
従来の問題点(1)

- 140Mbps 程度でドロップ発生



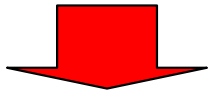
従来の問題点(2)

- CPU負荷率 100%



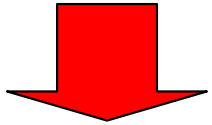
目標

- 問題未解決のままでの Sampling 解析



- 見るべき現象が「本当はみえていない」のでは?

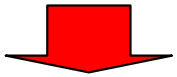
- だから Non-Sampling でやってみよう!!



- 要件
  - フルレートパケットキャプチャ
  - CPUパワーの確保

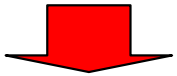
解決策とアプローチ

- 課題：フルレートパケットキャプチャ

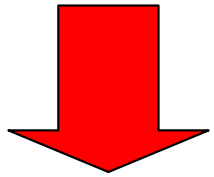


解決策：PCI-X による高速転送

- 課題：CPUパワーの確保



解決策：パケットキャプチャ処理をハードウェア化



- アプローチ
  - これらを可能にするアクセラレータHWの開発

アクセラレータ ハードウェア

u10 Networks

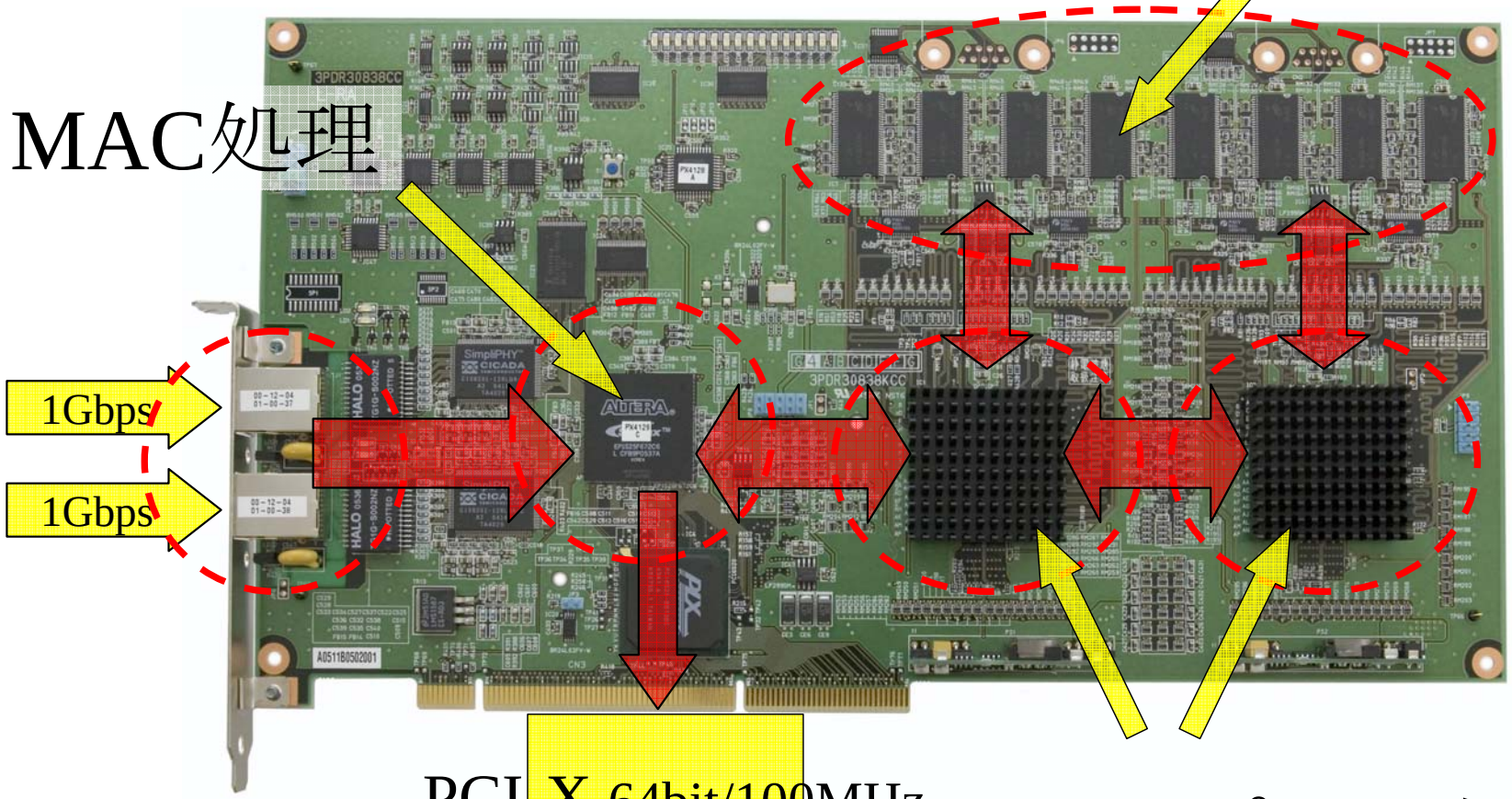
作っちゃいました。

GigaPcap の技術

u10 Networks

libpcap Accelerator

DDR-SDRAM
512MB



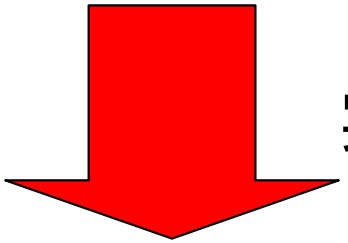
作った その次は

u10 Networks

じゃあ
動かしてみよう!!

