Global ICT Partner
Innovative. Reliable. Seamless.

NTT Communications

監視網設計/運用の苦労あれこれ

NTTコミュニケーションズ
秋本 哲也

自己紹介

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

▼名前：秋本　哲也

▼所属：NTTコミュニケーションズ株式会社

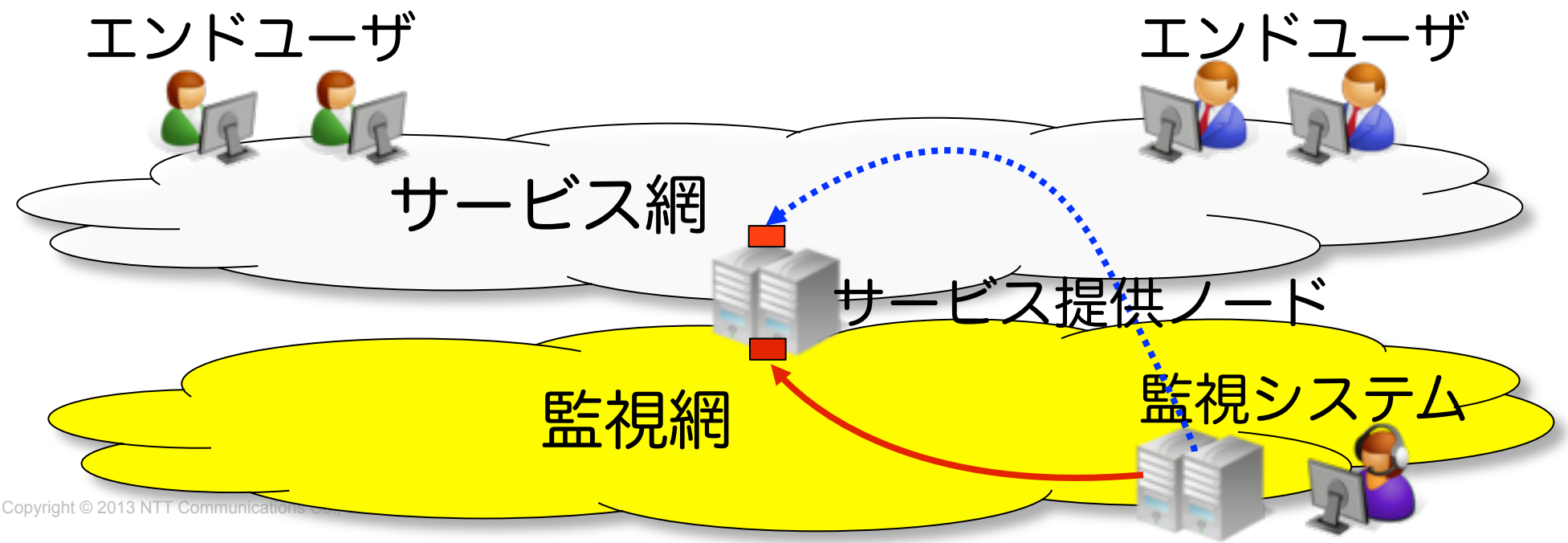
▼経歴：

- 1980年生まれ（S55）の32歳
- 2008年OCNやVPNの保守部隊で配線からBGPオペレーションまで保守現場を一通り学ぶ。
- 2011年保守の企画にて、オペレーション可視化、自動化の施策推進担当に異動。まず基盤となるネットワーク整備を担う。

