IRS23発表資料

SDNのセキュリティ

さくらインターネット株式会社
研究所 大久保 修一
<ohkubo@sakura.ad.jp>

最近のDCネットワークの要件

1. コンピューティングリソースのプール化
   – クラウドサービス、マルチテナント
2. プラットフォーム化
   – サービス間ローカル接続
3. ディズアスタリカバリ
   – 拠点間ローカル接続
4. モビリティ
   – ワークロードの分散、VMのライブマイグレーション等
5. オンデマンド、セルフサービス
   – 即時提供、設定の自動化

Why SDN?

- 従来のVLANをベースとした物理ネットワークの限界
  - VLAN数、VLAN ID数、FDB(MACアドレス数)
- 数万規模のノードをシームレスに扱え、柔軟で即時に構成変更可能なネットワークが望まれる

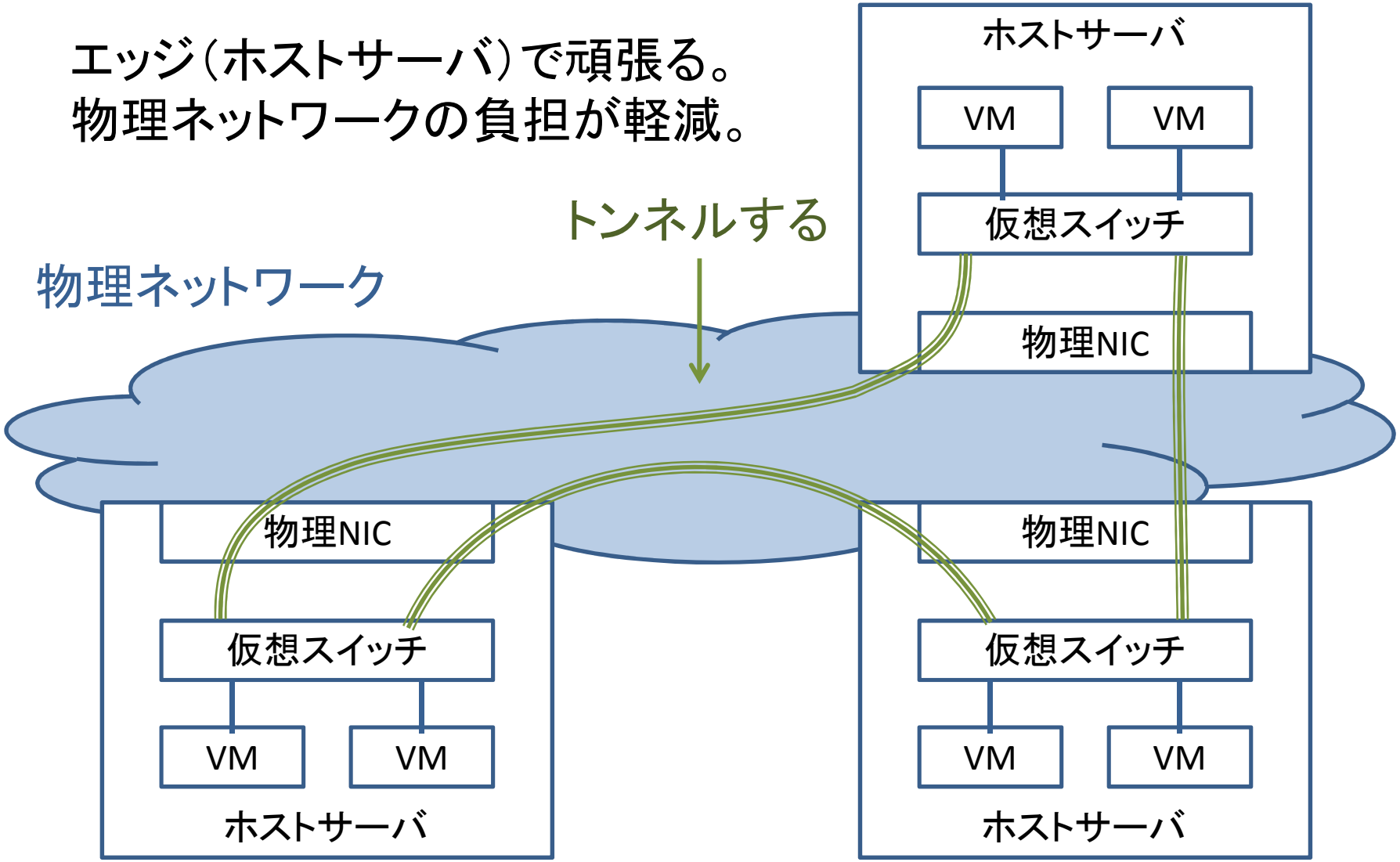
今後の方向性は？

- L2拡張
  - Trill, SPB, PBB-EVPN
- SDN
  - オーバレイ方式
  - Hop-by-hop OpenFlow
  - その他