実現性の検証

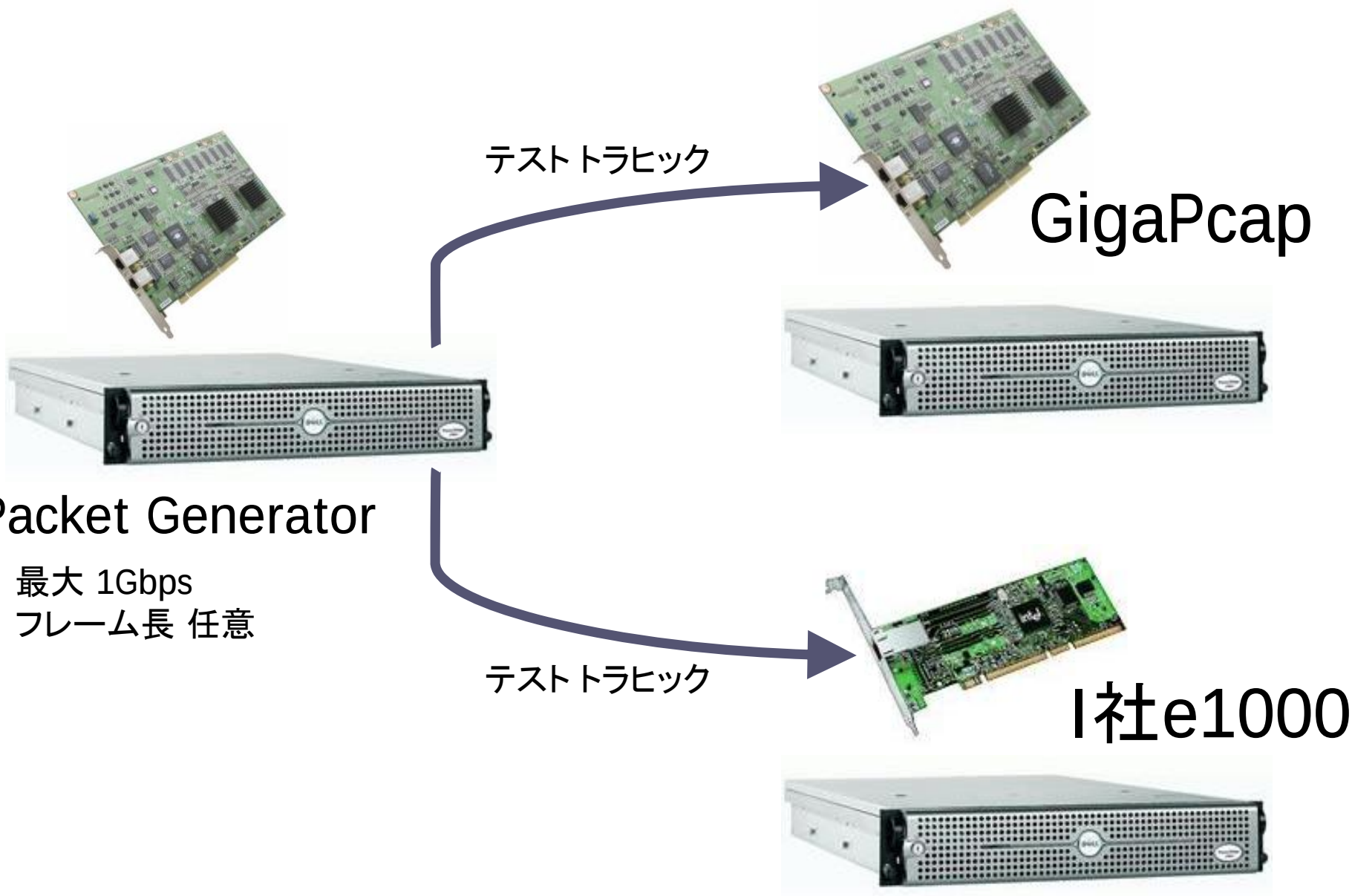
- 本当に、このアクセラレータによって
  Non-Sampling が実現可能??
- フツウのNIC だと、どこまでできる??



実験して確認

- パケットキャプチャ性能の評価を行う
  - パケットキャプチャ率
  - CPU負荷率 (tcpdump -w /dev/null 実行時)
  - トラヒックレート: 10Mbps～1Gbps
  - フレーム長: 1518byte , 64byte, 200byte