監視網の定義

この発表で監視網とは、サービス提供ノードが持つ監視用インターフェース（俗称：裏IF）への監視を行うNW部分です。

- サービス用の表IF（サービス監視）
- 監視用の裏IF（生死監視、MIB取得）

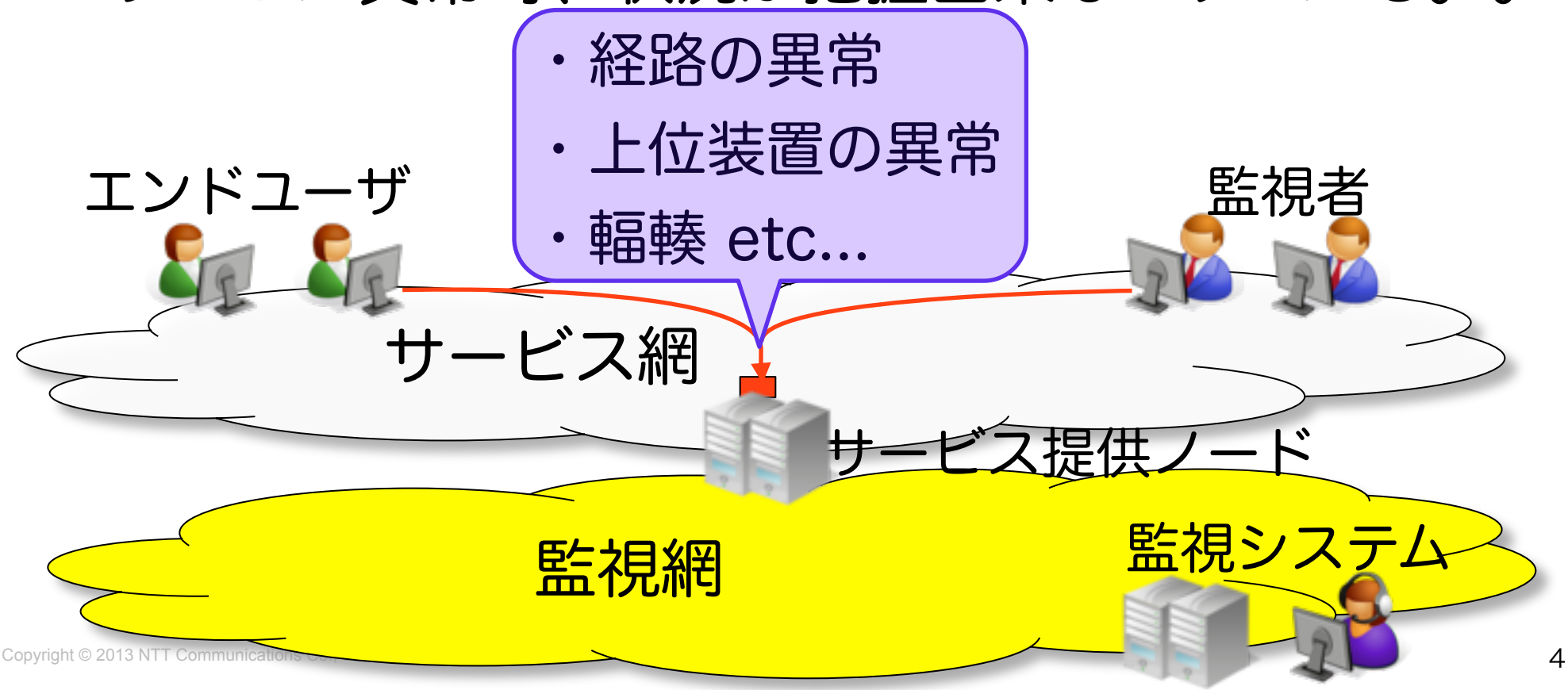


独立した監視網って必要？

ーサービス網で監視はできる、最近は帯域も十分。

→保守面からはあった方がいいです！絶対！

サービス異常時、状況が把握出来ないケースも。。



監視網って・・・

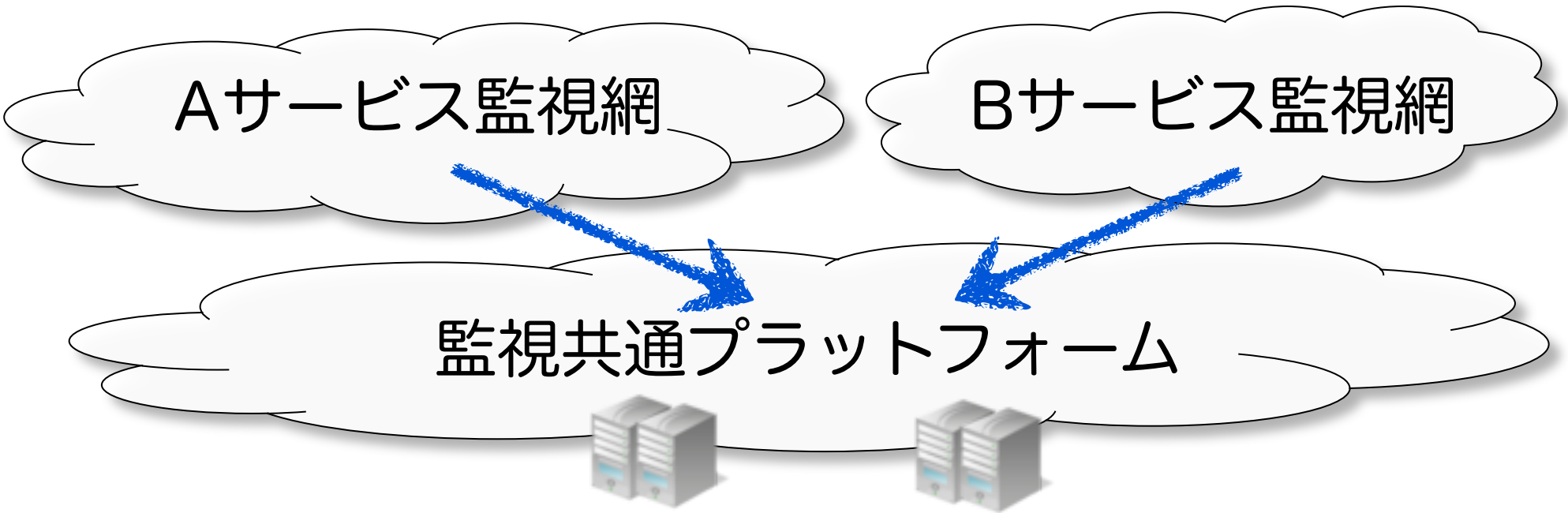
よくある監視網のイメージは・・・

- ー手間とお金が掛けられていない
- ーメンテナンス性が考えられていない(Viva暫定)
- ードキュメントがない

そんなネットワークを扱うエンジニアに取って身近に存在する監視網を突然扱う事になったのが事の始まり・・・

発表動機

私に下された任務は

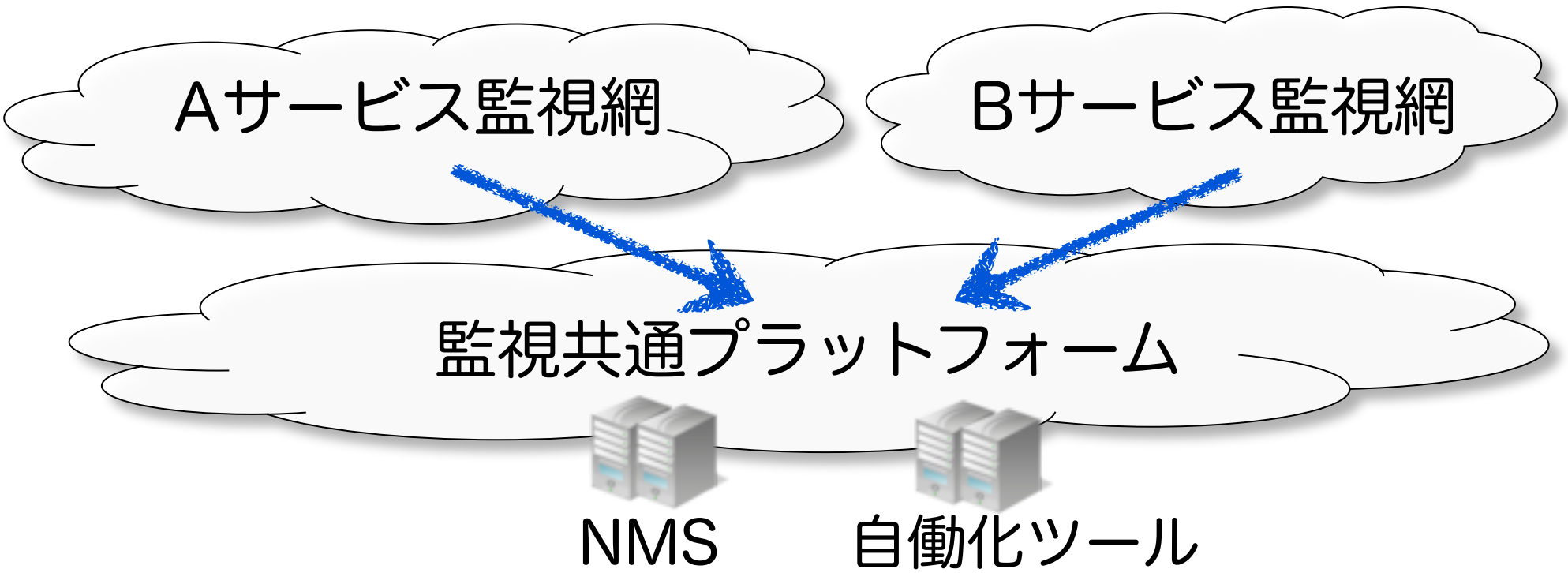


一元的な監視基盤の構築

※一元的な監視基盤:監視共通プラットフォーム(PF)

