# レンタルVPSでのネットワーク分離について調べてみた件

(JANOG57.5 LT 2026/06/19)

スパークスシステムズジャパン 若梅 友則

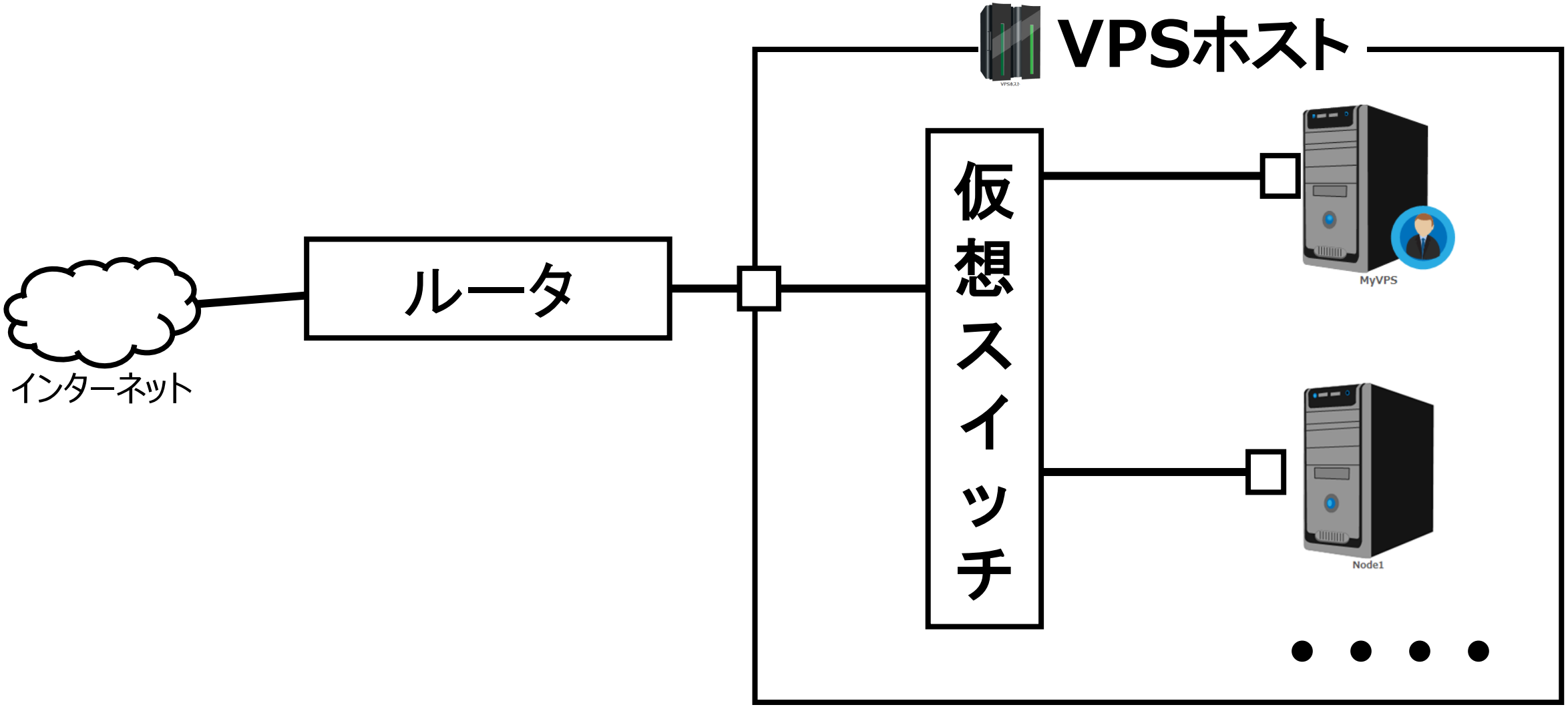
SparxSystems Japan Co., Ltd.

