Flow Inspection Project

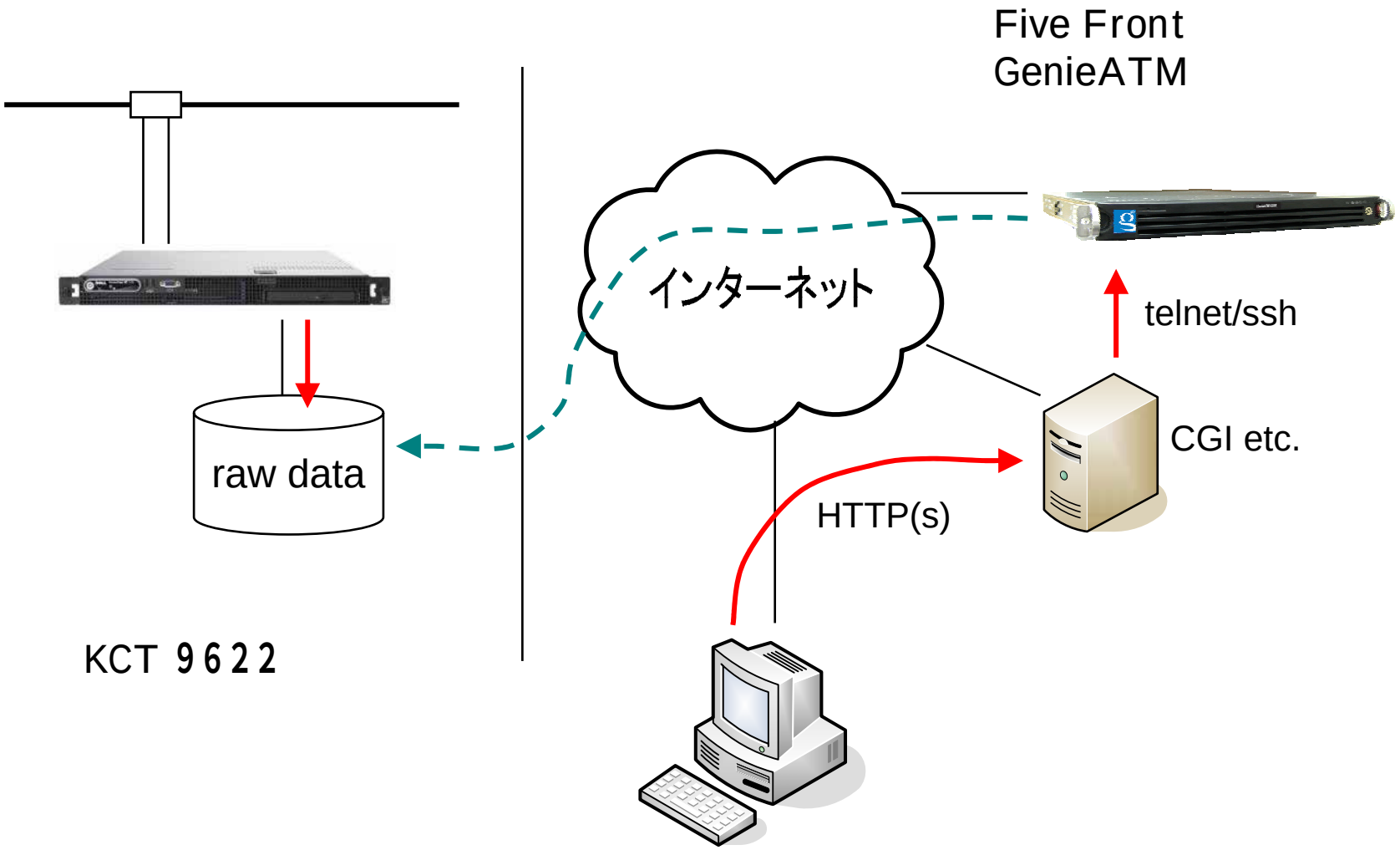
KCT Corp. Kaihei Koyama

モチベーション - 1

- **保険としての要求**
  - やっぱり、フルキャプチャー出来る環境 (機械) は欲しい。
    - 昔のトラフィックなら、楽勝だったんだけど。
    - どのような問題も必ず解決出来る保証は無いけど、フルキャプチャー出来ないから気づかないというのは悔しい。
  - 保険として検討できるコストで導入可能になりつつある。
- **BOTによる攻撃などへの対策工数を減らしたい**
  - サンプリングでは不可能な検出や対策も可能ではないか。
    - 対処療法よりも進んだことが出来ないか？
- **トラフィック分析活用し、ユーザーに有益なイベントを打ちたい。**
  - コスト的にコレクターの導入を断念 (延期) した経緯あり。