発表動機

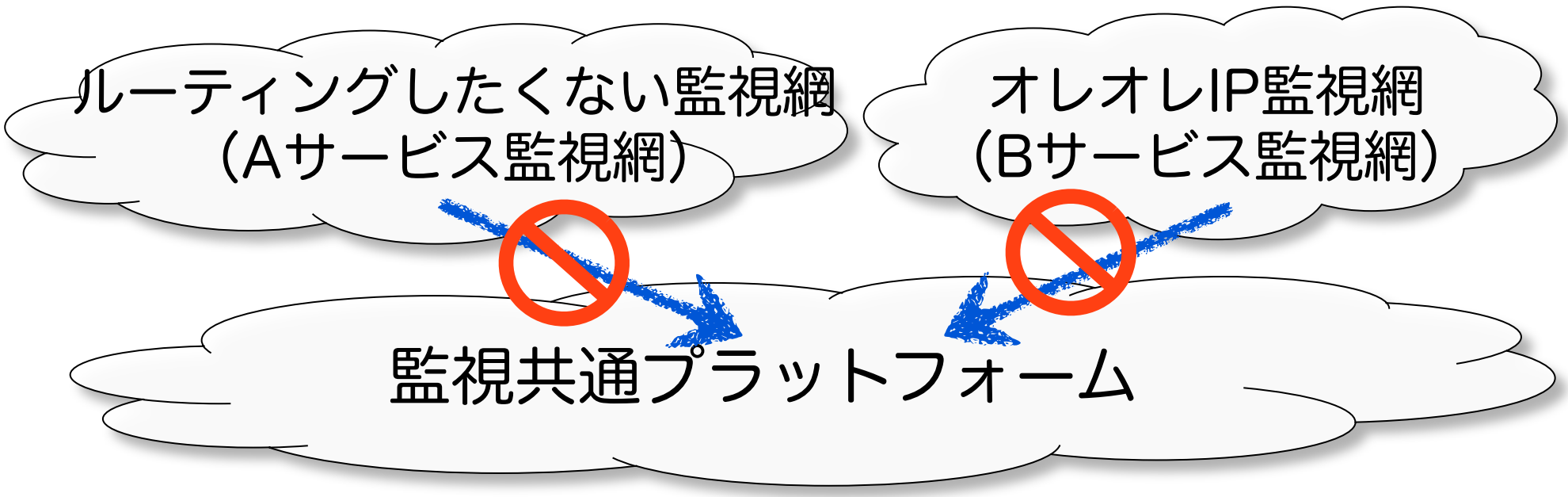
なんで統合するのか？



このオペレーションシステム（ツール）を他の監視網でも使いたい！

発表動機

それぞれの網をリサーチしてみたが、



一筋縄ではいかない問題が発覚。。

発表動機

今回このミッション遂行で凄く苦労しました。。
　ー出来るだけ同じ苦労をする人を減らしたい
　ーニッチだが監視網について皆で考えてみたい

発表の流れは以下の形で進めます。
　ーいろいろな監視網の例
　ーいろいろな監視網との付き合い方例

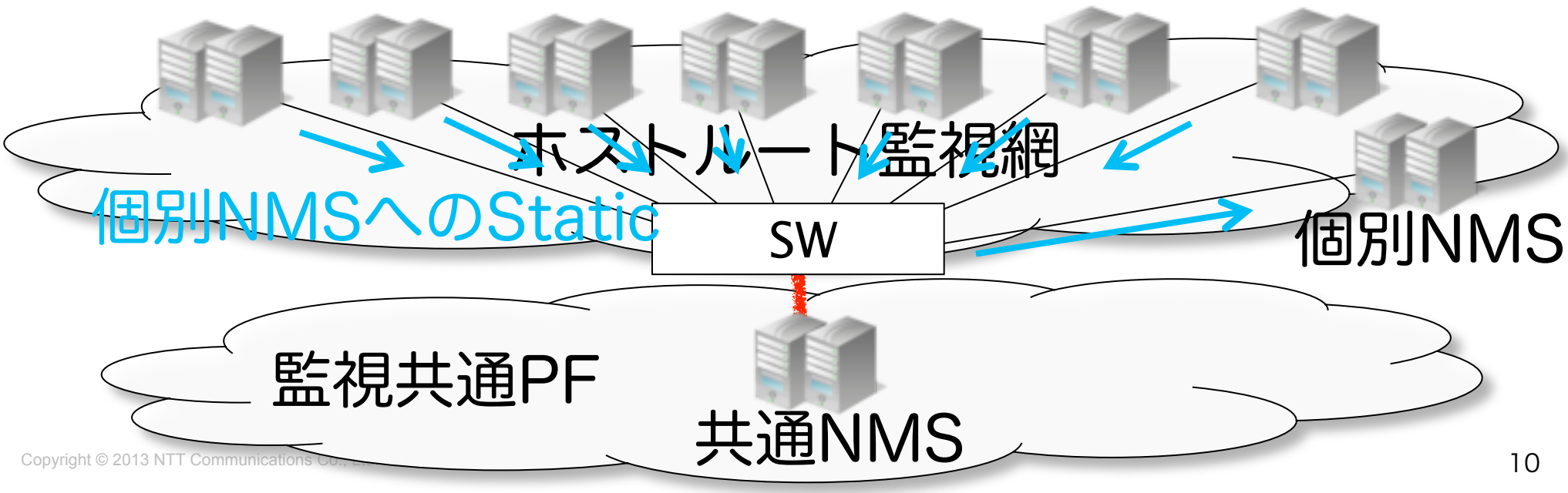
とある監視網の例

▼とある監視網１：ルーティングしたくない監視網

ー各ホストに監視経路を書いている

ー経路追加は全ホストに追記要

ー経路追加がサービス影響にするものも

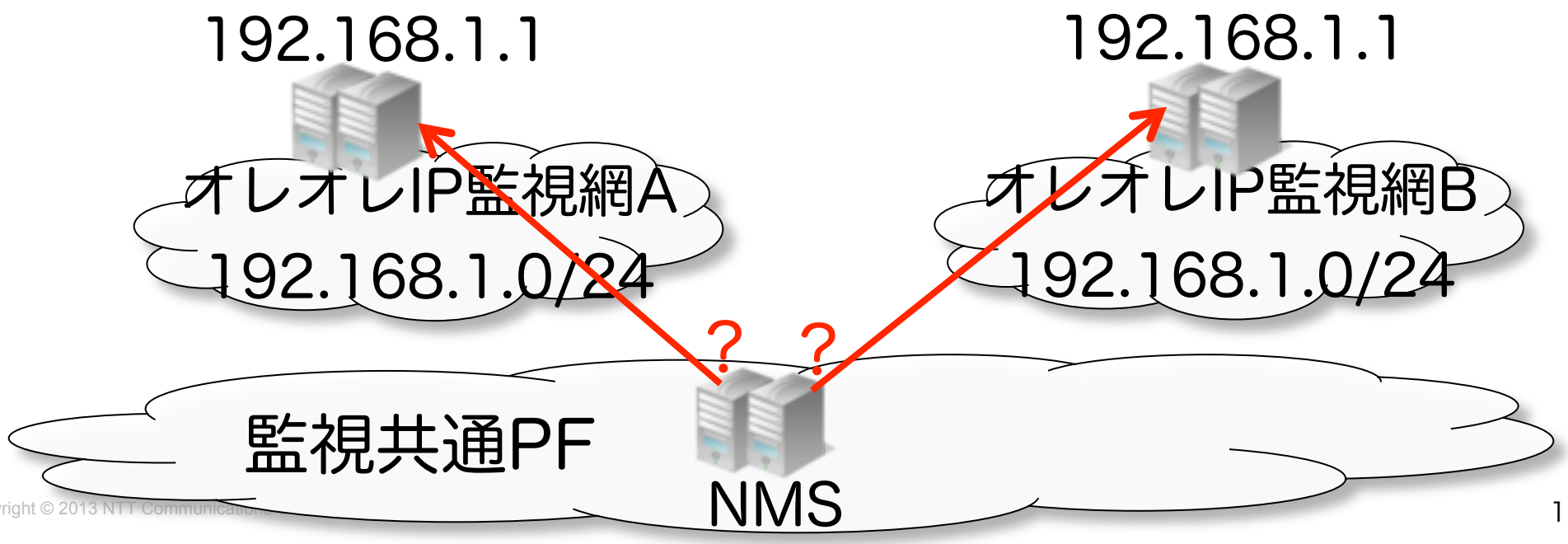


とある監視網の例

▼とある監視網２：オレオレIP監視網

ー管理下のプライベートIPアドレスを管理外で利用

ーIPリナンバはサービス影響ありで難しい。。。

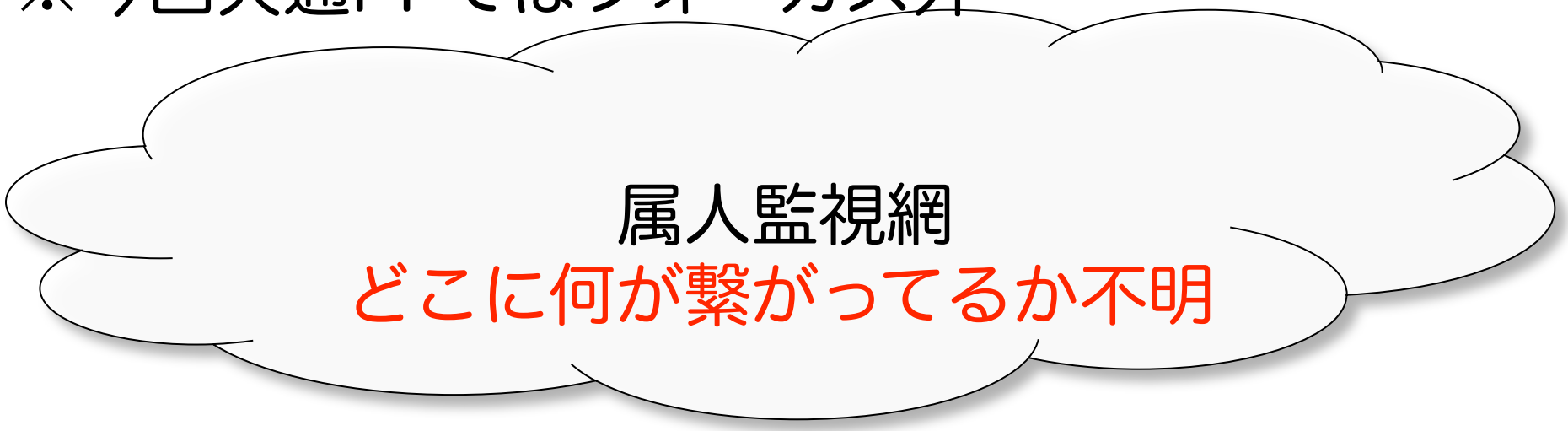


（参考）とある監視網の例

▼その他の監視網：属人監視網

　別名、あの人しか知らない網。ほとんどの場合、ドキュメントがなく、特定の人に聞かなければ分からない。暫定で様々な物が繋がっている事が多く、ディスクリプションを信じてはいけない。