# 自己紹介・背景

- 名前：若梅 友則
- 所属：スパークスシステムズジャパン株式会社
  - ➢UML・SysMLモデリングツール等の開発支援ツール販売
  - ➢オンライン販売・オンラインサポート（電子メール）
- E-mail: wakaume@sparxsystems.co.jp
- サーバ運用・管理 実施
  - ➢**ユーザ（ネットワーク運営側ではない）**
  - ➢サーバ（DNS, Web, Mail）は運用中

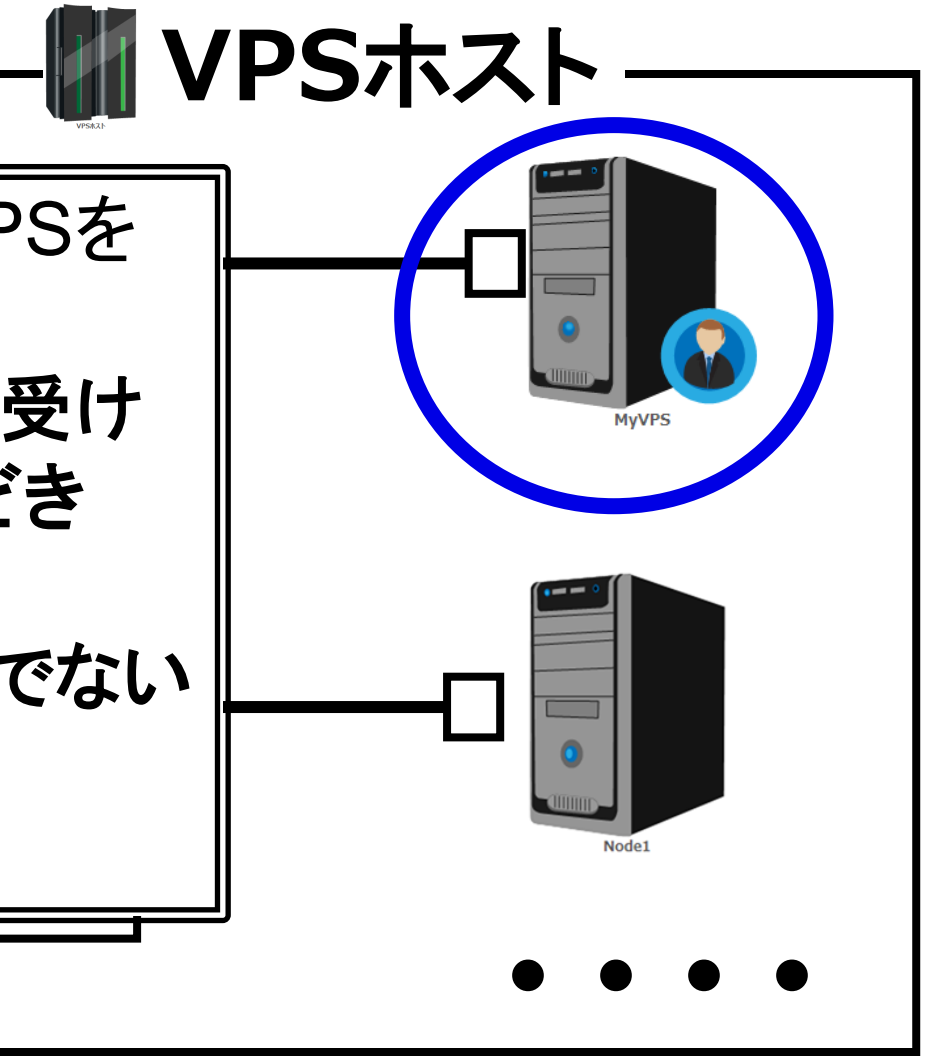
# 前提ネットワーク(1)

# 前提ネットワーク(2)



# 経緯

- 業務上いくつかのVPS事業者のレンタルVPSを単独で利用中
- とあるレンタルVPSで**「SYNフラッド攻撃」を受けたことがあったので、iftopコマンドで、ときどきネットワーク監視を実施**
- **iftopコマンドで、src/dest両方自サーバIPでないユニキャストパケットが見えた**
- tcpdumpコマンドでパケット取得で確認