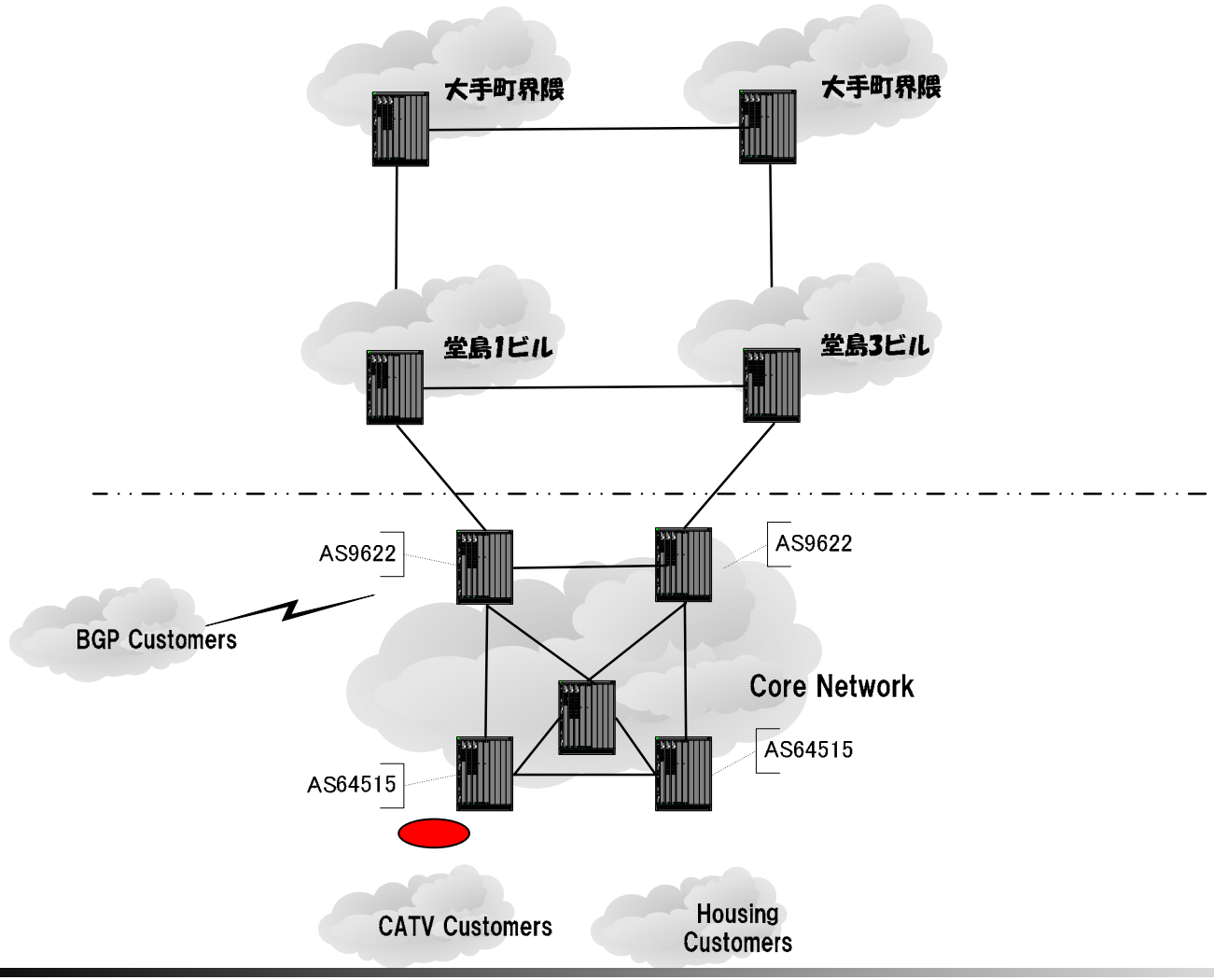
モチベーション - 2

- コレクターのＡＳＰモデルが始まる？



導入 - 1

ネットワーク構成



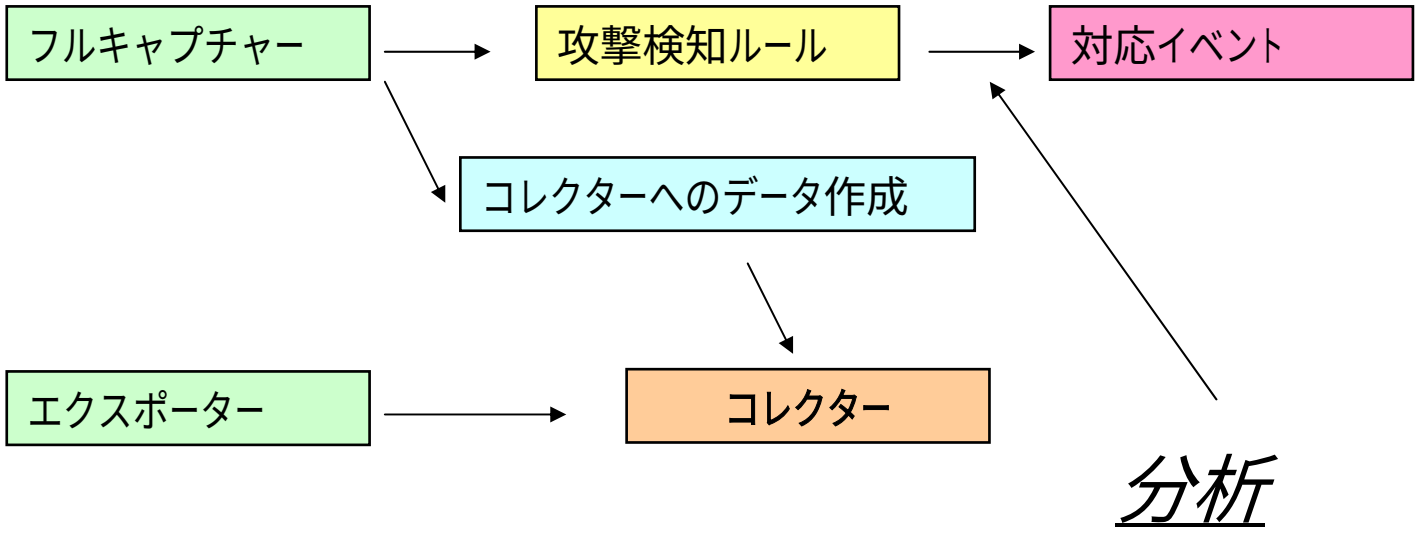
導入 - 2

- Mirrorさせる場所に結構悩む。
  - 対外接続に近い所。
  - カスタマー収容機器に近い所。
  - 既にCopperでは辛い。
  - 遠隔地にあるコロケーション場所とかとなると、回線の問題がある。
- 導入と稼動に関しては、一部バイナリのみではあるものの、LinuxでのOpenな環境であり、ある程度のサーバー知見があれば楽に導入可能。

使ってみて

- **保険という意味では、まだ…**
  - がん保険に入って一ヶ月でがんになるのは幸せ？
- **サンプリングでは出来ない攻撃検知と対応。**
  - ケースはかなり思いつく。実装の問題。
  - Module化して、ＩＳＰで共有したいですね。
- **傾向分析**
  - 知りたい傾向とか分析とか、ＡＳＰ利用で十分可能そう。
    - 今回はつけていないがやっぱりＢＧＰの情報も欲しい。
    - アプリケーション別トラフィック傾向、時間帯別の傾向。必要があって外へ２５番が出ていってるのか、ＳＰＡＭか？とかを確認。