※今回共通PFではフォーカス外・・・



いろいろな監視網との付き合い方

みなさまが不運にも、先の例のような監視網と付き合うことになったら・・・

私は監視共通プラットフォームを作るにあたって、このように付き合ってみました、の例をご紹介します。

監視共通PFの機能検討

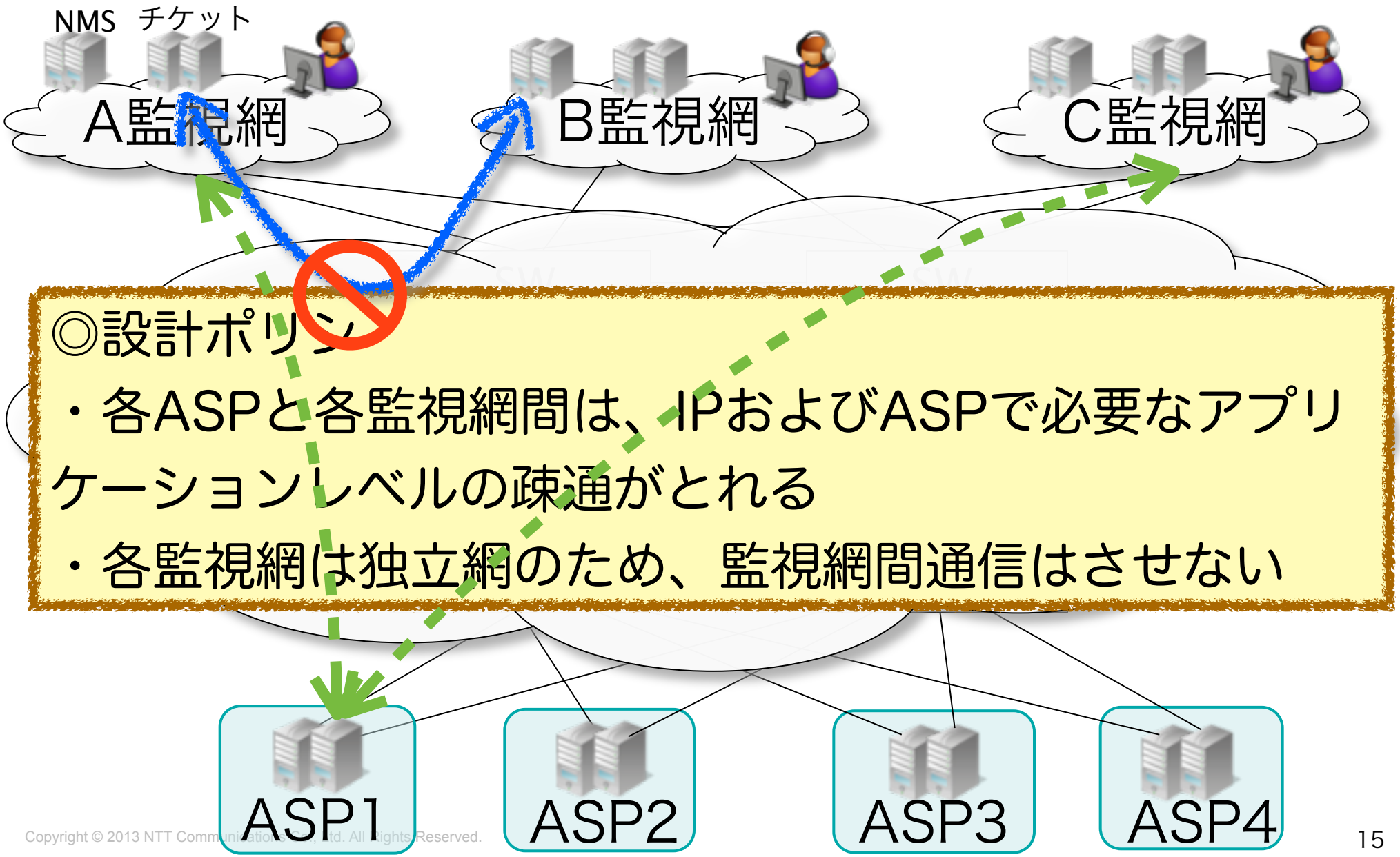
監視共通プラットフォームを設計する際に検討したことは・・・

・各監視網と接続出来る事

・各監視ツールをASP（アプリケーションサービスプロバイダ）として収容出来る事

・耐障害性を高める事

まずは設計してみた



監視網統合の課題

初期設計でうまくいく・・・はずもなく、いくつかの課題が。。その中でも３つ大きな課題が以下。

・課題１：
　　ルーティング（ルーティングしたくない監視網）
・課題２：
　　IPアドレスバッティング（オレオレIP監視網）
・課題３：
　　アプリケーション（NATしたくないASP）

