Create New Value by

エンタープライズ向けVPNサービスNW 運用自動化への挑戦

株式会社NTTPCコミュニケーションズ

加藤史章

水口直哉

NTT PC COMMUNICATIONS

01 自己紹介

Create New Value by CDI

加藤　史章
株式会社NTTPCコミュニケーションズ

- 2008年入社
- エンタープライズ向けVPNサービスの設計/構築/運用
- 最近は運用自動化がメイン

JANOG歴：

- JANOG43：初一般参加
- JANOG44
- JANOG46：初スタッフ参加(Hackathon)
- JANOG47：初登壇

01 はじめに

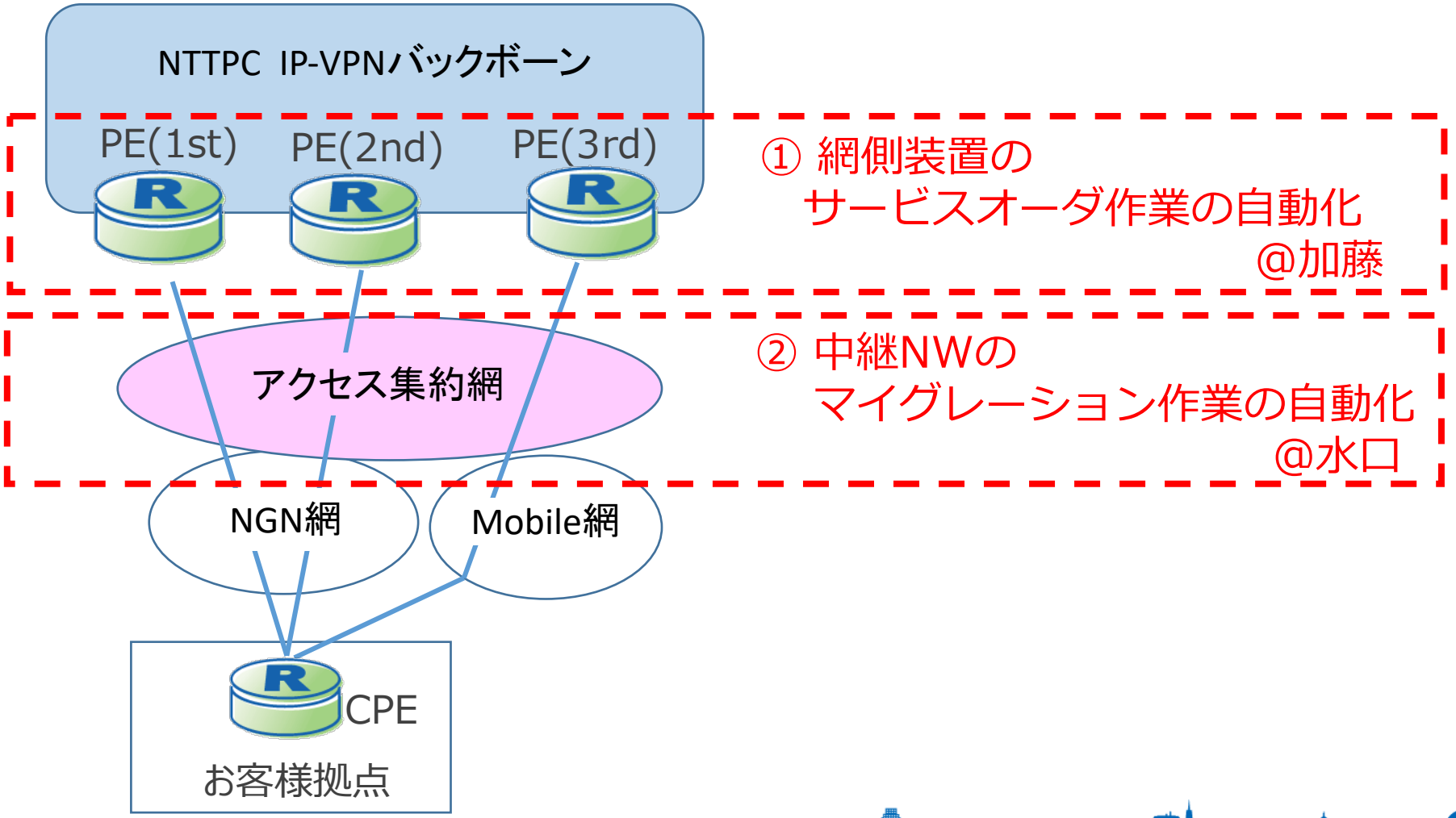
- 私達はエンタープライズ向けVPNサービスの設計、運用を行っており、
NW装置の設定変更作業においては、テキストの雛形を
置換して作業手順書を作成する運用を現在でも行っています。