# 確認コマンド・結果

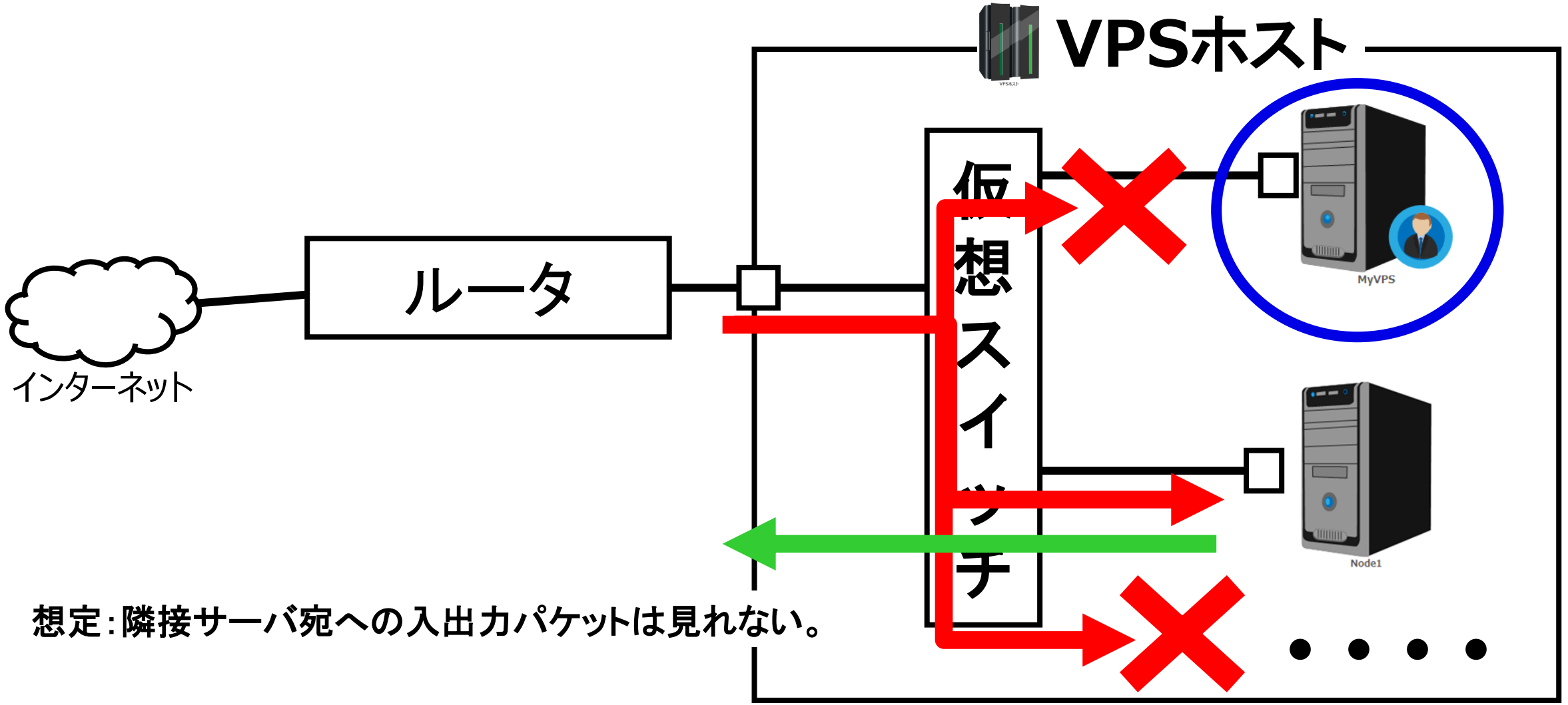
- tcpdump -w tcpdump.dmp not host (自IP) and not ether broadcast and not ether multicast
- Wireshark
  - キャプチャフィルタ: not host (自IP) and not arp

- **いくつかのVPSサービスで、隣接ホストへのパケットをキャプチャできてしまった (Flags [S] / [SEW] / [P.] / [.] / など)**
- もちろんキャプチャできないVPSサービスも存在