今回は、こちらをモデルケースにセキュリティを考えてみる

オーバレイ方式とは？

エッジ（ホストサーバ）で頑張る。
物理ネットワークの負担が軽減。

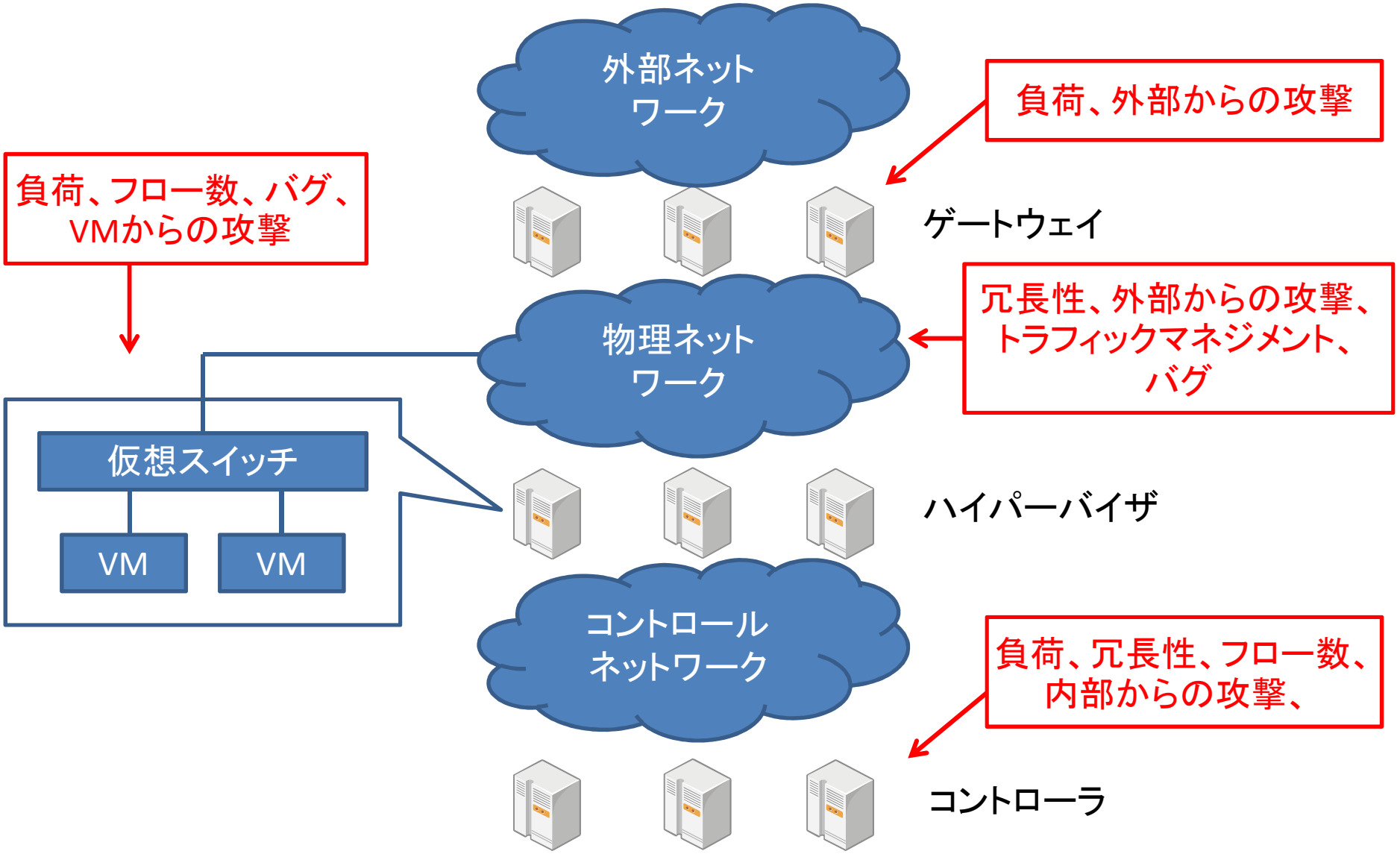


ただし・・・SDN導入で全て解決か？

- 答えは「NO」

- 実装上、運用上新たに生じる課題もある。

SDNセキュリティ課題マップ



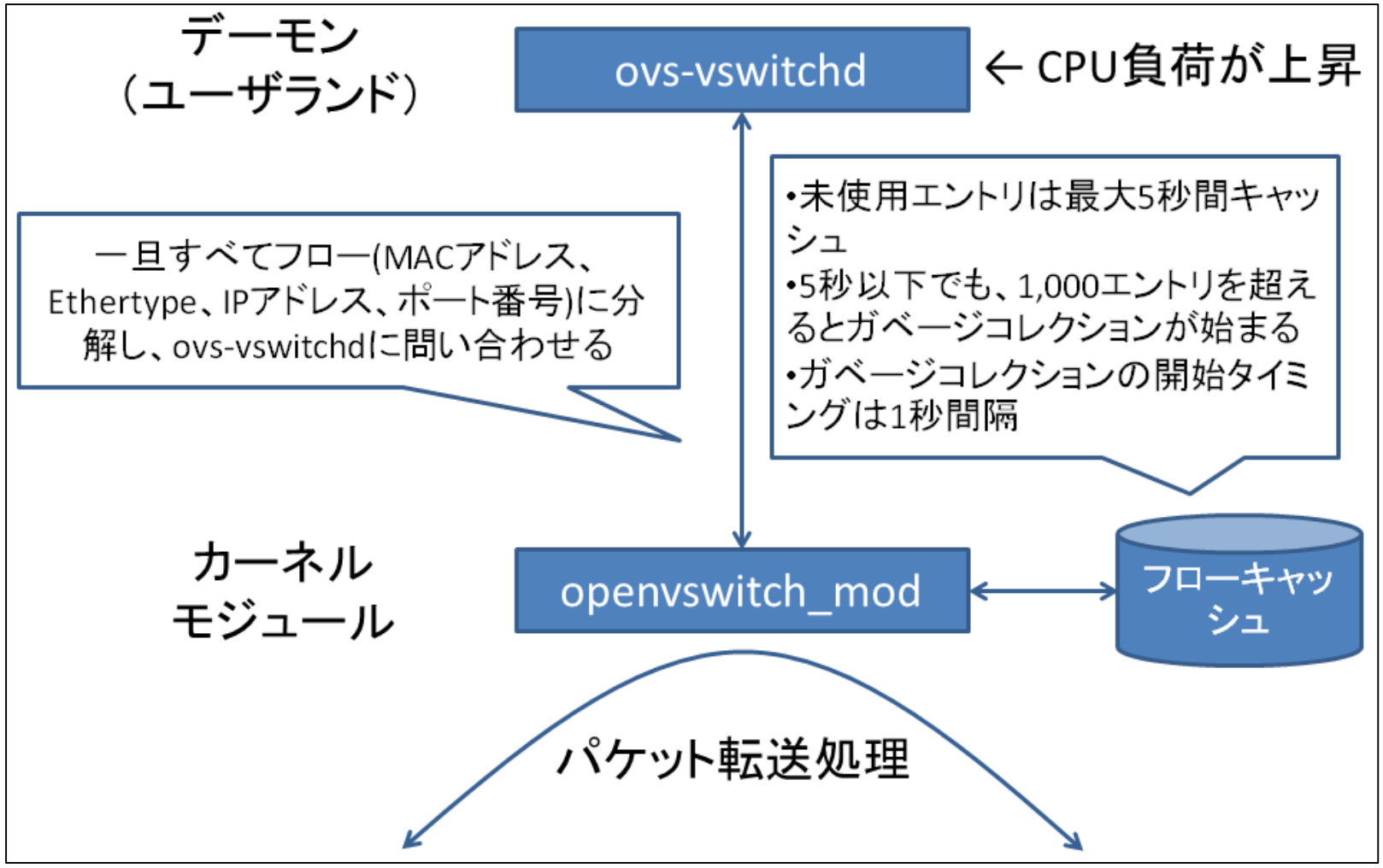
今日のお題

- （1）フローテーブルの爆発問題
- （2）セキュリティインシデント対応

（1）フローテーブルの爆発

