JANOG50 マネジメントNW野良BoF
監視NWどうしてる？

2022年07月13日
NTTPCコミュニケーションズ
大塚 悠平

DISCLAIMER

このスライドは個人意見を述べるものであり
所属組織を代表する見解ではありません

このBoFの目的

- 最近あまり扱われないマネジメントNWをテーマとする
- サービスやスケール、企業文化などにより思想や設計に違いがあるはず
- マネジメントNWに関するノウハウや悩みを議論・共有する

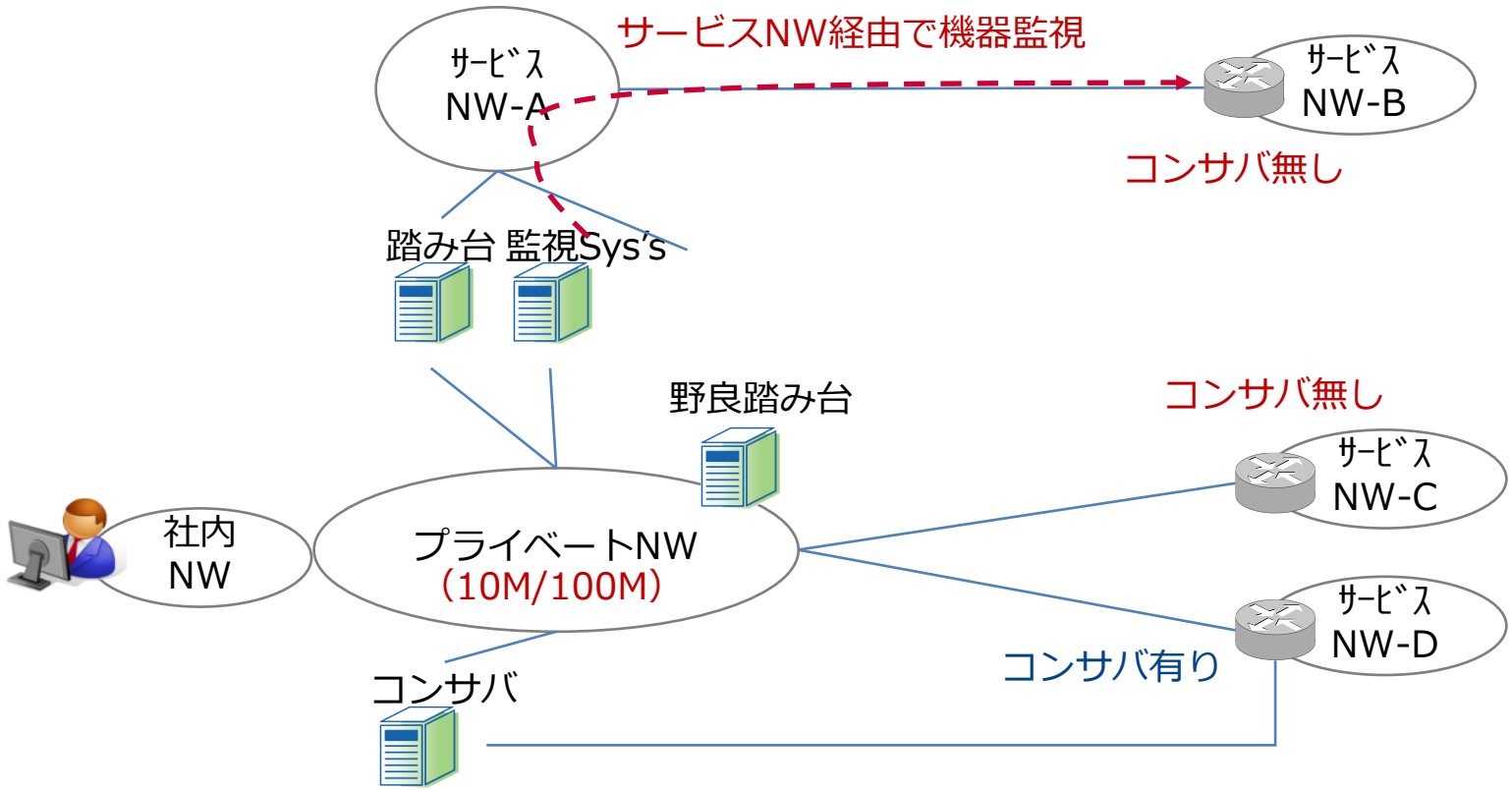
監視NWに関する悩みごと

- 監視NWにどこまでの性能や信頼性、接続性を求める？
- そもそも監視NW必要？
- サービストラフィックと監視トラフィック混ぜる？分ける？
- 機器の監視ポートを商用トラフィックのポートと混ぜる？分ける？
- 踏み台的なもの使ってる？権限設計どうしてる？
- Console/IPMIでさらに分けたりしてる？
- 物理機器とVMで監視方法分けてる？
- 出来るだけセキュアにしたいけど何をどこまで繋がせる？
- クラウド接続どうしてる？閉域接続？
- ACL/NAT困ってない？