# キャプチャ例

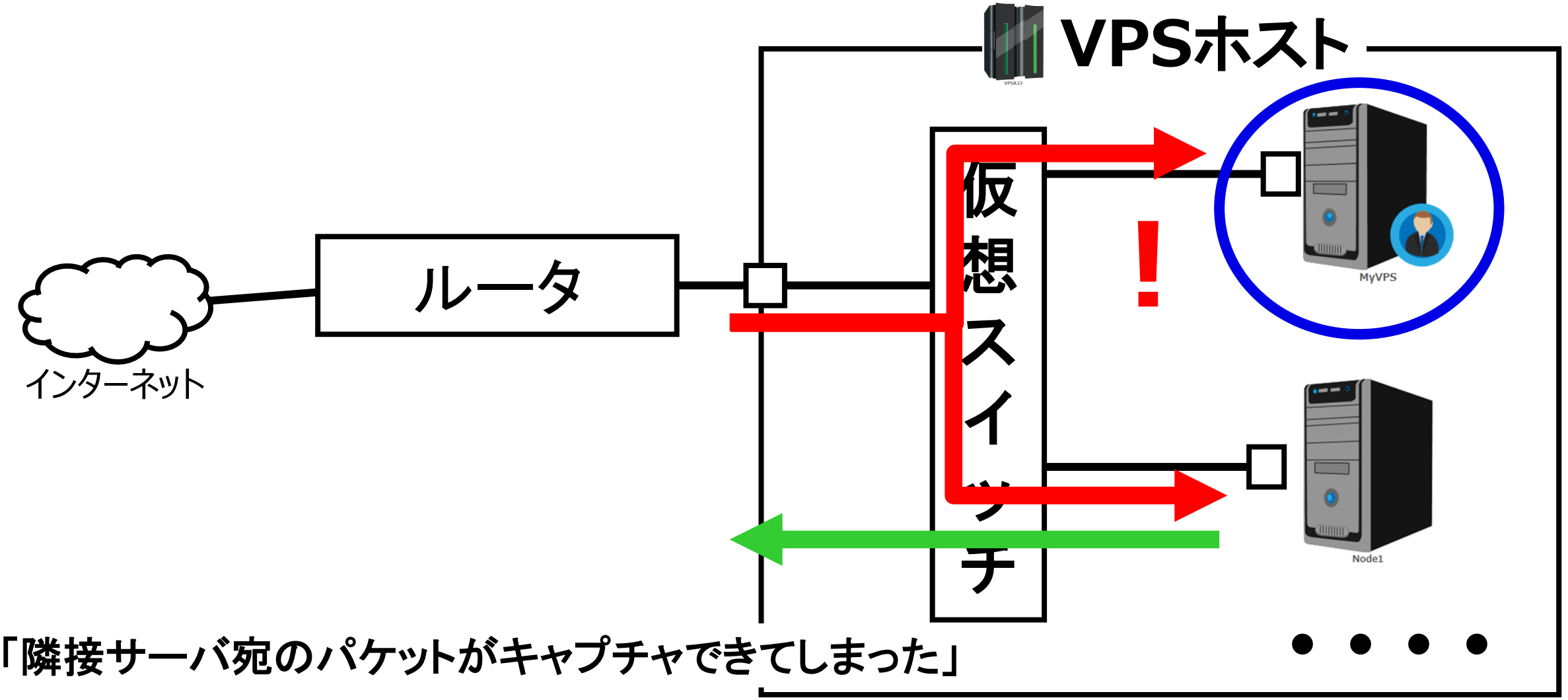
- 13:31:09.862830 IP XXX.XXX.83.48.18229 > AAA.AAA.AAA.AAA.**ssh**: Flags [S], seq 2543821898, win 1025, options [mss 1460], length 0
- 19:27:52.020981 IP XXX.XXX.185.241.11689 > BBB.BBB.BBB.BBB.**smtp**: Flags [S], seq 4047428906, win 65535, options [mss 1460,sackOK,TS val 2019603095 ecr 0,nop,wscale 9], length 0
- 17:10:26.368337 IP XXX.XXX.156.72.52386 > CCC.CCC.CCC.CCC.**domain**: 64206+ **A? dnsscan.CCCCCCCC.org.** (42)
- 17:57:38.651503 IP XXX.XXX.XXX.XXX.45678 > DDD.DDD.DDD.DDD.**http**: Flags [P.], seq 0:133, ack 1, win 229, options [nop,nop,TS val 3636153989 ecr 2328909035], length 133: **HTTP: GET / HTTP/1.1**