- 数年前からこれらの設定作業の自動化に着手しており、
サービスオーダやNWマイグレーションにおける
設定作業の一部を自動化することが出来ました。

- 本セッションではこれらの自動化するまでの課程においての
課題やその解決法と、今後の展望について
共有、議論させて頂きたいと思います。

エントリーVPNサービス構成と運用自動化の対象

- NGN/モバイルNWを利用したエントリーVPNサービスを提供
- お客様に提供するCPEと接続するPEルータの開通設定作業を日々実施
- アクセス集約網の更改によるマイグレーション作業

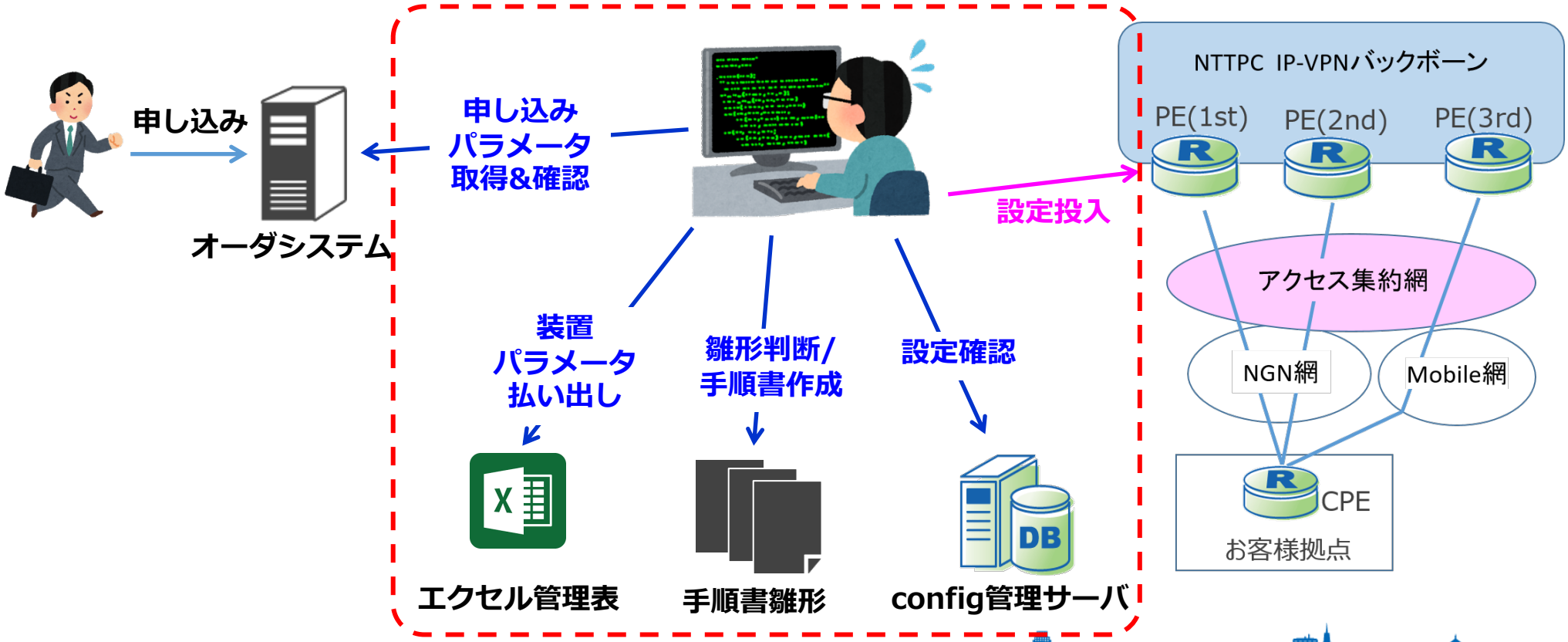


サービスオーダの自動化

01 自動化前の状況

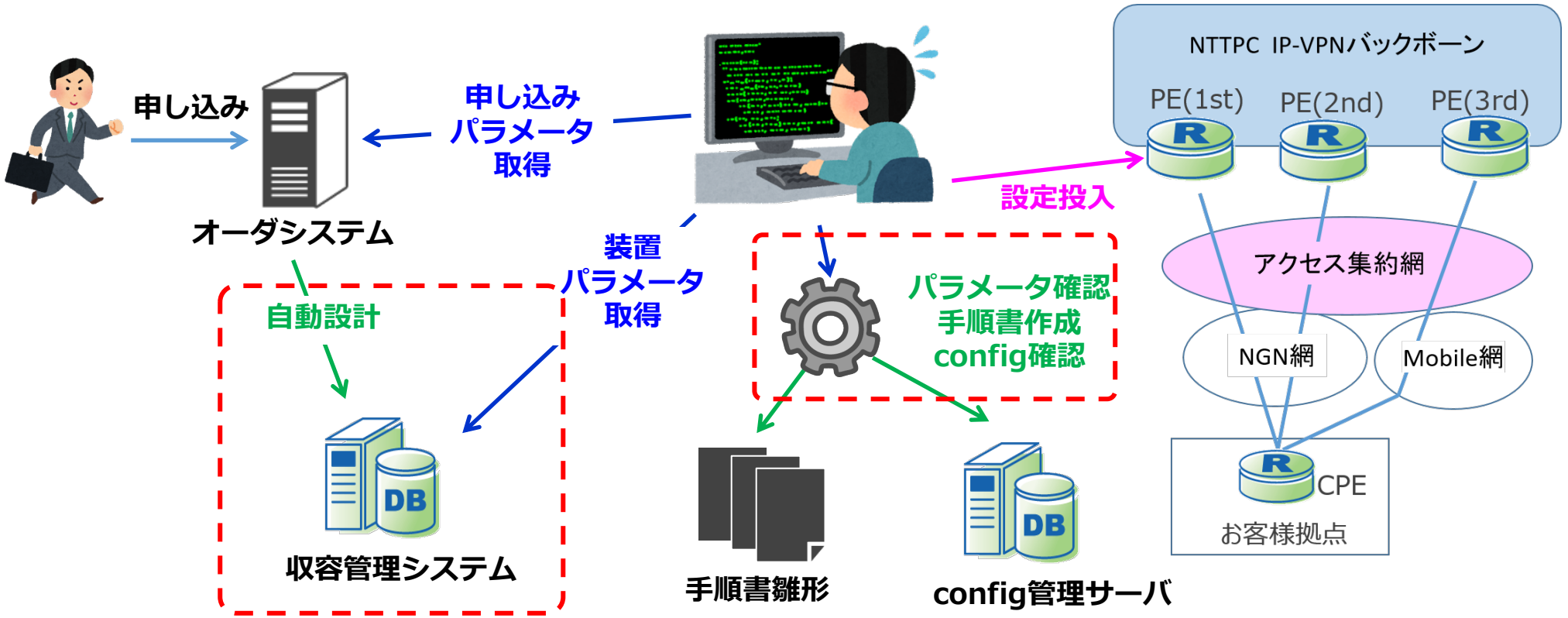
- 申し込みパラメータを目視確認
- エクセル管理表から装置の収容パラメータを手動払い出し
- 手順書の内容や設定の正常性を目視確認
- テキストの手順書をコピー&ペーストで設定