性能比較 評価系の構成



性能比較 比較カードとホストマシン仕様

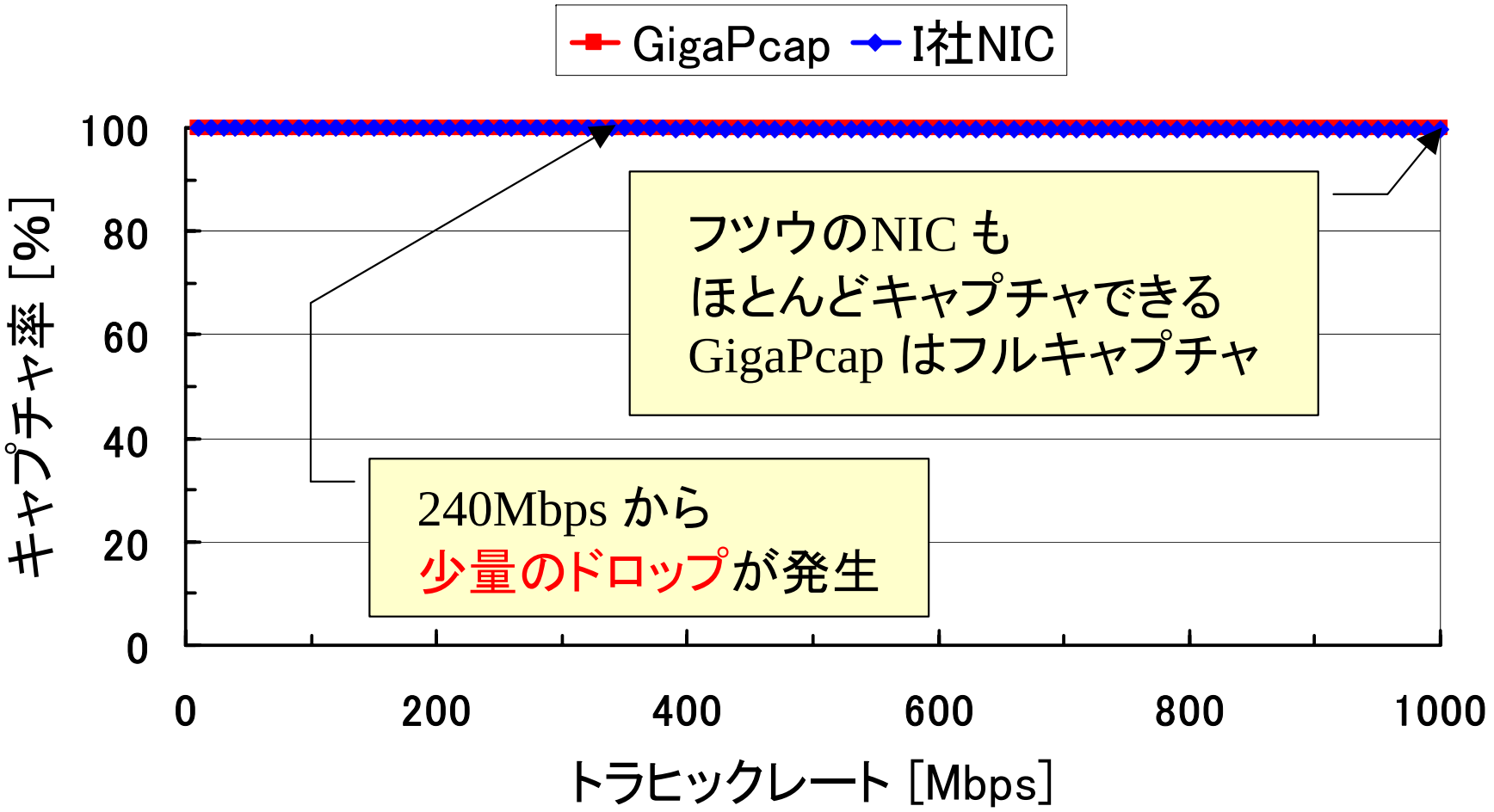
- 性能比較するパケットキャプチャカード
  - フツウのNIC代表 I社 e1000
  - u10 Networks GigaPcap

- 特別なところの無い、至ってフツウなマシンで評価実施
  - ホストマシン構成
    - Dell PowerEdge2850 / 2U ラックマウント型
    - Intel Xeon 2.8GHz (single)
    - RAM 1GB (PC3200, DDR2, 400MHz)
    - PCI-X スロット×3
  - ホストOS
    - Red Hat Enterprise Linux ES 4
    - Kernel 2.6.9-5EL, Uni-processor Mode