監視網統合の課題

課題１：
　ルーティング（ルーティングしたくない監視網）

　ホストルート監視網のように、経路追加に大きなコストが掛かる、サービス影響が出るなどの場合、ルーティングしてくれない。

　ホストルート監視網以外にも、ポリシとして外部経路を流したくないという網も・・・

監視網統合の課題

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

課題１：ルーティング（ルーティングしたくない監視網）

監視網統合の課題

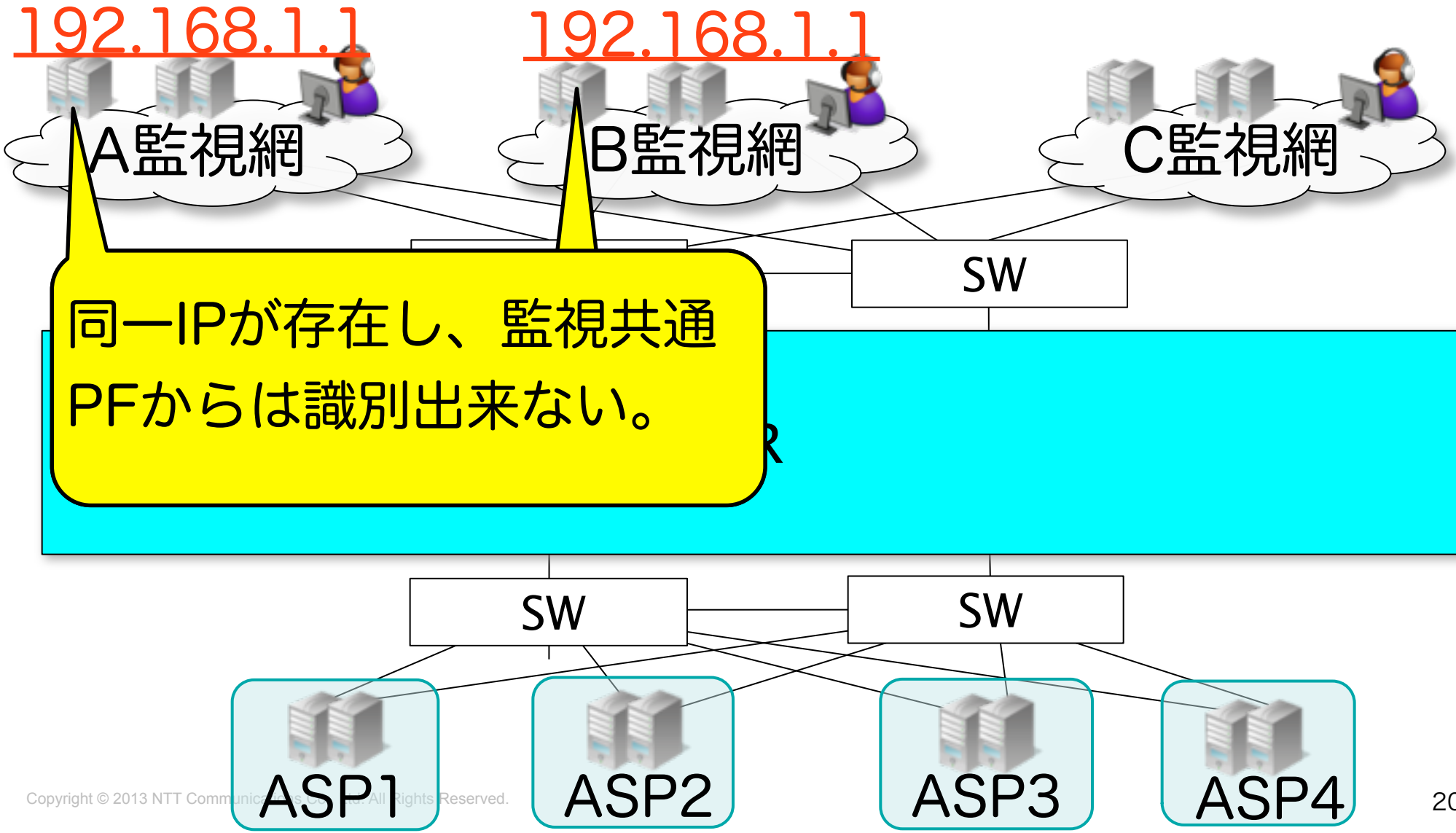
課題２：

　IPアドレスバッティング（オレオレIP監視網）

　弊社ではプライベートなIPを利用する際にもバッティングしないように組織で一意なIPを準備している。しかし、一部の網で使っていないことが判明・・・

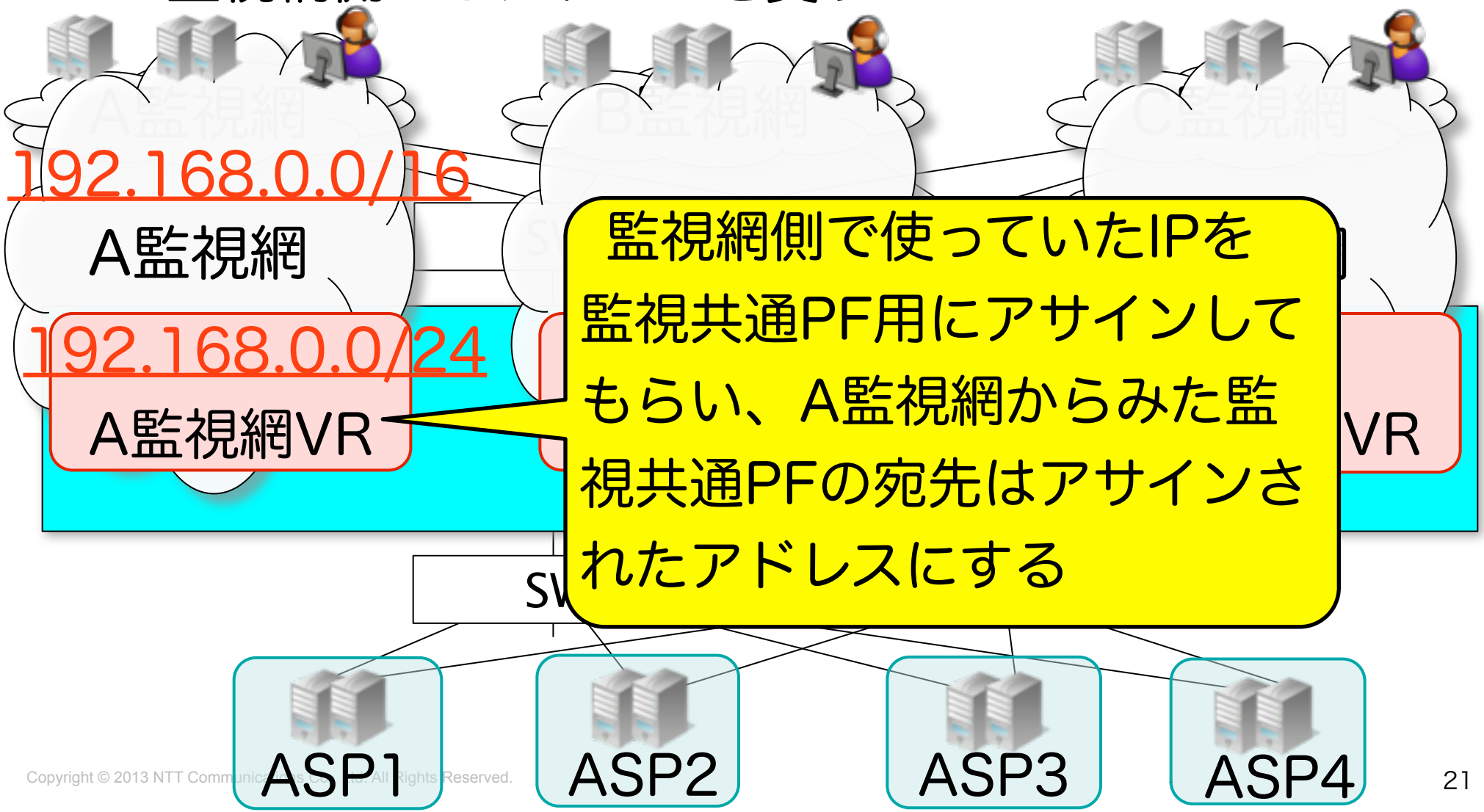