▶ 人手に頼った作業で毎日数十件分実施



01 自動化の準備

- システム、ツール導入によって人の判断の排除
  - ✓ 収容管理のエクセル管理表 ⇒ システムによる自動設計
  - ✓ パラメータや設定の目視確認 ⇒ ツールによる判定



01 自動化に向けた問題

- 設定雛形は柔軟に変更できる必要がある
  - ✓ 不具合等で急遽変更する可能性を考慮
- システム運用の経験が無い
- 旧装置はconfigの整理が必要
  - ✓ 本来1拠点1policy設定が、同一内容の場合複数拠点1policyが存在
- 申し込みパラメータで特定条件のみ重複NGとするものが存在

01 自動化に向けた問題

Create New Value by CDI

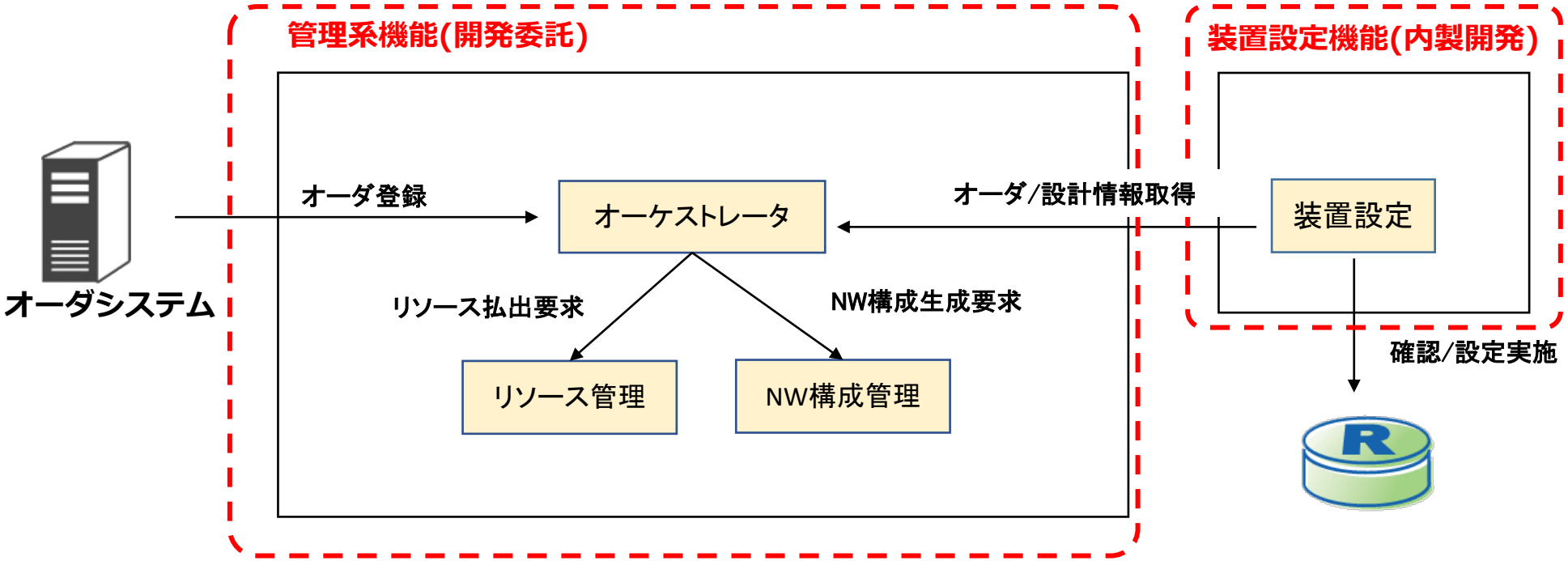
- 設定雛形は柔軟に変更できる必要がある
  - ✓ 不具合等で急遽変更する可能性を考慮
- システム運用の経験が無い