事例紹介

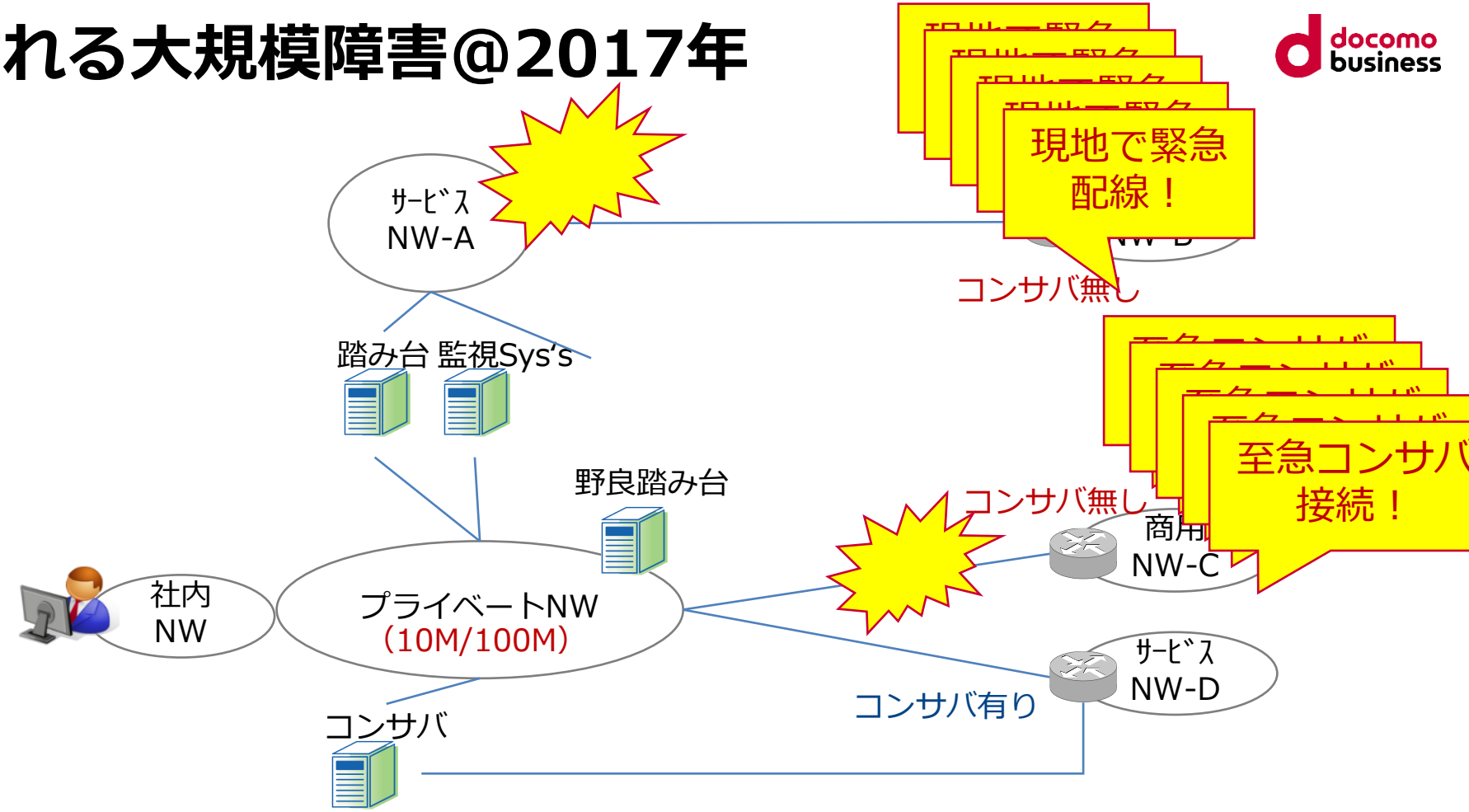
とある監視NW　～2017年頃

※この図に収まらない個別構成やHUB置いてるだけ的なパターンも複数有り



- サービスNW上経由で機器監視するパターン有り、シングルポイント有り
- 監視専用ポートの無いインバウンド監視多め、コンサバ接続あったりなかったり
- 野良踏み台の存在、証跡管理不可
- OSイメージ転送でトラフィックアラート出る低帯域なNW
- 監視NWというよりかは単なるプライベートNWだった