# 想定していたネットワーク分離状態



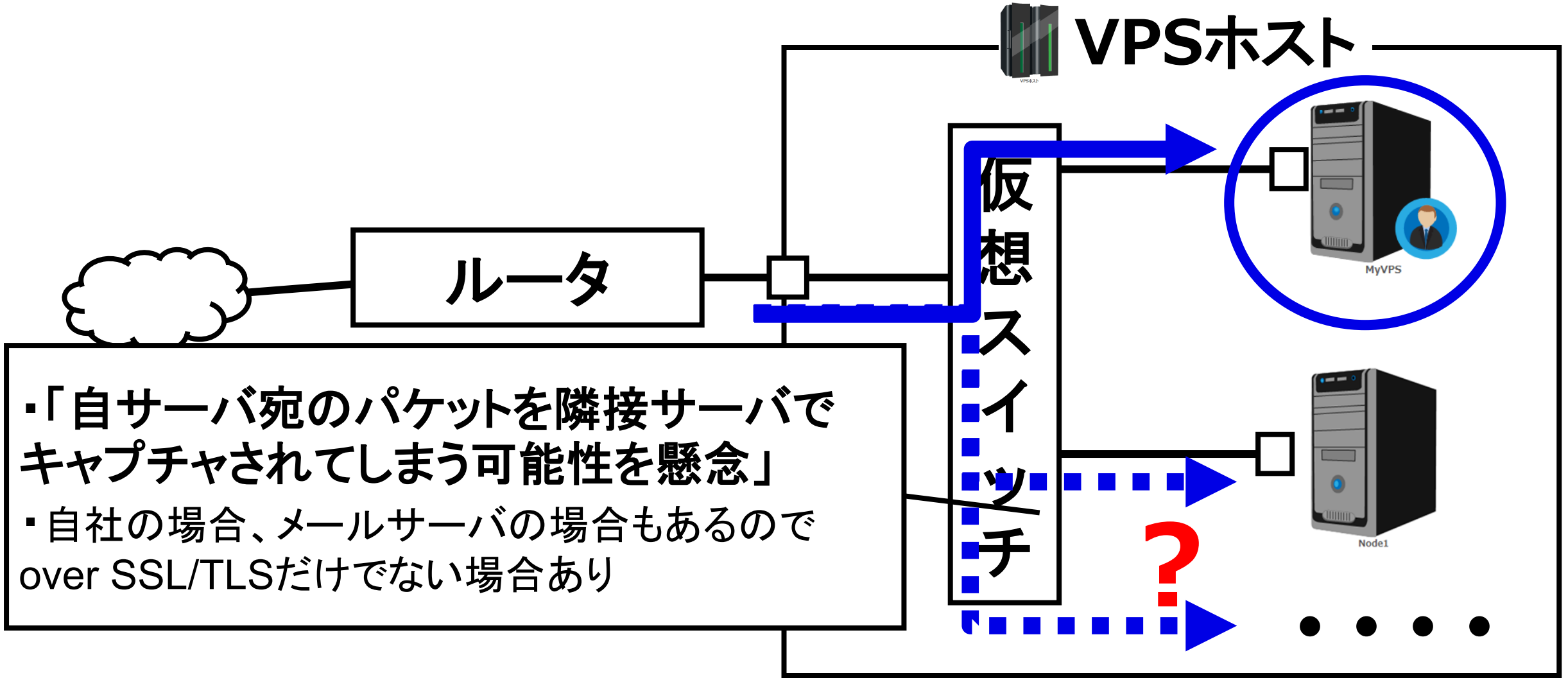

想定：隣接サーバ宛への入出力パケットは見れない。

# ネットワーク分離が不十分？




「隣接サーバ宛のパケットがキャプチャできてしまった」

# ネットワーク分離が不十分な場合の懸念



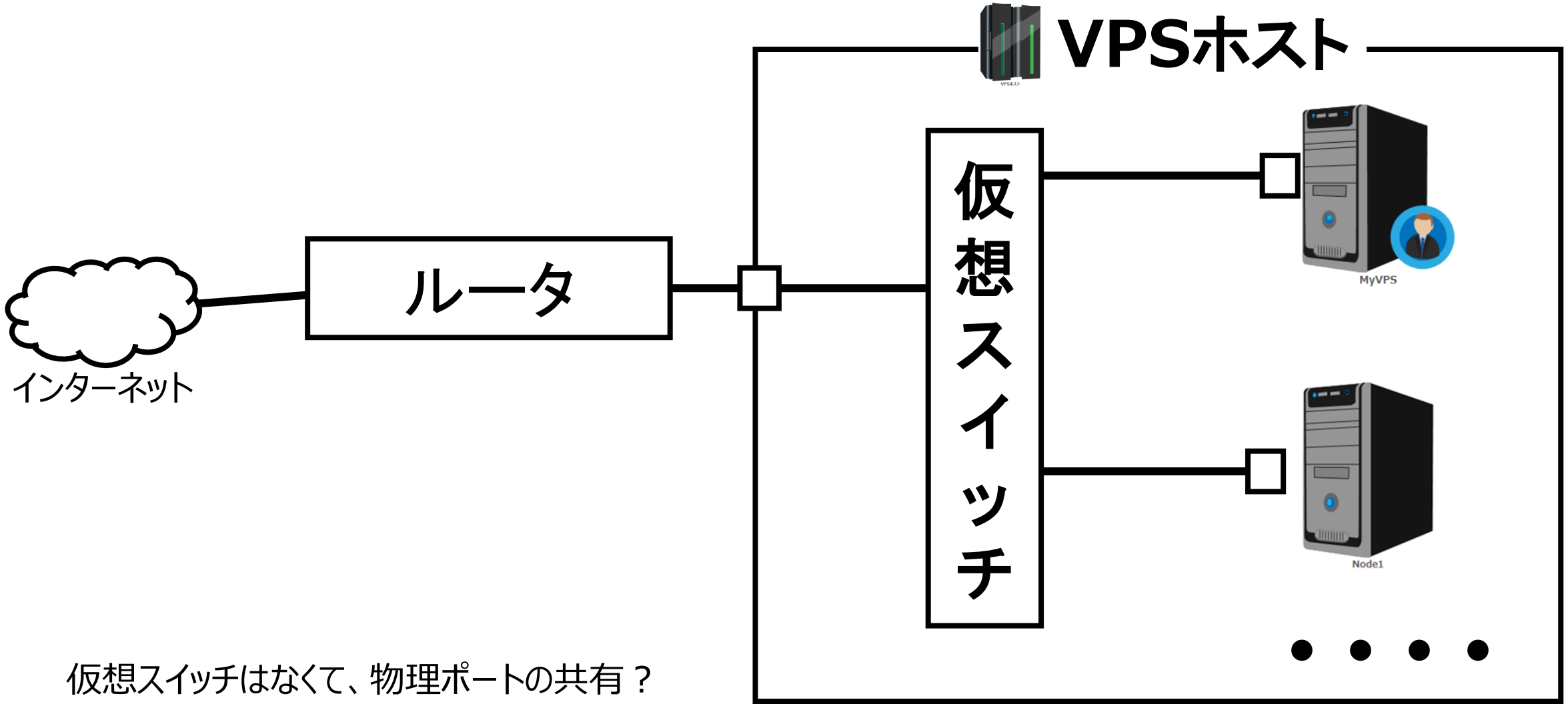

・「自サーバ宛のパケットを隣接サーバでキャプチャされてしまう可能性を懸念」

・自社の場合、メールサーバの場合もあるのでover SSL/TLSだけでない場合あり

# レンタルVPSでのネットワーク分離について調査(1)

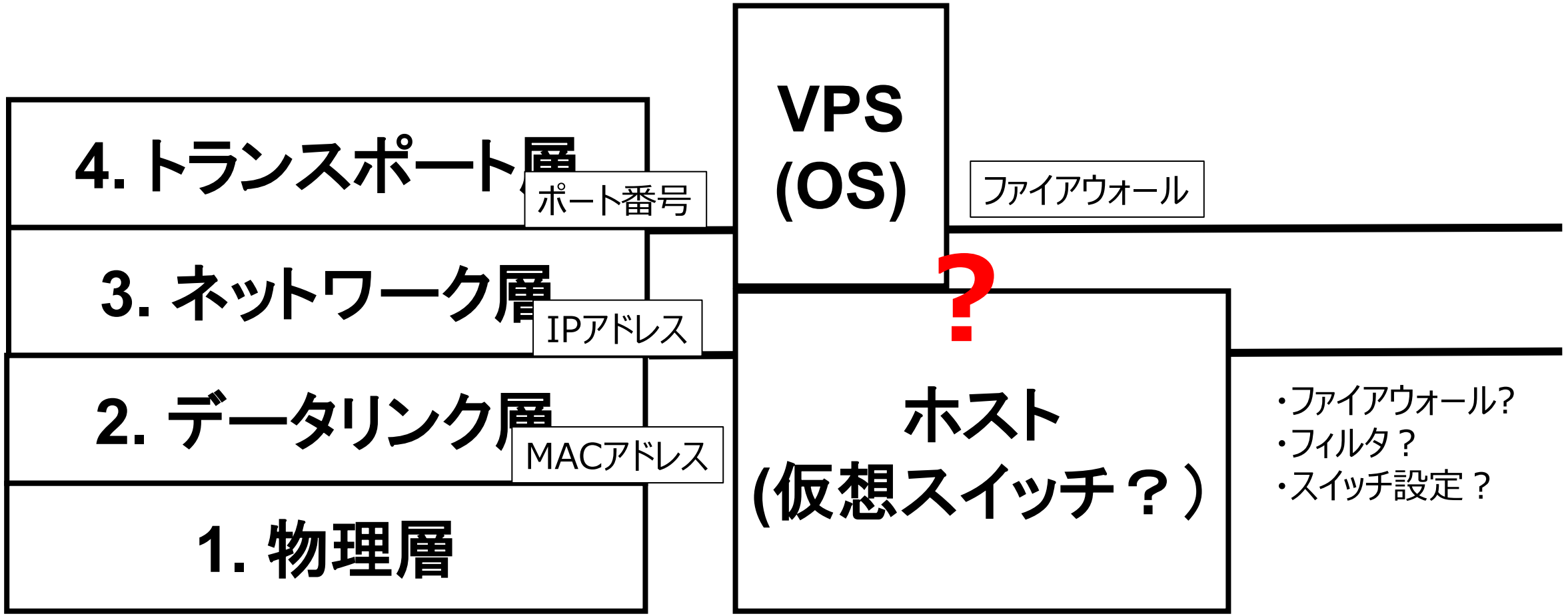
- 「自サーバ宛のパケットを隣接サーバでキャプチャされてしまう可能性を懸念」（セキュリティ）
- 調査
  - 技術的観点
    - ✓ネットワーク構成を整理
    - ✓検知可能性
  - 法的観点
    - ✓電気通信事業における通信の秘密の漏えい（他人が知り得る状態に置く行為）に形式的に該当する可能性の懸念