- 旧装置はconfigの整理が必要
  - ✓ 本来1拠点1policy設定が、同一内容の場合複数拠点1policyが存在
- 申し込みパラメータで特定条件のみ重複NGとするものが存在

▶ 自動化の対象範囲の制限等で暫定回避

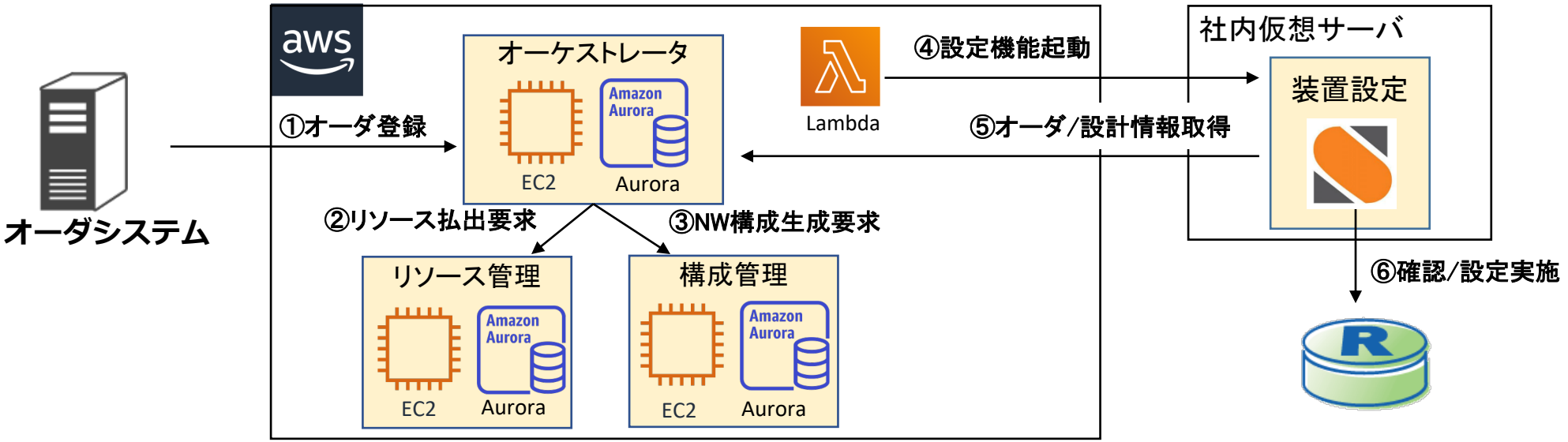
01 自動化システムの機能の分離について

- 管理系機能(オーダ受付、オーケストレーション、リソース管理、NW構成管理)と装置設定機能(config生成、設定確認/投入)で分離
  - ✓ 管理系機能 ⇒ 開発委託
  - ✓ 装置設定機能 ⇒ 内製開発
- 装置設定機能は内製開発のため、設定雛形の変更は稼働次第で可能