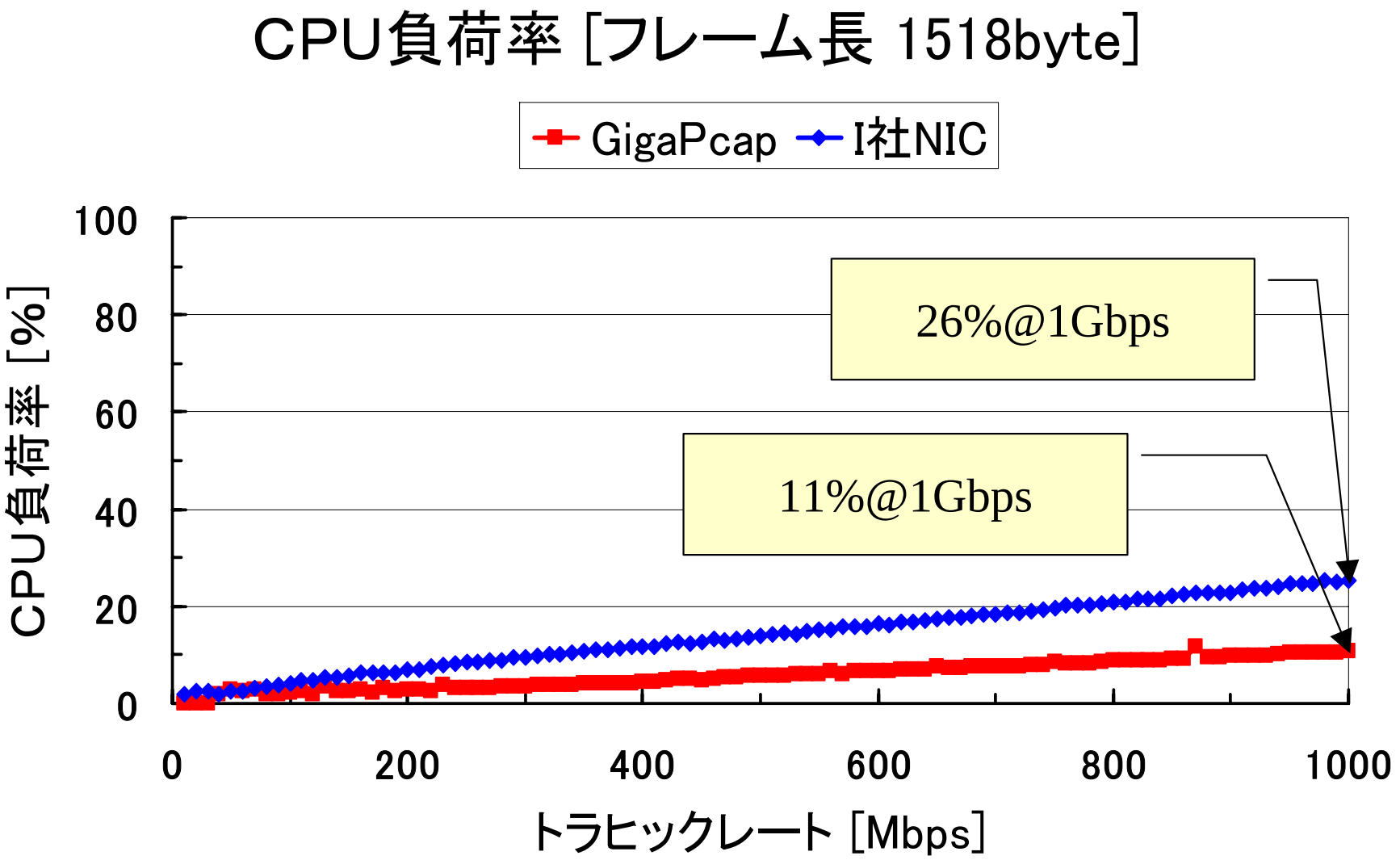
性能比較(1) フレーム長 1518byte

u10 Networks

パケットキャプチャ率 [フレーム長 1518byte]