監視網統合の課題

課題２：IPアドレスバッティング（オレオレIP監視網）



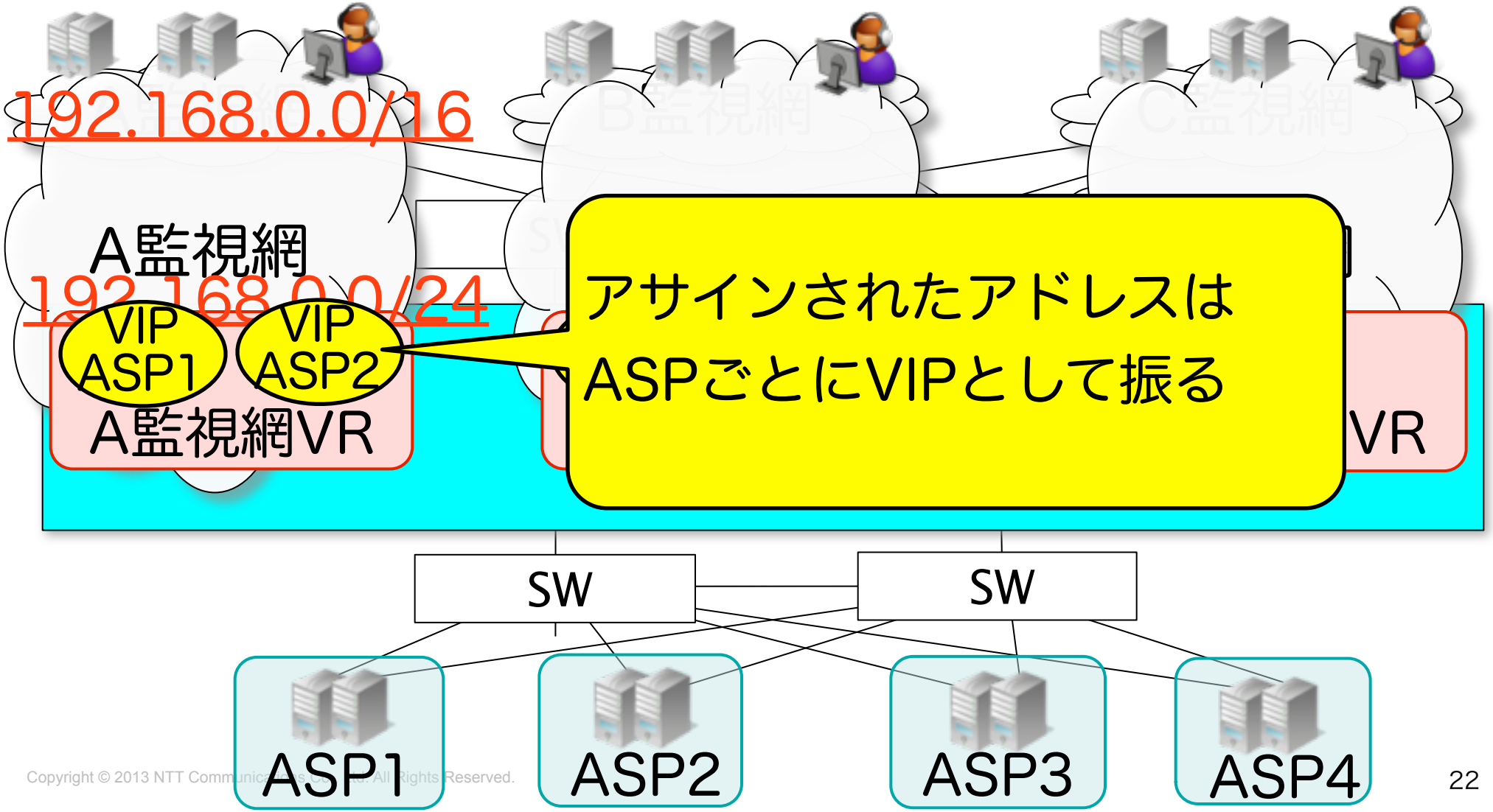
監視網統合の課題解決策

▼課題１/課題２に対する対策（１）
→監視網側からアドレスを貰う



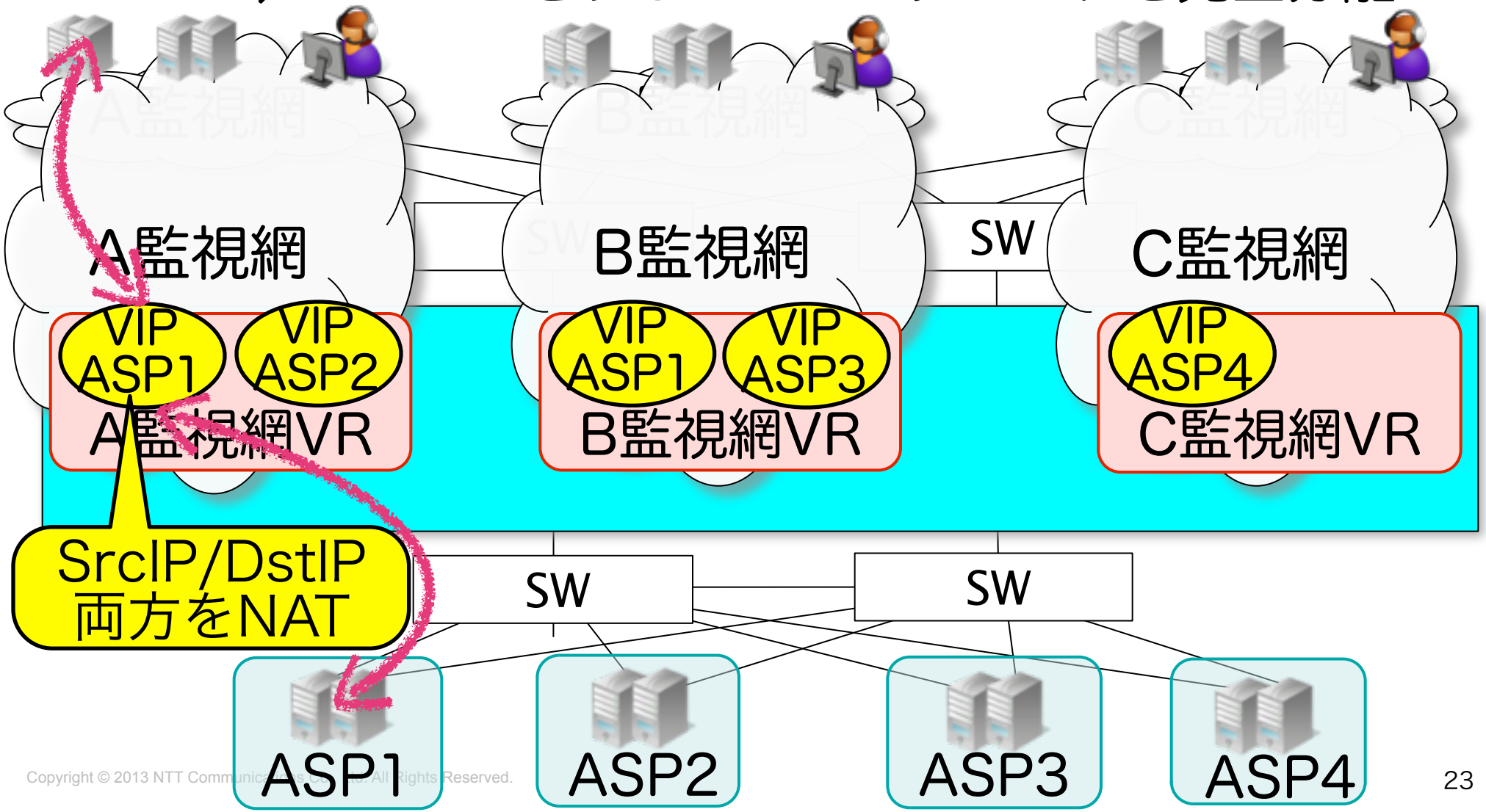
監視網統合の課題解決策

▼課題１/課題２に対する対策（１）つづき
→監視網側から貰ったアドレスをVIPとする



監視網統合の課題解決策

▼課題１/課題２に対する対策（２）
→Src／DstNATをすることでセグメントを完全分離



監視網統合の課題

課題３：アプリケーション（NATしたくないASP）

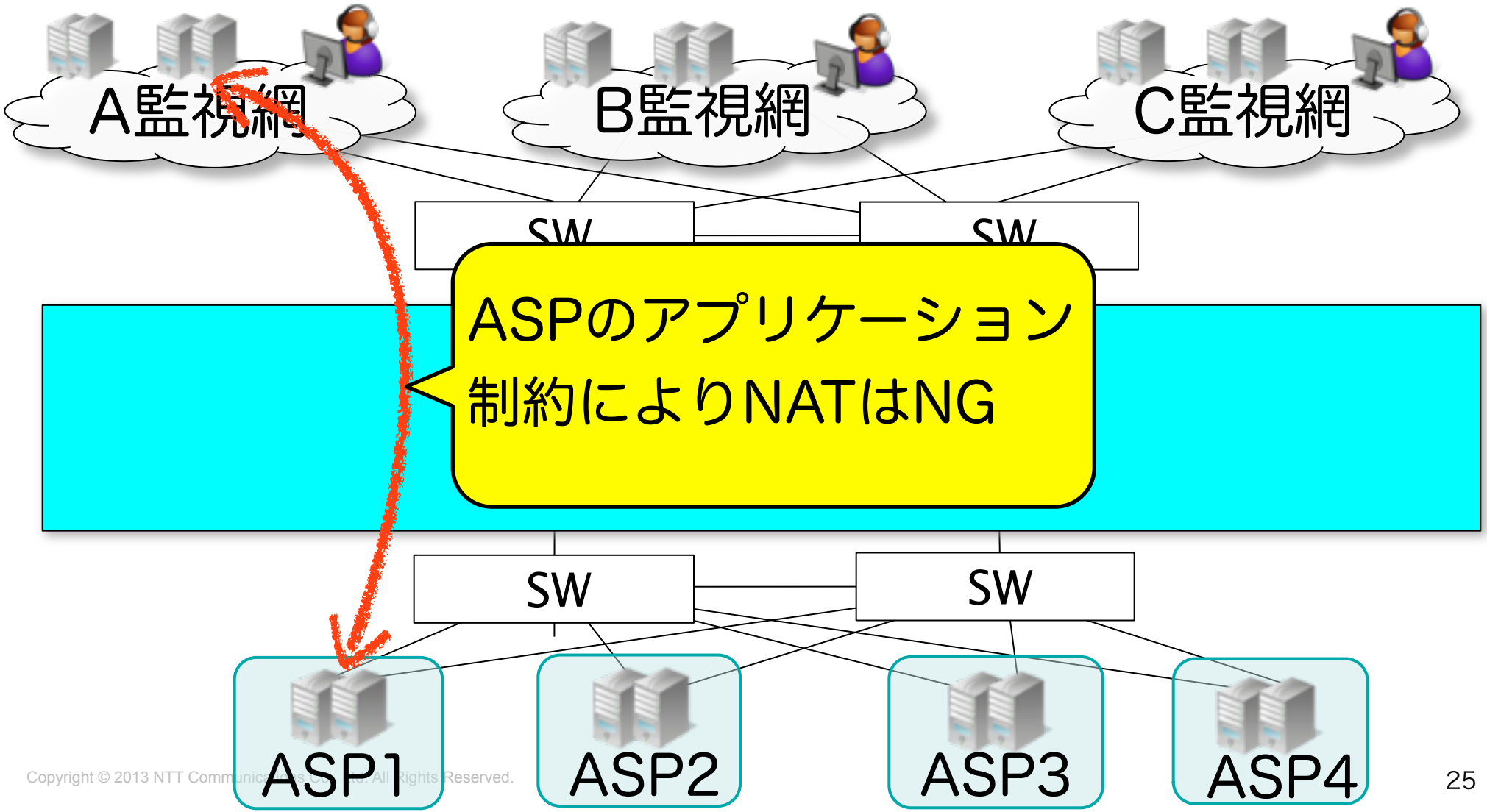
監視共通PF上でASPとして存在する監視ツールには、NATが苦手なアプリケーションが存在する。。