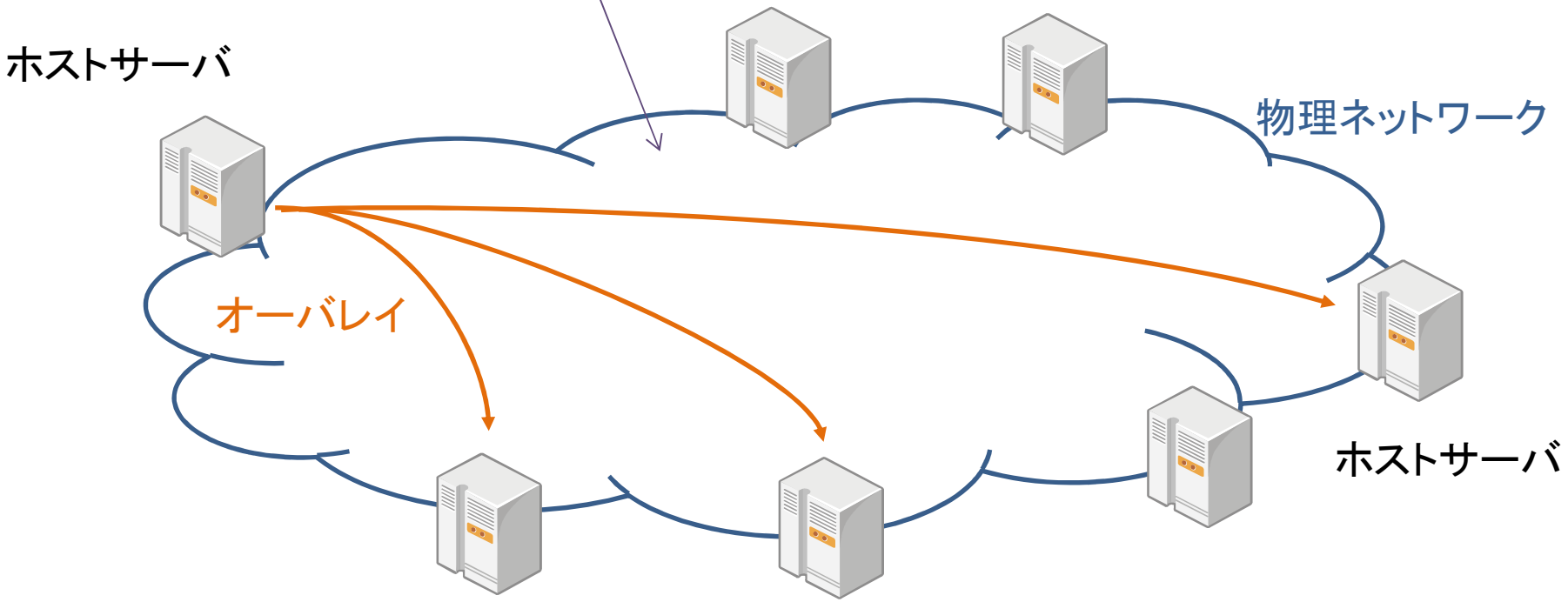
- フロー単位での制御は現実的？
- Open vSwitch利用環境での弊社内インシデント発生例
  - DoSアタックなど、大量のフローが発生すると、転送性能が極端に低下する
  - 同一ホストの別のお客様のVMに影響が及ぶ

参考資料：hbstudy発表資料より抜粋



（2）セキュリティインシデント対応

物理ネットワークでは、カプセリングされて中身が見えない。
仮想トポロジは、刻一刻と変化する。
→ 従来のフロー管理、トポロジ管理手法では後から
　追跡ができない。



こんなケースにはどう対処？

- 仮想ネットワーク内の疎通障害
  - お客様申告→事業者側での調査は可能？
- 外部からアタックを受けた
  - オーバレイネットワーク上でどこからどこに流れたのか？
  - 送信元IPアドレス等の追跡はできるのか？
- お客様にスプーフィングされてしまった
  - どの仮想ポートで、どんなIPアドレス、MACアドレスが使用されたのか？
- 仮想ネットワークのトポロジ、トラフィック情報の履歴を保持する必要がありそう・・・

話者紹介

- 石黒 邦宏氏 (株式会社ストラトスフィア)
- 永尾 禎啓氏 (株式会社ストラトスフィア)

- よろしくお願いします！