突然訪れる大規模障害@2017年



- とにかく制御出来なくなった
- 正常性確認や復旧対応が遅れた

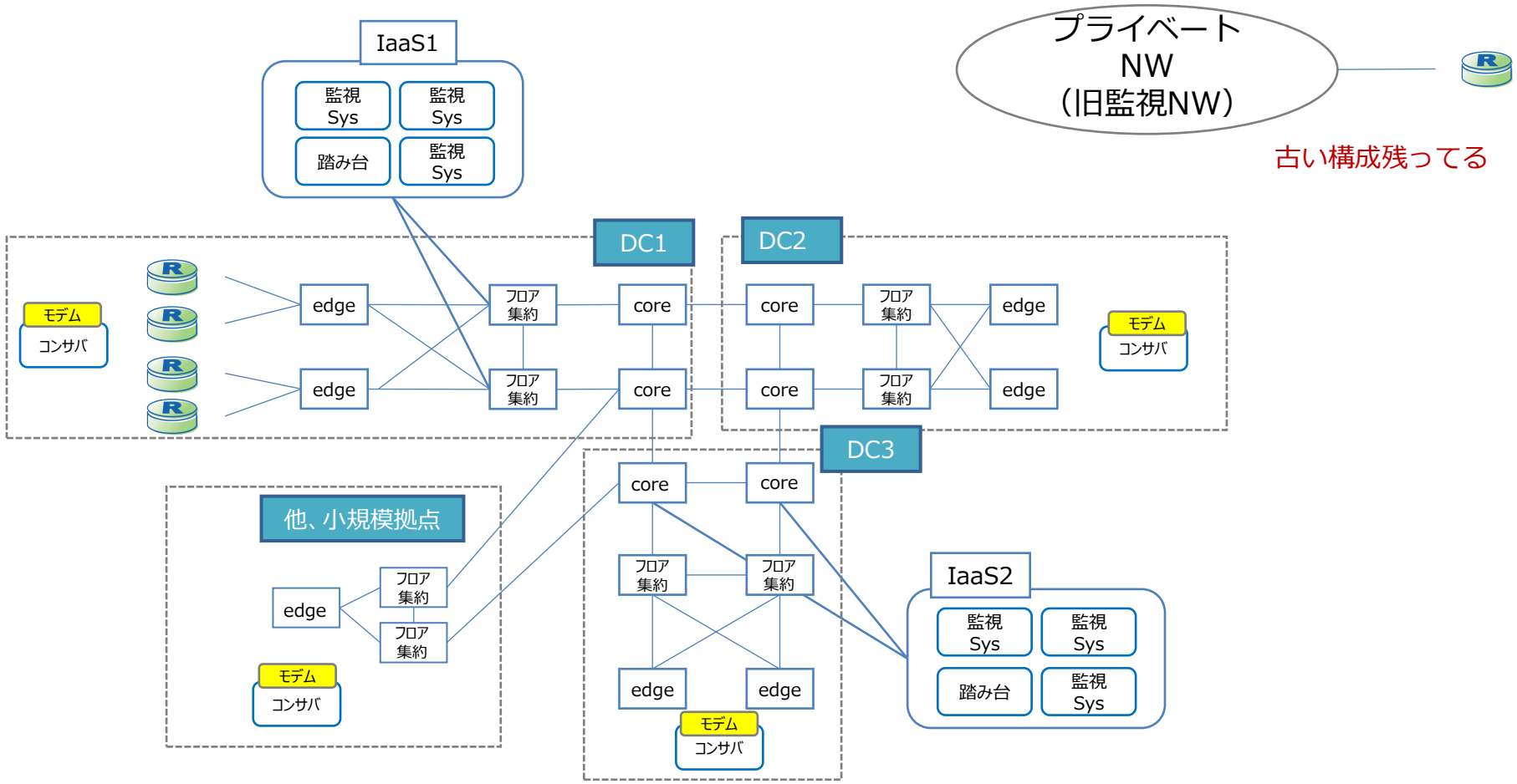
阿鼻叫喚

是正計画開始

- サービスNWの障害影響によりオペレーションを止めない
- 監視NWがコケても商用装置へログイン出来る手段を確保する
- 監視NWへ接続出来るシステムやユーザーを限定する
- 野良踏み台撤廃しNW機器へのアクセスを限定、証跡管理もキッチリ
- せめて1Gくらいに容量Up
- 安く作る