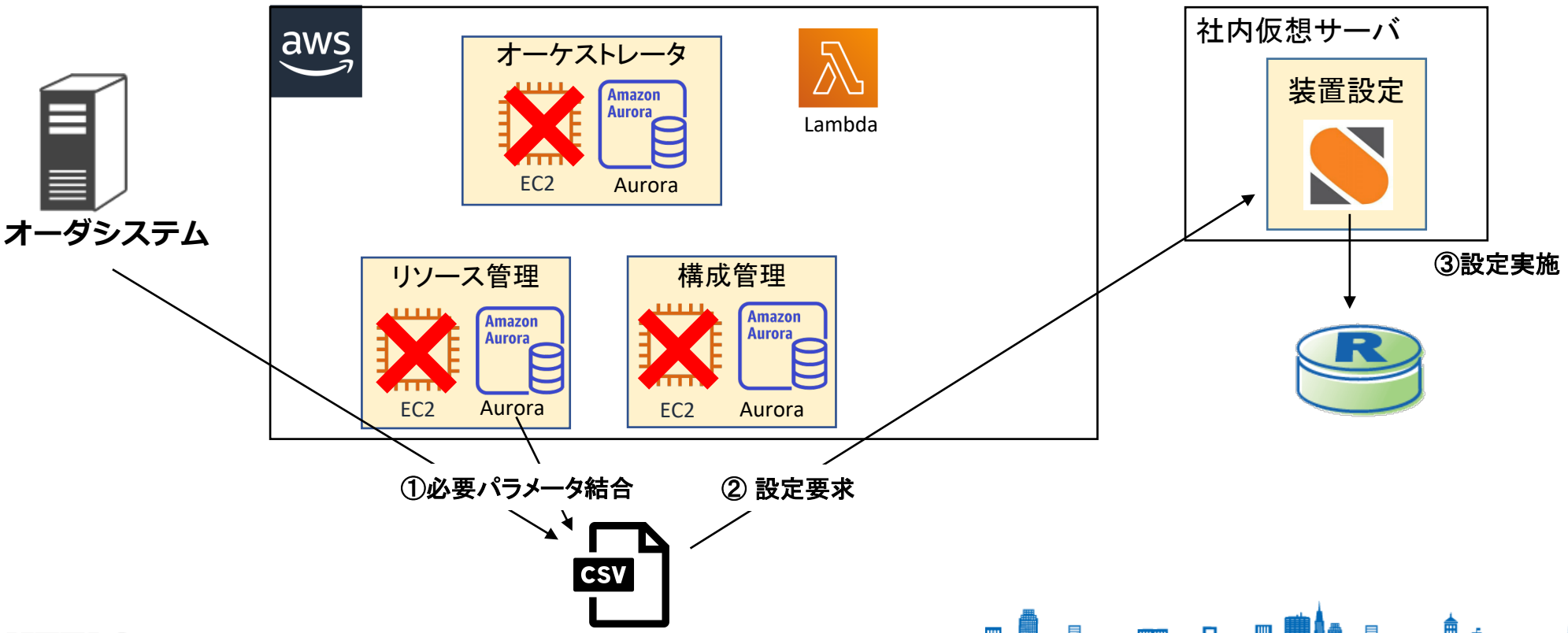
01 自動化後の構成

- 管理系機能はAWSを利用して運用リスクを低減
- 装置設定にはStackStorm+python(netmiko)を利用
  - ✓ 装置設定機能部分ではデータを保持しない設計
  - ✓ docker版を利用し、異常時に初期化でリカバリ可能に
- 装置設定機能は手作業だった頃がベースになっており、
  1拠点ずつを繰り返して設定する仕様
  1. Lambdaによって設定機能を定期実行
  2. 実行されるとオーダを取得し、最優先の1件の設定処理を実行
  3. 設定完了をトリガーに自動的に設定機能を再呼び出し
  4. ２～３を未完了オーダが0になるまで繰り返し