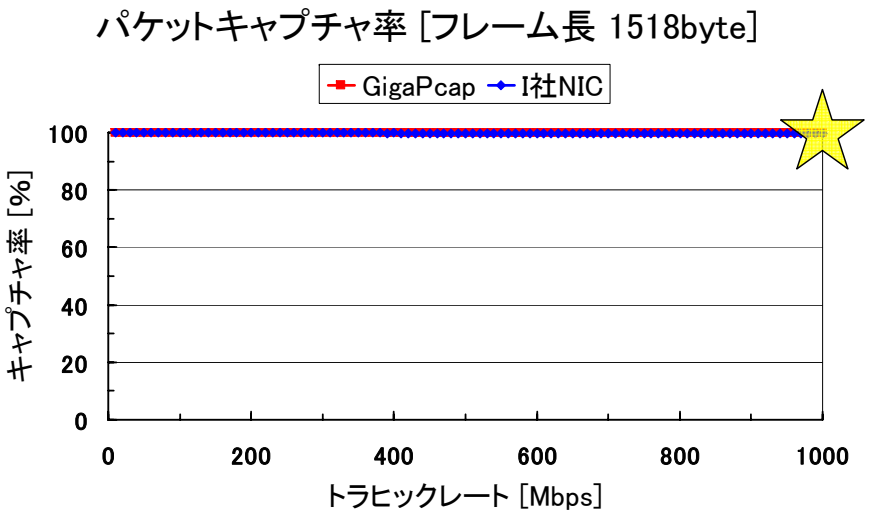


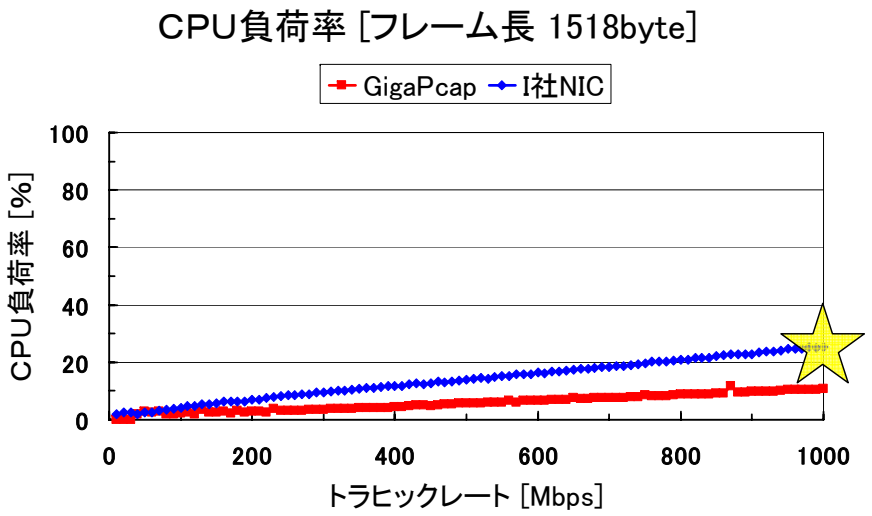
性能比較(1) フレーム長 1518byte



性能比較(1) フレーム長 1518byte

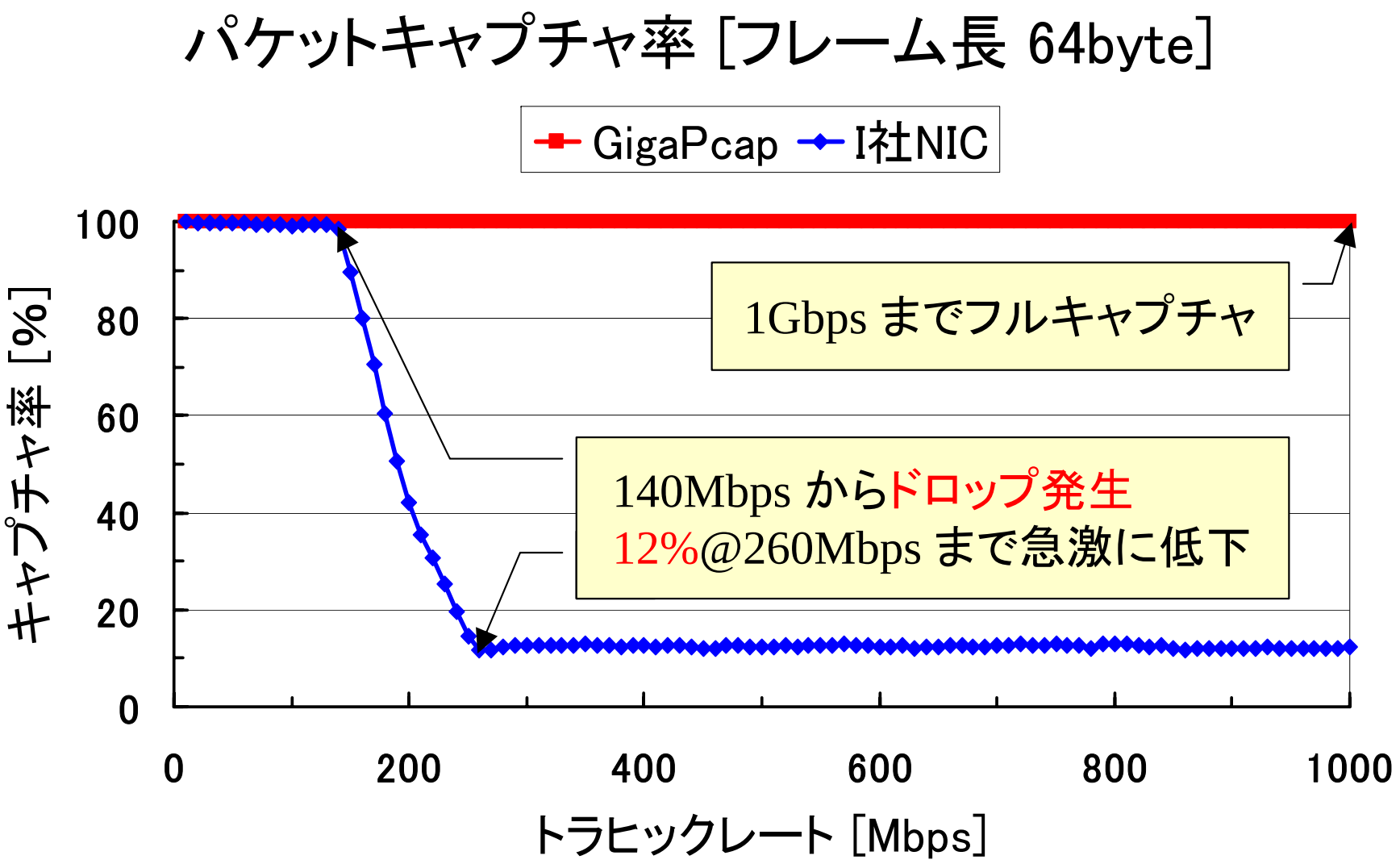
フツウのNICでも、ほとんどキャプチャできる
CPU負荷率 26%@1Gbps