大規模障害後あるある

2018～

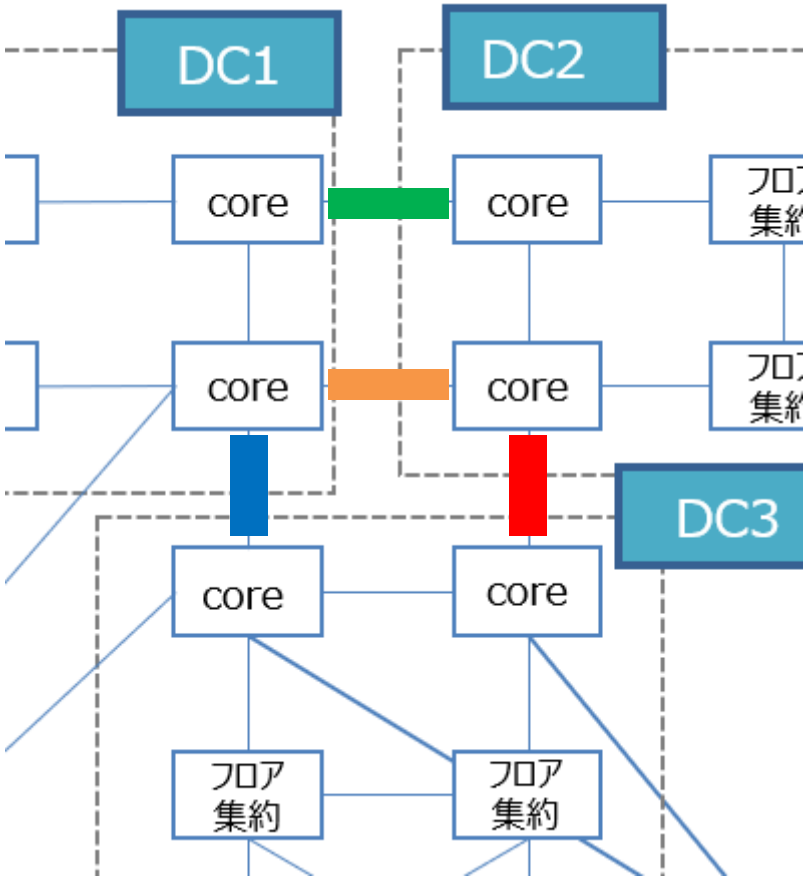


- 冗長構成、1G/10Gベース、ホワイトボックススイッチ採用
- コンサバも増やしてNW機器は絶対コンサバ繋ぐことにした
- 絶対踏み台踏むことにした

うまくいったポイント

冗長設計　DC間

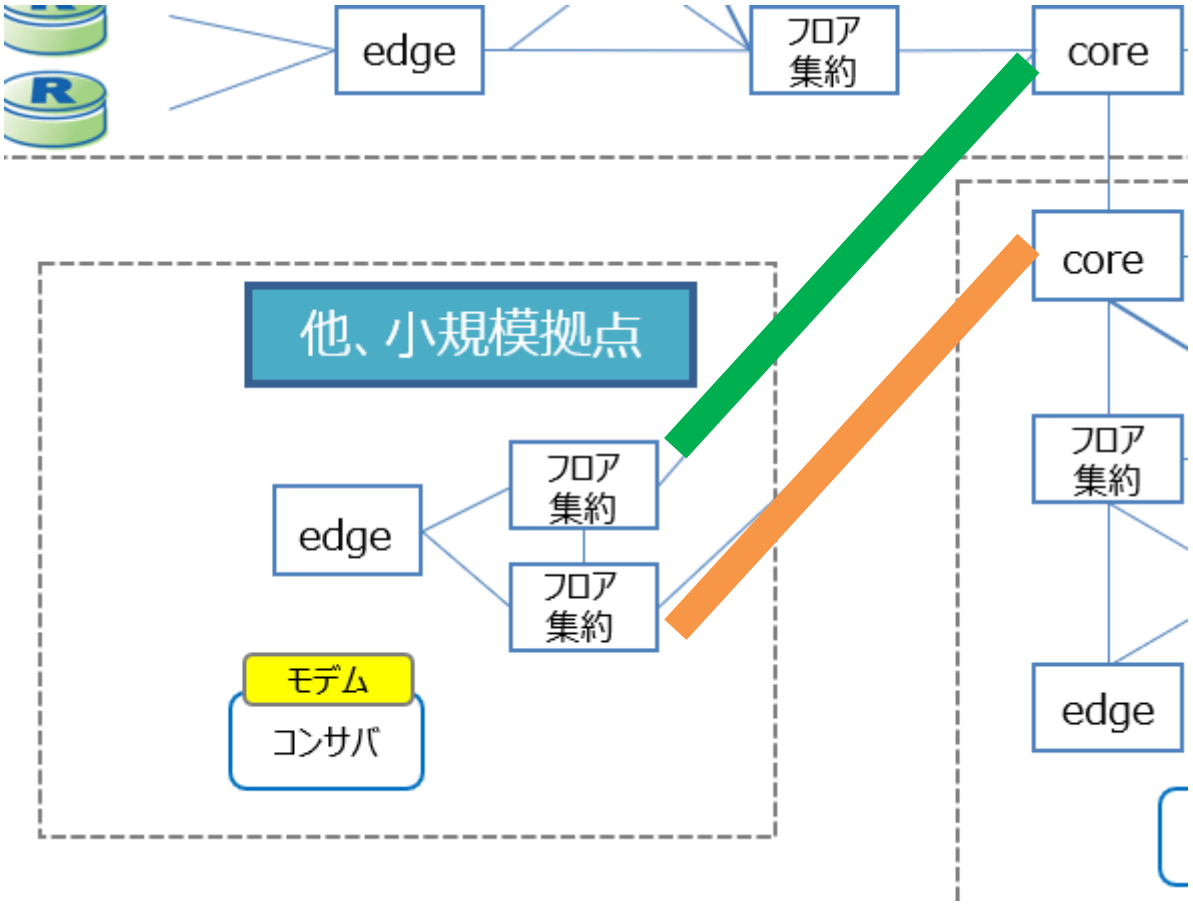
DF/WDMはサービス
NWとあいのり



L1異経路化（DF/WDM）

冗長設計　小規模拠点パターン1

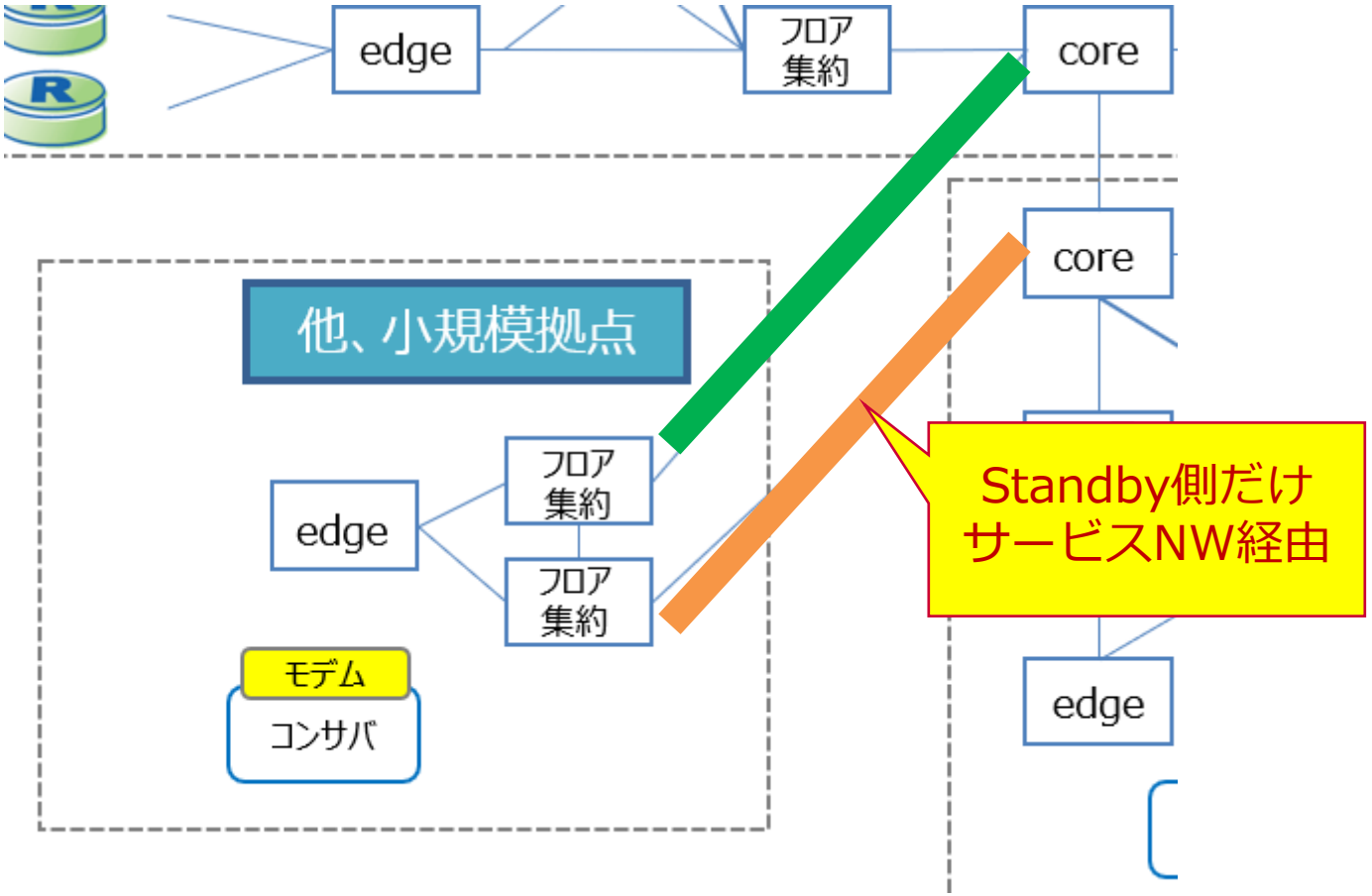