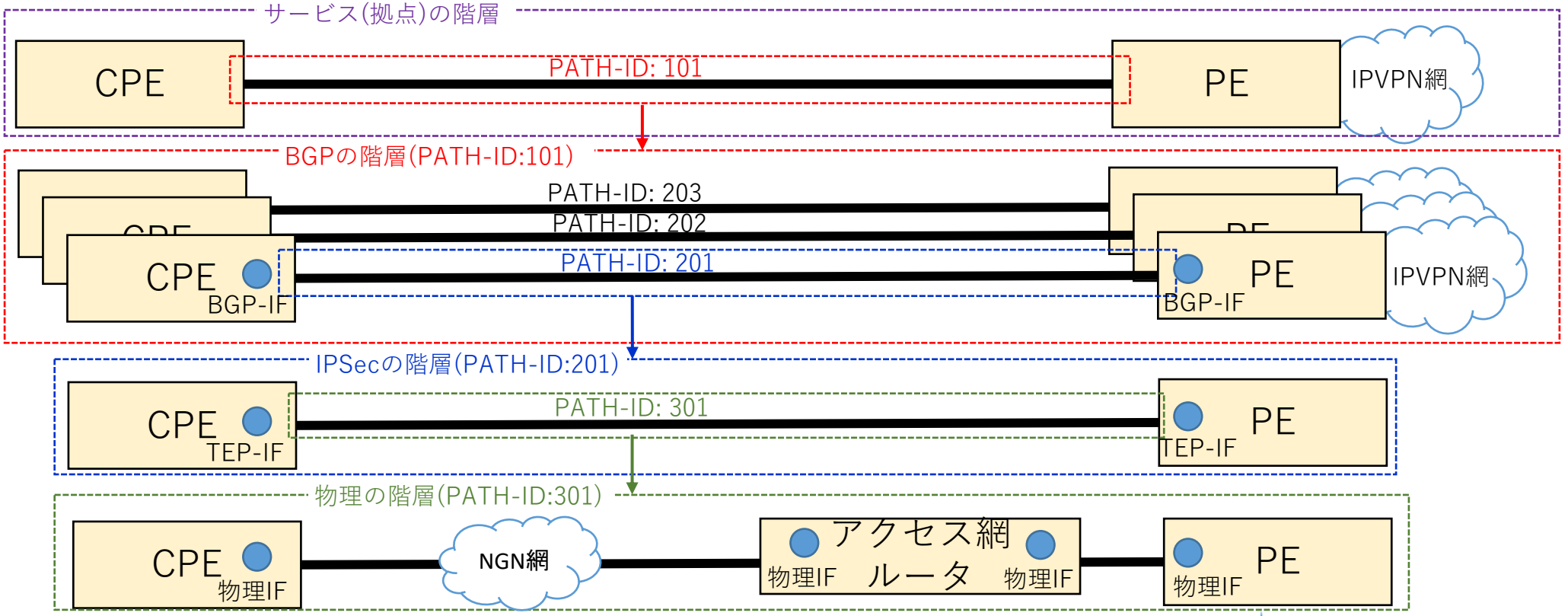
01 問題発生時の保険について

- 管理系機能が動作しなくても設定できるように装置設定機能は設計
  - ✓ オーダシステムからの申し込みパラメータは今まで通りDL可能に
  - ✓ リソース情報はマネージドRDSのため、取得可能と想定
  - ✓ これらを手動で組み合わせて装置設定機能の確認/設定を行っている処理を直接実行することで設定可能とした



01 NW構成情報管理について

- 構成図の自動生成が出来るよう、NW構成情報をパス管理することにした
- 拠点の接続情報を階層化し、その階層の構成を装置/パス/網の要素で表現
  - ✓ 今回のサービスはBGPoverIPSecのため、下図のような階層になる
  - ✓ パスの要素はIDを保持し、ID検索することで1段下の階層の情報参照が可能
  - ✓ 装置や網のはIF情報などの付加情報を保持し、それによって各階層のリソースなどの情報の取得が可能
- 現状ではサービスごとの階層化モデルの検討に時間を要するのが問題



振り返り・課題と展望

○自動化してよかったこと

- 日々の設定業務からの解放
  - ✓ 緊急での設定依頼も対応不要に
- 自動化に適した作業フローやconfig設計が分かった

○課題

- 1拠点ずつの繰り返し設定のため、時間がかかる
  - ✓ 許容量以上のオーダ数があると間に合わない
- 冗長の一部装置が故障していると、回復まで次のオーダの設定ができない
  - ✓ オーダが溜まる

○展望

- 装置設定機能はオーダに基づき設定するのではなく、
  NW構成情報をもとにコンフィグを生成するようにしたい
  - ✓ 手続き型 → 宣言型
  - ✓ オーダはNW構成情報を書き換えるためのものとし、
    装置設定機能は筐体設定をNW構成情報に合わせるものとする
  - ✓ 装置の初期設定＋NW構成情報による拠点情報 によって
    対象装置の全コンフィグを生成し、差分反映することで実現