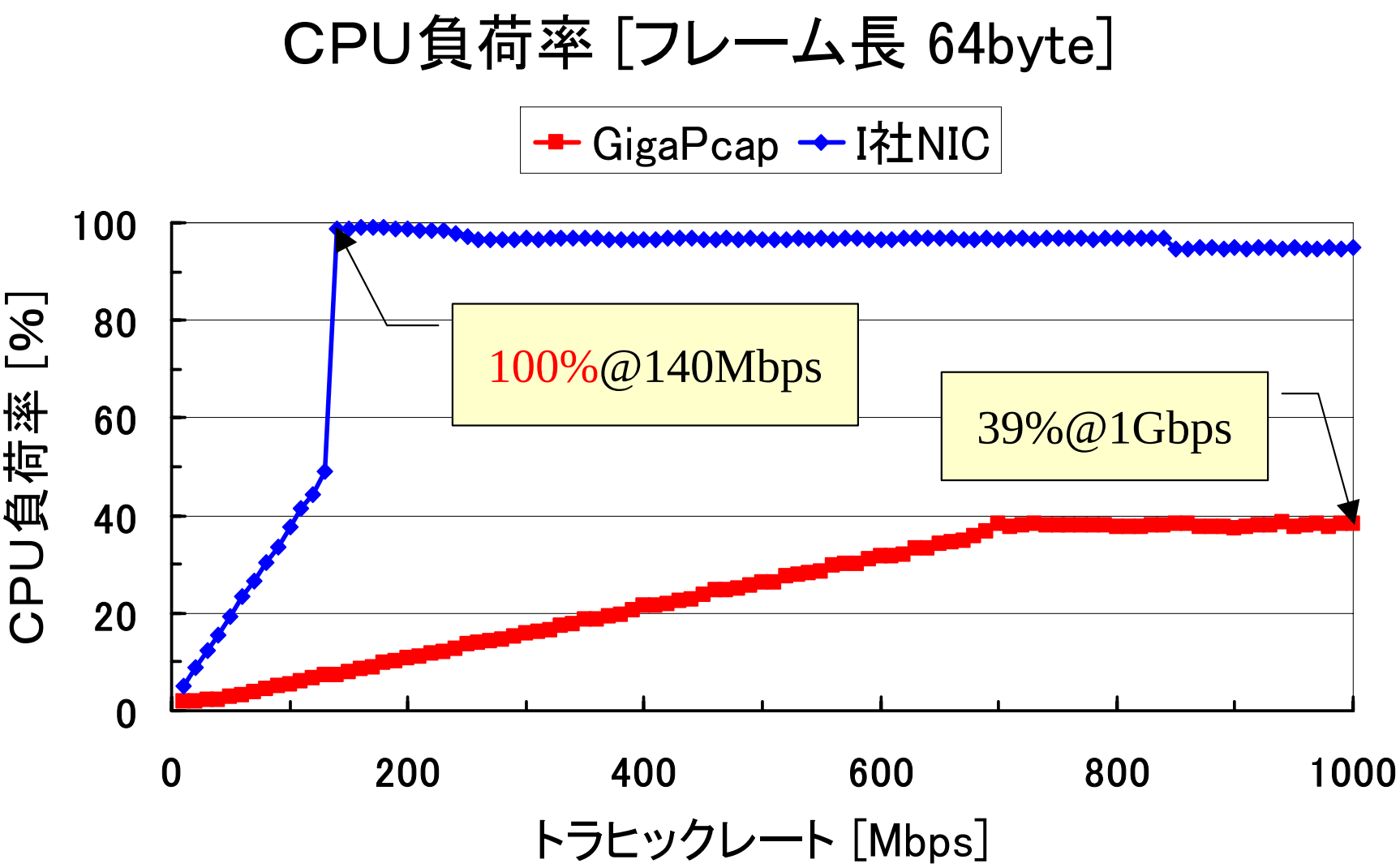


これなら分析処理も行うことができるが…
少量のパケットドロップがあるから
Non-Sampling になっていない

性能比較(2) フレーム長 64byte



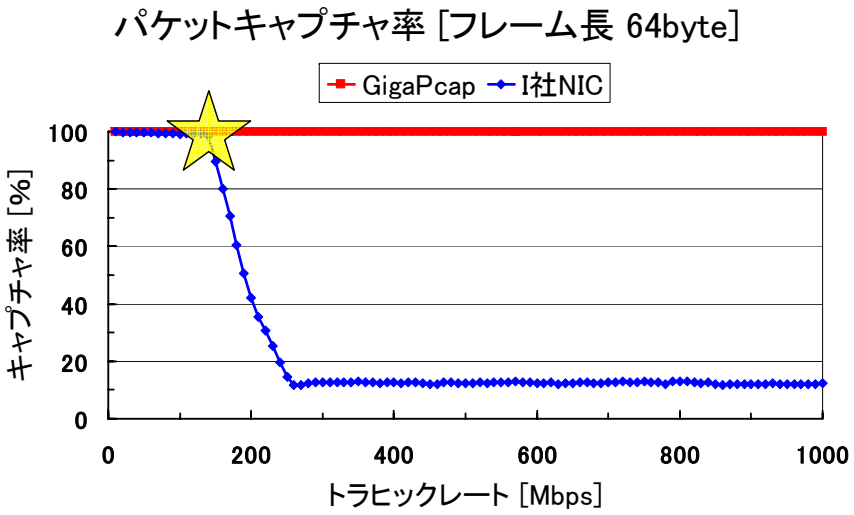
性能比較(2) フレーム長 64byte