例：

- NMS
- 自働化ツール

監視網統合の課題

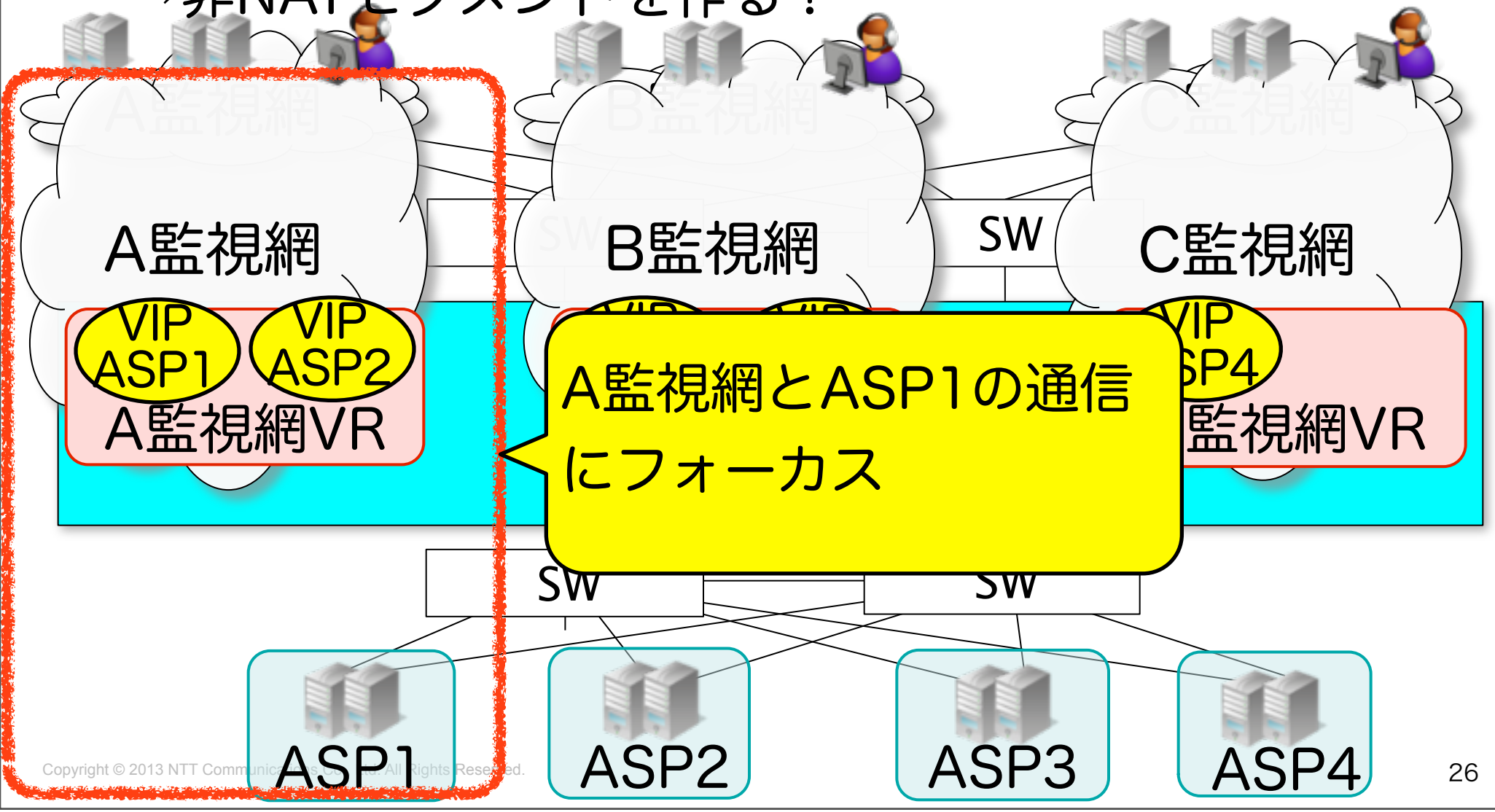
課題３：アプリケーション（NATしたくないASP）



監視網統合の課題解決策

▼課題３に対する対策

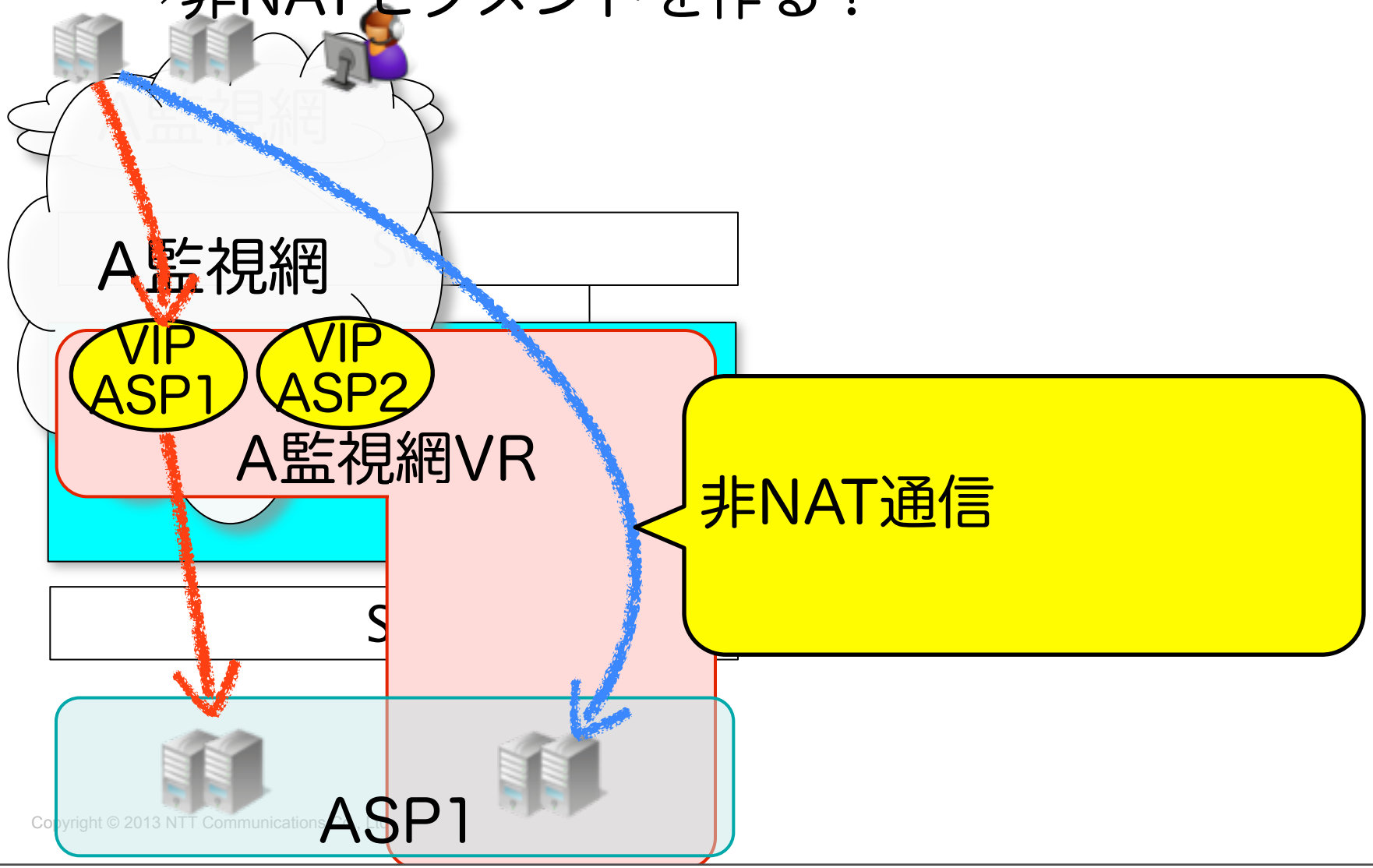
→非NATセグメントを作る！



監視網統合の課題解決策

▼課題３に対する対策

→非NATセグメントを作る！



今回検討した事の振り返り

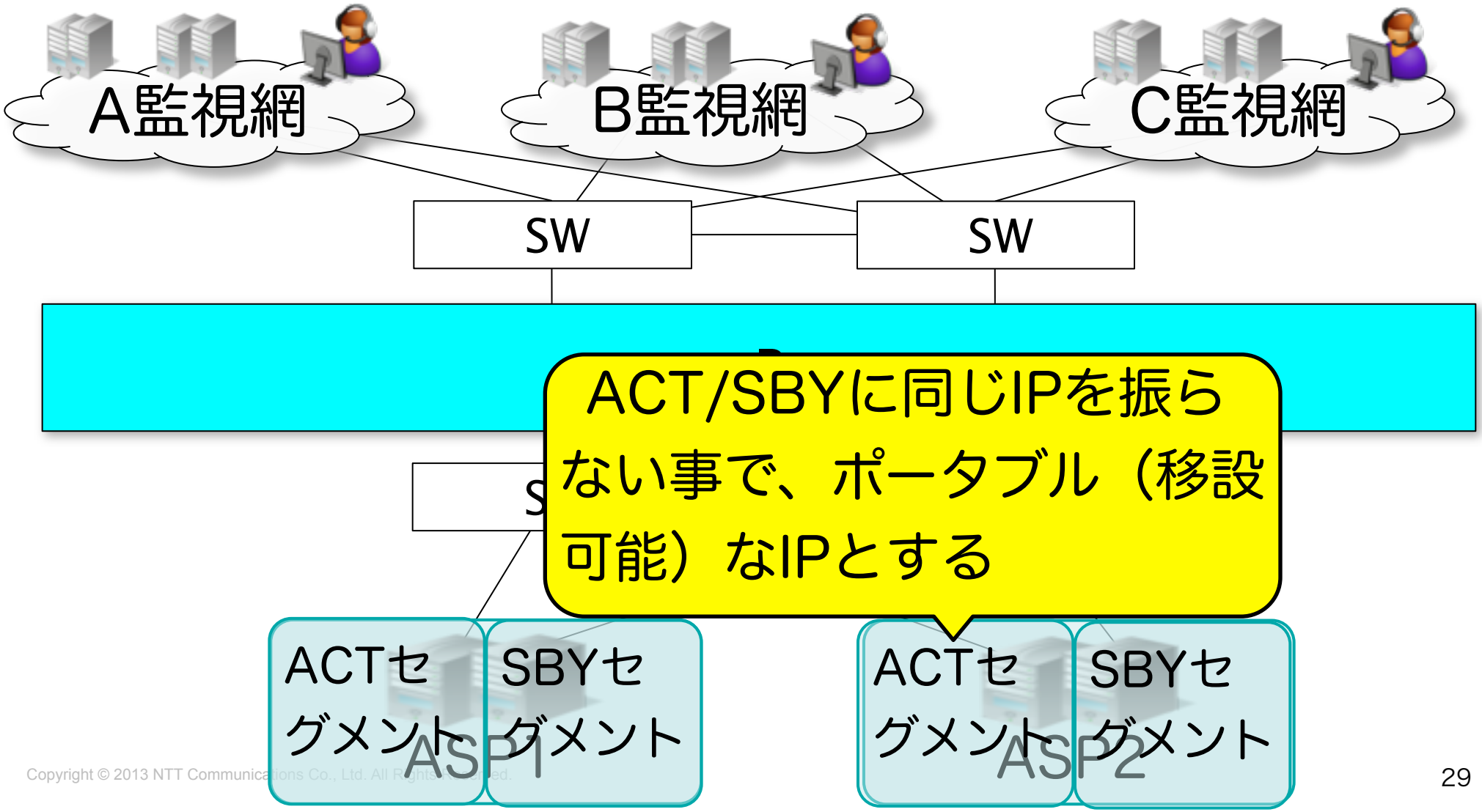
改めまして、監視共通プラットフォームを設計する際に検討してきたことを振り返ると・・・

- 各監視網と接続出来る事 →VR収容のNATで解決
- 各ASPを収容出来る事 →NAT/非NATで解決
- 耐障害性を高める事 →IPアドレッシングを工夫
  （次ページ詳細説明）

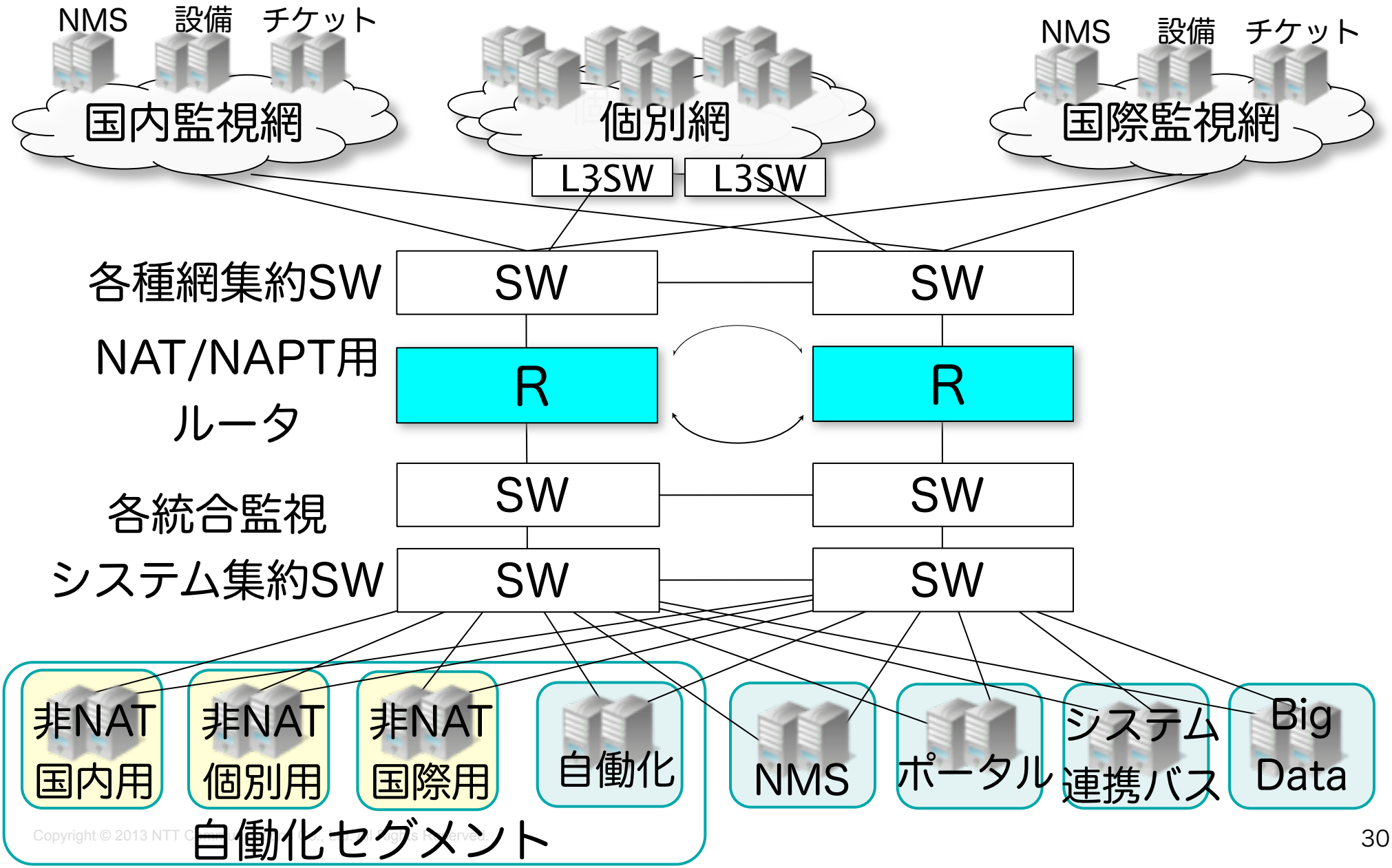
（参考）監視網デザイン案

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

拠点分散など将来を見据えたIP設計



監視共通PF NW構成図



（参考）監視共通PFについて

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