  - 傾向分析の過程から、一定のルールでフルキャプチャへ。
    - 最初のルール作り。
    - ルール化出来れば自動化へ。攻撃検知と対応のルールとして標準化されていくものもあるだろう。

まとめ（運用イメージ）



まとめ - 1

- ISOでは無いけど、PDCA (Plan Do Check Action) の循環型サイクルにのせたい。
  - ハコもの、自動化は、人が循環型サイクルを運用するためのサプリメントみたいなもの。
    - 週に１２レッスンはエアロをしている僕には、通常の食物摂取だけでは体を維持出来ません。サプリメントですけど無いと困る。
- ホスティングやサイト運営をしているハウジングユーザー向けのオプションサービスとしても使える。
  - フルキャプチャーする方はFree版もありかな。トラフィック次第。
    - Deviceメーカーもkernel driverを書いてくれるようになってるし。
  - それ以外の仕組みが同じリソースで出来れば。

まとめ - 2

- コレクターのＡＳＰモデル。
  - データの受け渡しは要検討。
  - 利用性はＡＳＰタイプでも気にならない。
  - お金があれば購入？
  - ルールとか分析ポリシーとかリソース共有のメリットがあれば、ＡＳＰサービスの方がうれしいかも。
    - 対外接続料金のオプションみたいに契約出来ればもっとうれしい。