DF/WDMはサービスNWとあいのり専用線は新設



L1異経路化（専用線＆DF/WDM）

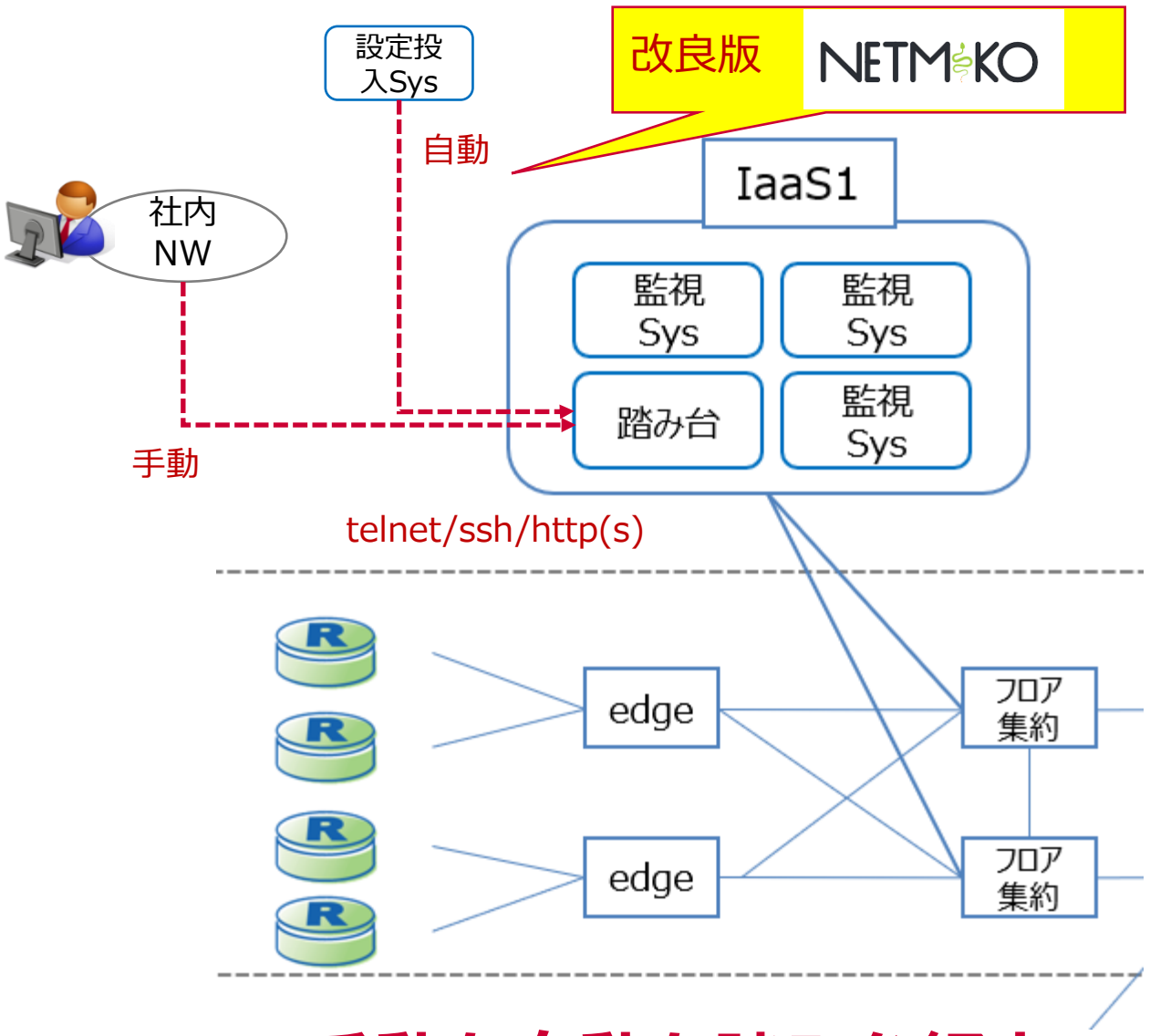
冗長設計　小規模拠点パターン2

DF/WDMはサービスNWとあいのり



L1異経路化（専用線＆サービスNW）

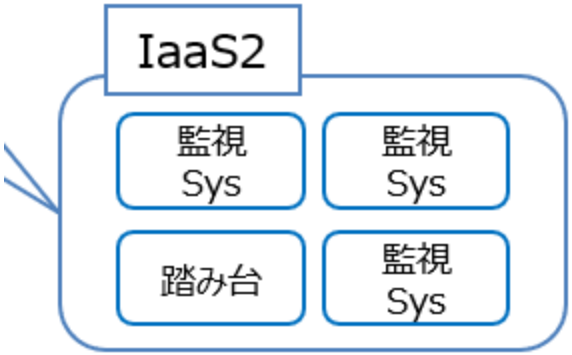
踏み台



手動も自動も踏み台経由

今後の検討ポイント

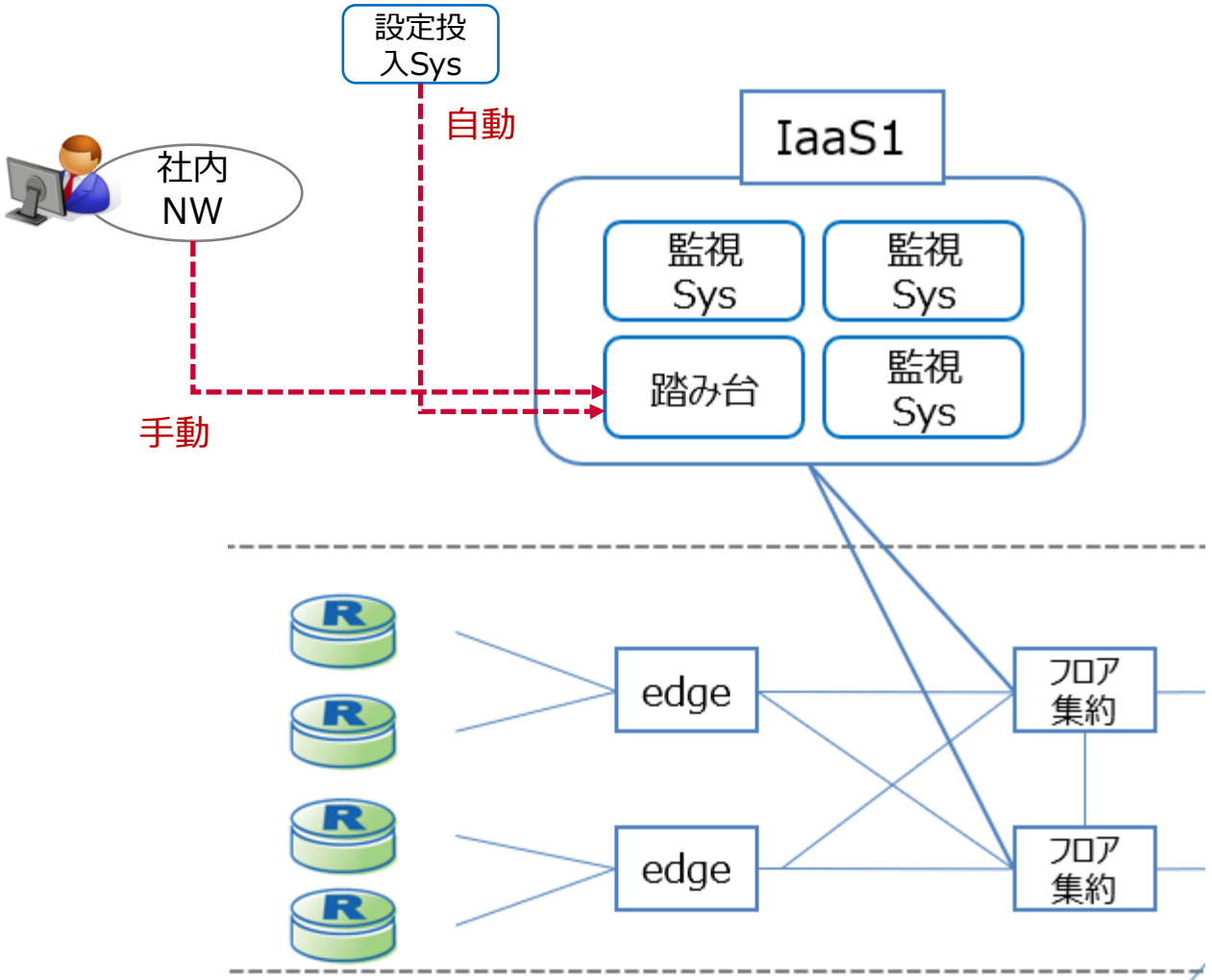
NW/SV監視統合



まだ踏み込めてない

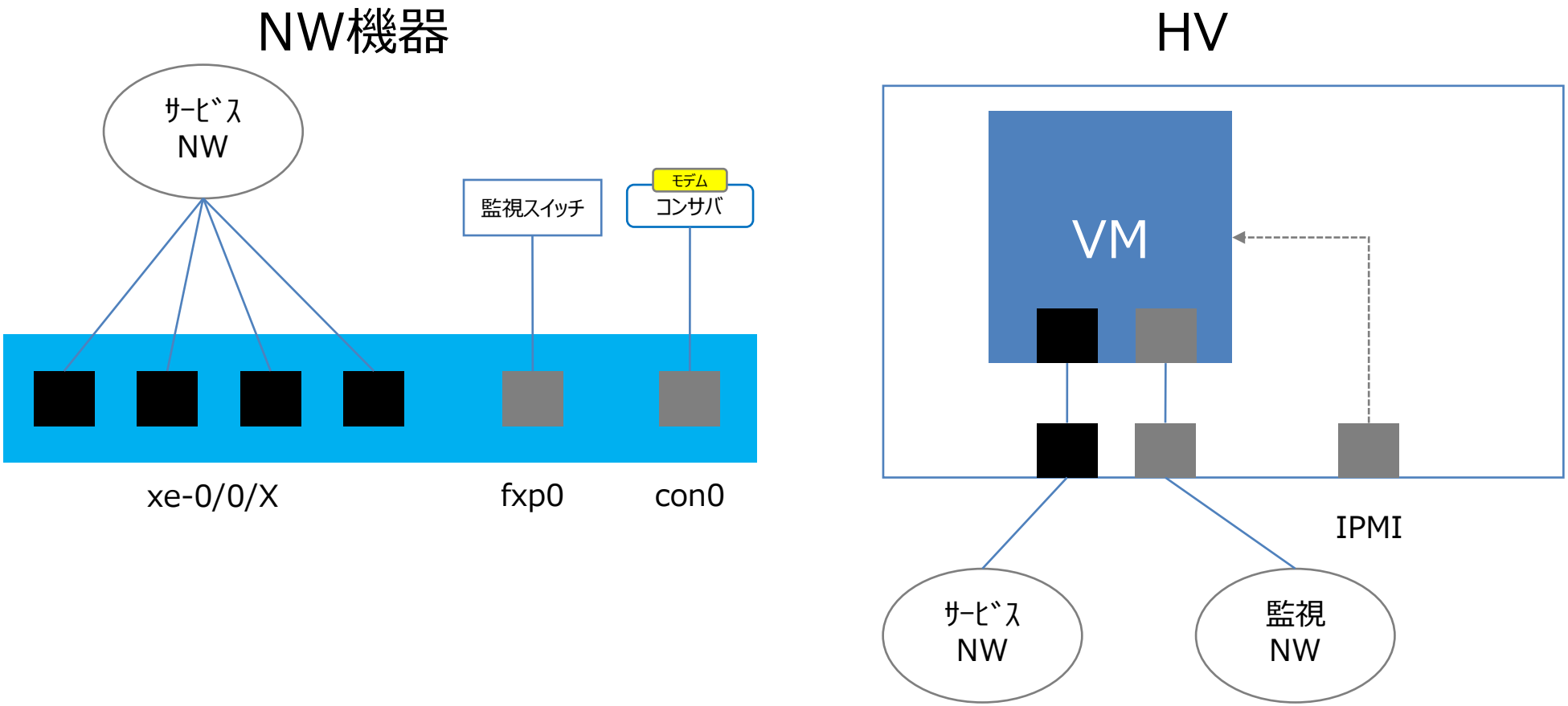