- 監視共通PFのカバー範囲
  ー現在はIPな監視をすべてカバーすべく拡大に
  　奮闘中（現在進行形）
  ー将来はＬ１からＬ７まで非IP機器含めて全部
  　カバーしたい。。
- せっかく作るので、良い監視網を作りたい
  と思って着手しましたが、、一時期属人網になっ
  たりしてました、、

まとめ

▼監視網って裏方だけど重要

ー問題のある監視網がなければ苦労は無かった

ーこれだけはやめた方がいい監視網づくり

・ホストルート監視網

・オレオレIP監視網

・（属人網）

→いくらクローズドでもNWは繋がってナンボ

まとめ

▼監視網の運用設計がどうあるべきか？

ー運用は理想論では回らない。しかし、技術や知恵で乗り切れる課題もある。今回は、

・VRを使ったSrc/DstNAT(NAPT)

・非NATセグメント作成

を1台のルータで、しかも要件定義含め約１ヶ月でクリア:-)

議論

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

- 議論のしたいこと
  - ー監視網っている？いらない？
  - ー監視網の位置づけ
  - ー監視網のあるべき姿
  - ー監視網あるある

- 答えづらい話題
  - ー 具体的なツールやシステムの話
    （NMS、Script、自働化ツールなど）
  - ー 非IPの監視

ご清聴ありがとうございました