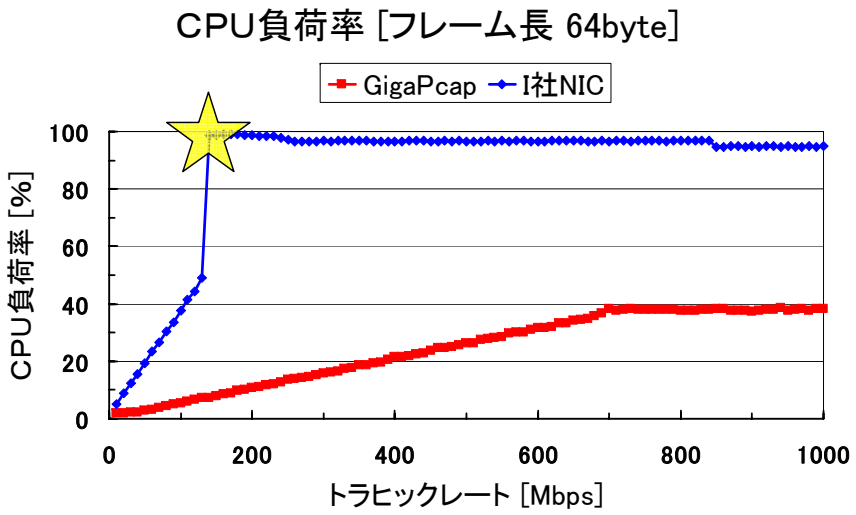


性能比較(2) フレーム長 64byte

u10 Networks

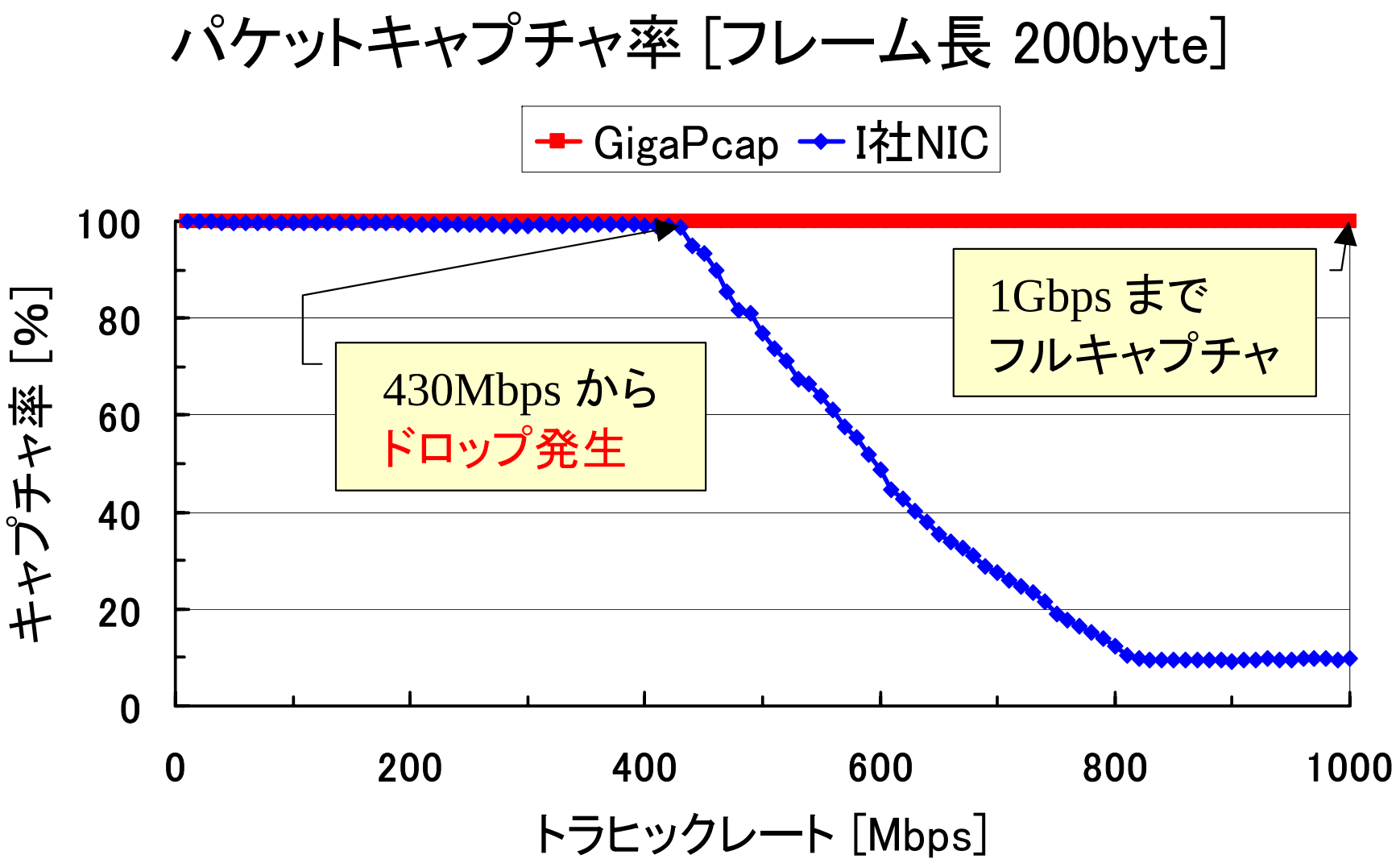
140Mbps程度から急激にドロップ発生
CPU負荷率 100%@140Mbps





ちょっと非現実的なトラヒックモデル??
しかしDoSアタックなどにまったく無力
そのうえ分析時にSamplingしちゃうの?!