IaaS/サーバーの要件はNW機器と異なる？統合出来る？

踏み台どこまでProxyするのか問題



NETMIKO以外の対応、NETCONF/Telemetry, etc…
地味にNW自動化を阻害するポイント

機器種別毎の監視方法



NW機器のInbound監視構成撲滅する？

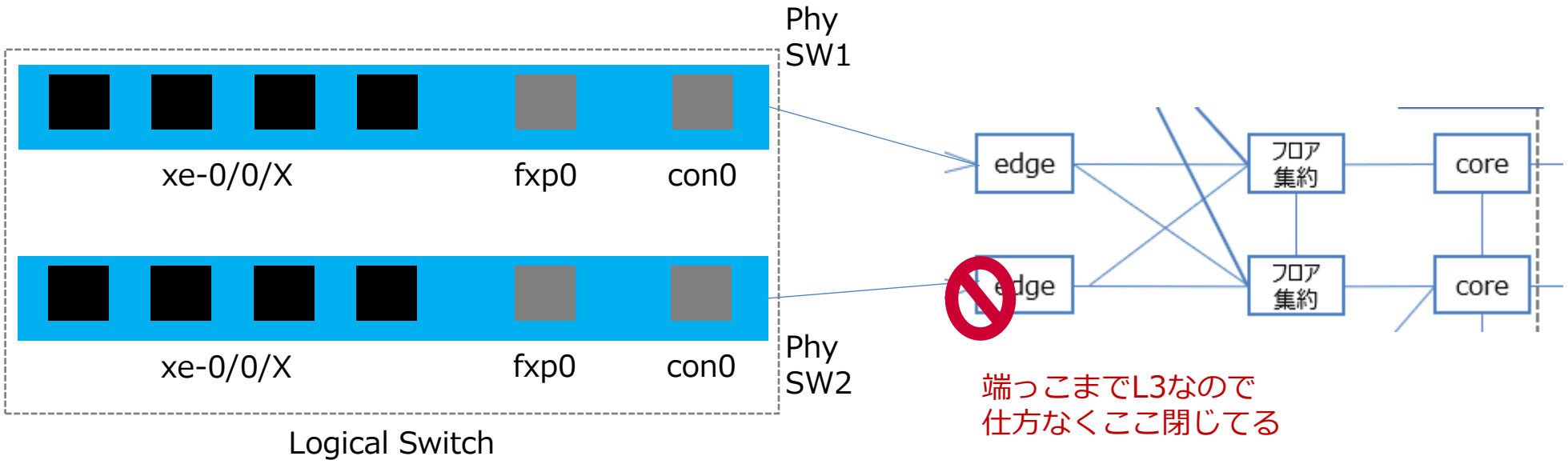
xFlow/inbound-Telemetlyなどはサービスネットワーク通す？

VMやHV、仮想アプライアンスとの監視方法違い？

なくなったらどうする？

モバイル使う？ラックの中まで電波入る？