    - ✓違法性阻却理由（何かしらの同意・規約）が存在？
- 問い合わせ結果

# （技術的観点）ネットワーク構成




仮想スイッチはなくて、物理ポートの共有？

# （技術的観点）通信レイヤ


4. トランスポート層
ポート番号
3. ネットワーク層
IPアドレス
2. データリンク層
MACアドレス
1. 物理層
VPS
(OS)
ファイアウォール
?
ホスト
(仮想スイッチ？)
・ファイアウォール?
・フィルタ？
・スイッチ設定？

# VPS上でパケットキャプチャすることは？

- tcpdump コマンドを実行すること自体が、VPSの利用規約に反しないか？
- 一部の VPS サービスでは、利用規約上、明確に別ホストへの通信の傍受を違反とするケースもあるようですので、利用規約などの確認もお勧めいたします。(JPCERT/CC様)
- 各社サポートに確認したところ、
  - 各社様問題ない旨の回答
  - **安心した半面・隣接VPSで取得されていても対応できない？**

# (法的観点)通信の秘密

**総務省「通信の秘密（電気通信事業法第4条）FAQ」**

https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/th_faq.html

◇問2-2記載より

VPS事業者様取り扱い中という認識

◇問2-3記載より

over SSL/TLS で暗号化されていても、通信の日時・回数、発信IP・受信IPを取得できており、保護の範囲と読み取れる

◇問3-1記載より

他VPSで観測出来てしまうこと ＝ 他人の知り得る状態に置くこと に読み取れる

- 特定VPS宛パケットが他VPSで観測できてしまうことは、VPS事業者において、**形式的に「通信の秘密の侵害（他人の知り得る状態に置くこと）に該当し得る」のではないかと推測**
- **形式的に該当しているとの認識の場合、違法性阻却理由（何かしらの同意・規約）が存在？**

# レンタルVPSでのネットワーク分離について調査(2)

- JPCERT/CCに相談
- VPS事業者サポートへ問い合わせ

# JPCERT/CCに相談

- 「弊社が契約したVPSサーバで、電気通信事業における通信の秘密の漏えい（他人が知り得る状態に置く行為）の状況の可能性の懸念があり、ご相談です。」
- パケットキャプチャを付けて相談