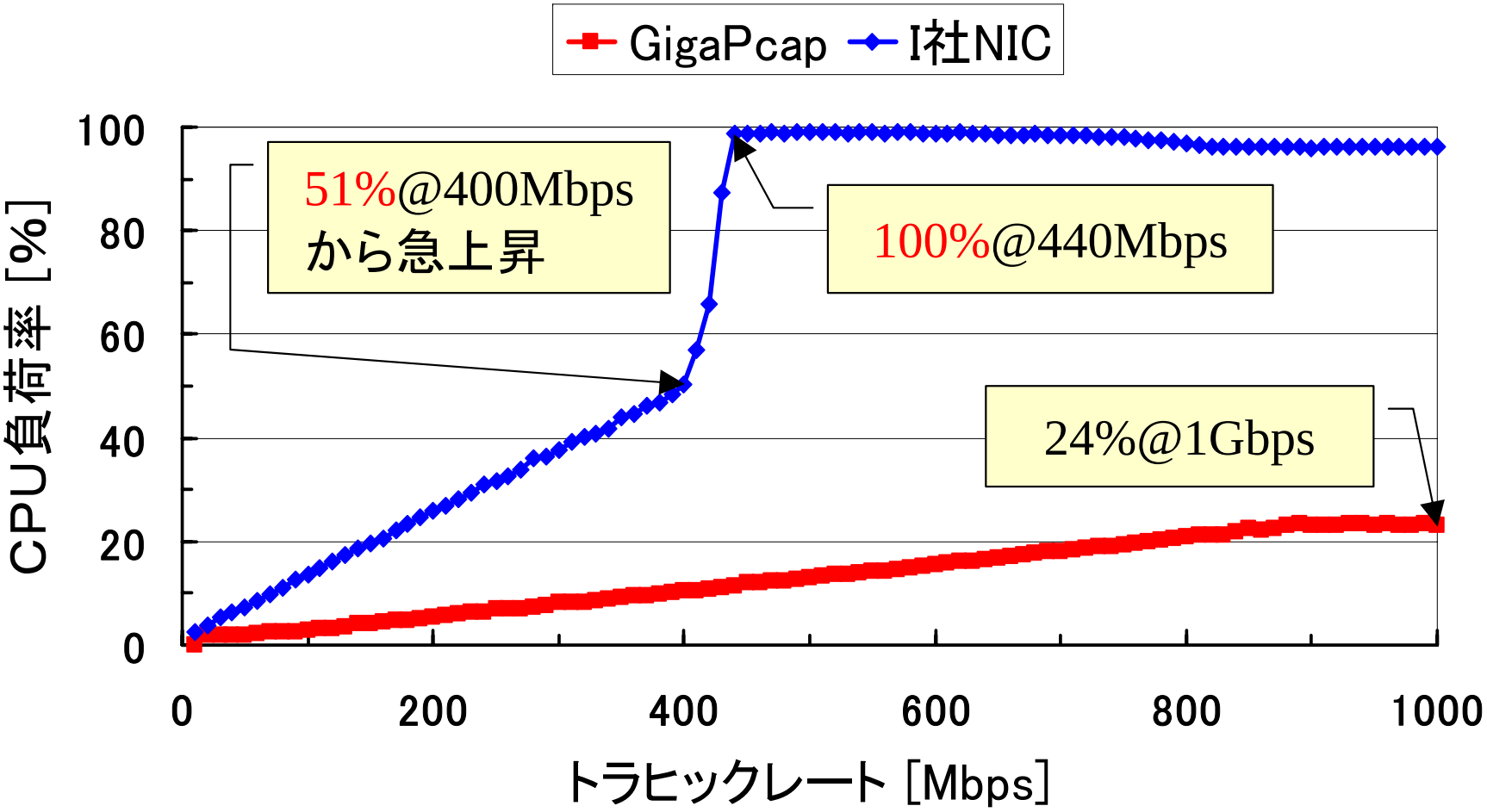
性能比較(3) フレーム長 200byte



性能比較(3) フレーム長 200byte

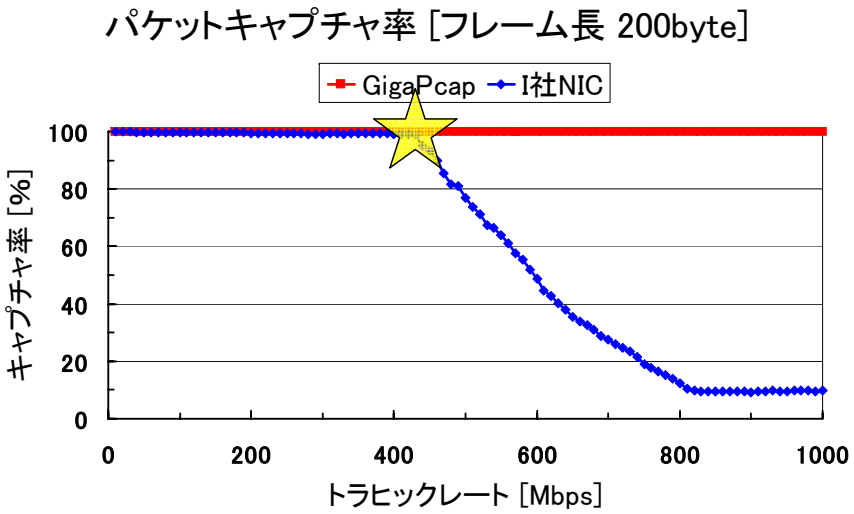
u10 Networks

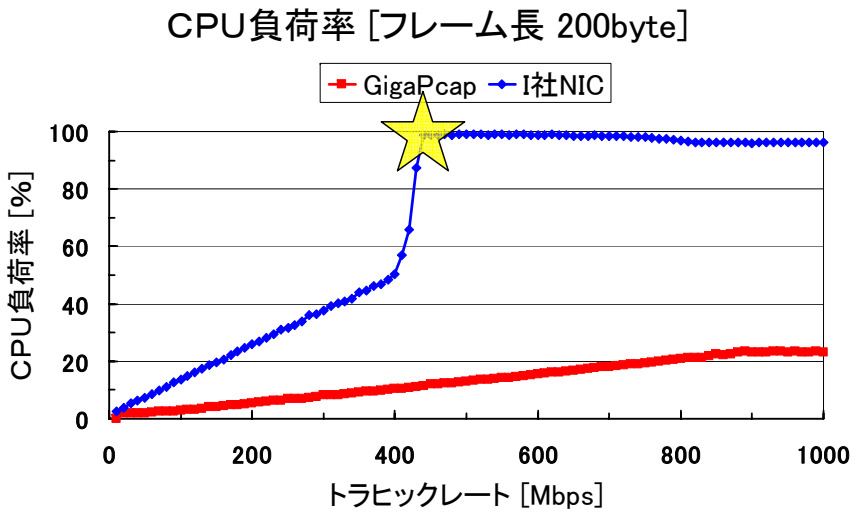
CPU負荷率 [フレーム長 200byte]



性能比較(3) フレーム長 200byte

430Mbps程度からドロップ発生
CPU負荷率 100%@440Mbps





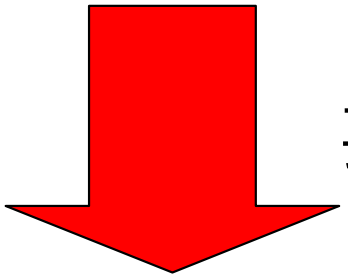
実トラヒックの短いパケットを想定
トラヒックレートが高いところでドロップが多すぎる
本当に見たいときに実用的性能が出ない

性能比較 まとめ(1) I社 e1000

- フレーム長 1518byte
  - ほとんどキャプチャ可能
- フレーム長 64byte
  - 140Mbps から急激にドロップ, CPU負荷率 100%
- フレーム長 200byte
  - 430Mbps からドロップが発生,
    CPU負荷率 100%@440Mbps
- 実は 約275kpps がドロップ発生の条件
- 結論 : I社 e1000 では …
  - Non-Sampling は達成不能

性能比較 まとめ(2) GigaPcap

- GigaPcap では ...
  - フルレートパケットキャプチャが可能
  - CPUパワーの確保が可能
    - 最大CPU負荷率 39%@1Gbps/64byte



要件を達成!!

- 結論：GigaPcap なら ...
  - Non-Sampling Flow Inspection を達成可能

結論と展望

- 結論
  - GigaPcap を使用すれば ...
  - Non-Sampling Flow Inspection が実現可能
- 発展
  - Non-Sampling NetFlow Exporter を実現
  - 次は sFlow, IPFIX 対応
  - Hardware Filter や 高度なリアルタイム分析
- 展望
  - 10GbE 対応
  - 分析アプリケーションの対応を増やす