モバイル使うなら他キャリア必須？
それとも潔くフレッツ引く？

スタッキング系NW機器の監視

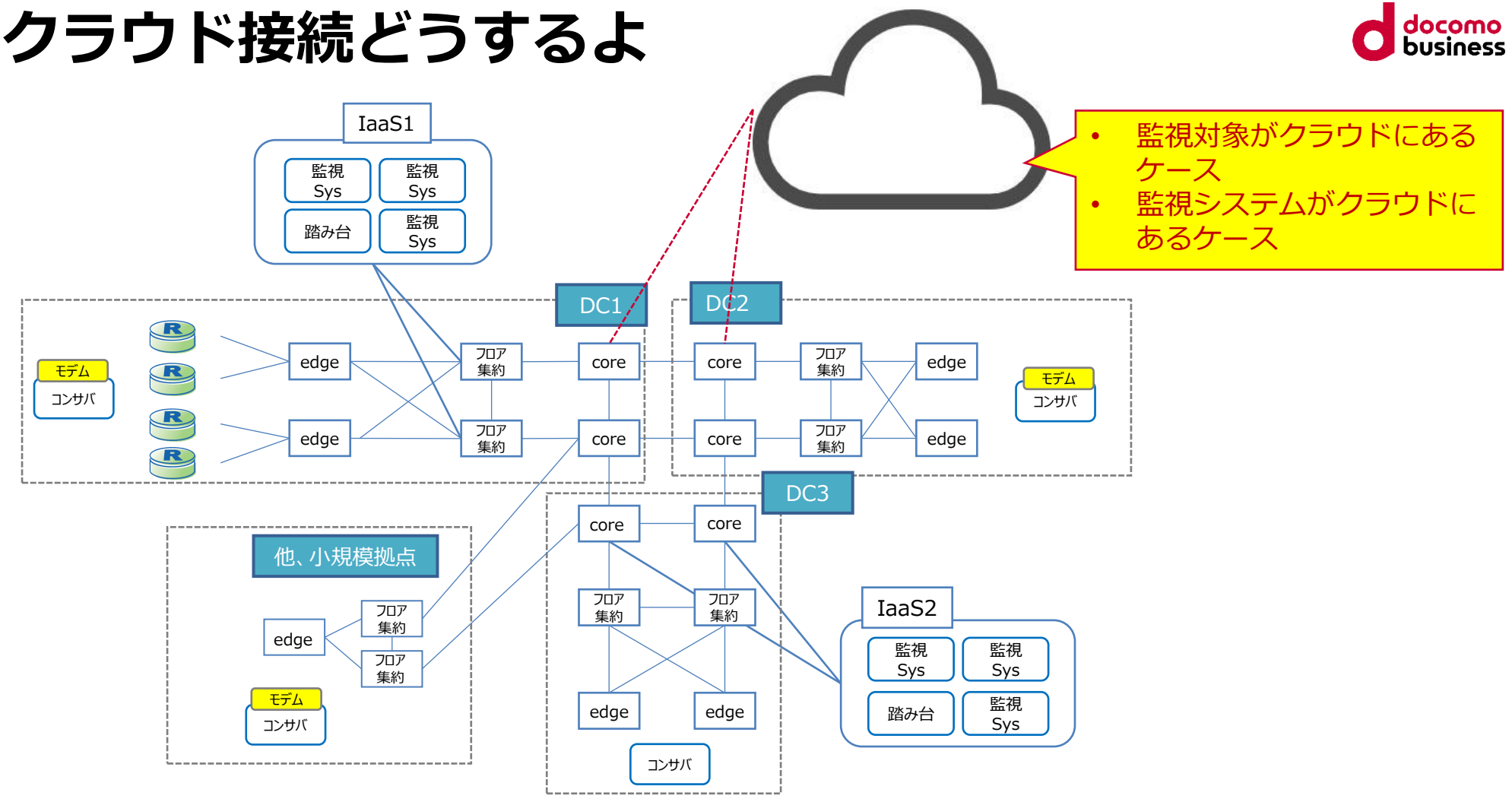


障害時の切り替え自動化する？L2 Overlayはやりたくない

IPv4プライベートアドレス空間逼迫問題

意外に足りなくなる、バッティングも多少ある
IPv6使えば解決？

クラウド接続どうするよ



- 監視対象がクラウドにあるケース
- 監視システムがクラウドにあるケース

インターネット経由？閉域接続？

オンプレとクラウドで監視をシームレスに繋ぐ？

まとめ

- 障害を機にシンプルな監視NWをコストミニマムに作った
- 基本オンプレ前提で設計思想もレガシーなまま
- DR/BCPやクラウド接続など複数の課題を抱えている

議論したいこと

- 監視NWにどこまでの性能や信頼性、接続性を求める？
- そもそも監視NW必要？
- サービストラフィックと監視トラフィック混ぜる？分ける？
- 機器の監視ポートを商用トラフィックのポートと混ぜる？分ける？
- 踏み台的なもの使ってる？権限設計どうしてる？
- Console/IPMIでさらに分けたりしてる？
- 物理機器とVMで監視方法分けてる？
- 出来るだけセキュアにしたいけど何をどこまで繋がせる？
- クラウド接続どうしてる？閉域接続？
- ACL/NAT困ってない？