- 回答
  - 「**技術的な観点**」ネットワークの**構成次第**
  - 「**通信の秘密の漏えいに該当するか**」JPCERT/CCでは**判断できない**
  - （事業者のサポート以外の）**別の報告先も把握しておりません**
  - 一部の VPS サービスでは、利用規約上、明確に別ホストへの通信の傍受を違反とするケースもあるようですので、利用規約などの確認もお勧めいたします。

# それぞれのサービスのサポートへ問い合わせ

- 問い合わせ内容　**（状況と懸念）**
  - 「他サーバ宛のパケットを、サーバ上で確認できてしまいます。これはセキュリティ上問題ないのでしょうか？」
  - 「自サーバ宛のパケットを他のサーバでキャプチャされてしまう可能性を懸念しております。」

# サポートの回答とその後

- **サービスA**
  - ➢**「状況を確認」「基盤側をチューニング」**
    - ✓隣接VPS宛のパケットは**キャプチャできなくなった**
- **サービスB**
  - ➢**「仮想ネットワーク構成上、想定内かつ正常な挙動」**
    - ✓再問合せ
  - ➢特に説明がなかったが、仮想ネットワーク構成を変更されたらしく
    - ✓隣接VPS宛のパケットは**キャプチャできなくなった**
- **サービスC**
  - ➢**「どうしても発生してしまう正常な動作」「フラッディング」**
    - ✓やり取り実施
  - ➢「機器パラメータの最適化（チューニング）中」/ 引き続きやり取り中
    - ✓**問い合わせ前よりは、非常に少なくなっている状況**

# 調査まとめ

- レンタルVPSでネットワーク分離は十分されているか？
  - **事業者様次第**
  - グローバルIP割り当てなので、相互通信はできなければならないので、サブネットで分離は容易ではないと推測
  - ローカルネットワークの設定も可能だと、複雑であると推測
  - 低価格VPSの場合、特に十分ではない場合があると想定が必要か？
  - VPSサーバ側で暗号化すればそこまで気にする必要はない？
- ネットワーク分離が十分でないと
  - **隣接VPSの利用者は、契約VPSのパケットをキャプチャ可能である可能性あり？**
  - **隣接VPSでパケットキャプチャされていても気づかない**
  - 隣接VPSの利用者は「通信の秘密」の対象外？
    - ✓ 悪意を持ってキャプチャされても、対応できない？
  - 隣接VPSでIPアドレスを重複されたらどうなる？

# 専門家の皆さんに確認したいこと

- **VPS事業者様側へネットワーク分離を求めるべき？**
  - ➢セキュリティ上、行ってほしい（ユーザとしては希望）が、**完全分離は難しいのかも**
  - ➢ 隣接VPS宛のパケットがキャプチャできてしまうことへの、**他の懸念点は？**
- **ユーザ側の対処案**
  - ➢**全ての通信を暗号化（over SSL/TLS）にする？**
    - ✓メール（ポート25/587)等をどうする？
    - ✓UDPは？
  - ➢別VPS事業者へ移動
  - ➢**他に対処案存在？**

# 他にも知りたいこと

- 今回の現象についての**相談先・相談窓口**は？
  - IPA:「受付可能な相談内容」でなさそう？
  - 総務省： 電話のみ？
  - 他は？

- 単独VPSのネットワークでネットワーク分離されている場合
  - ARPパケット必要？
  - HSRPパケット必要？

# まとめ

- レンタルVPSではネットワーク分離が十分ではないと思われる事業者様が存在していた
  - ユーザとして今後どうするかは検討中
- サーバにおける、解放ポートはすべて暗号化(over SSL/TLS)を前提にすべき時代か？
  - SMTPやUDPは悩み
- 以下について、ご意見・ご教授頂けましたら幸いです
  - **事業者様側へネットワーク分離を求めるべき？**
  - **ユーザ側の対処案**
  - **相談先・相談窓口**（事業者様サポート以外の）
  - 法的観点（レンタルVPS における「通信の秘密」の取り扱い）

# ご清聴ありがとうございました

ご意見・アドバイス・コメントなど頂けましたら幸いです。
・懇親会
・E-mail: wakaume@sparxsystems.co.jp