NWマイグレーションの自動化

02 自己紹介

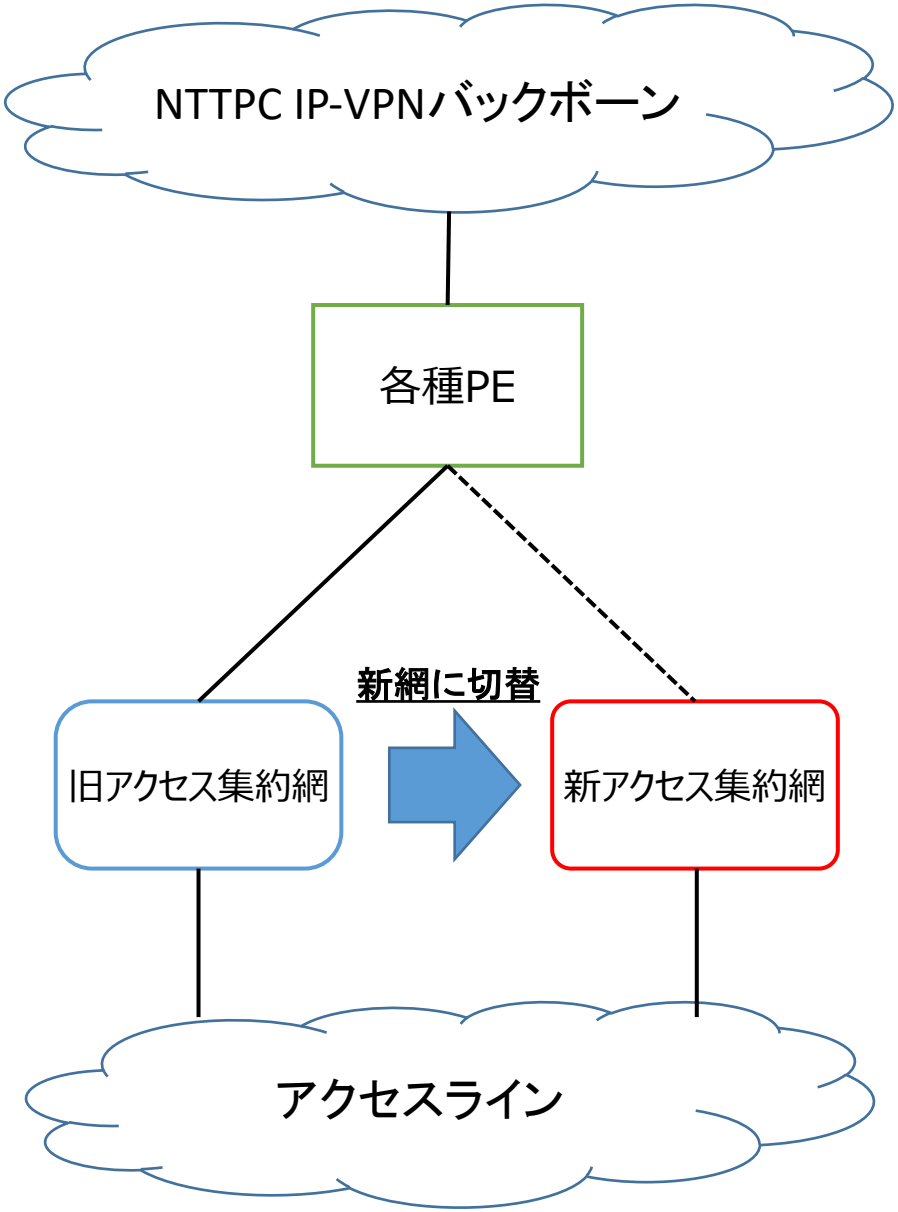
- 水口直哉 (Naoya Mizuguchi)
  - 2019年4月 NTTPCコミュニケーションズ入社
- 担当業務
  - IP-VPNサービスの設計/開発/構築/運用
  - 各種ネットワーク自動化システムの開発
- JANOG
  - JANOGは入社以来はフル参加 (4回目)
  - JANOG44にてぺちゃくちゃに登壇
  - プログラム登壇は初めて

02 はじめに：NWマイグレーション作業について

- 機器更改に伴いNWのマイグレを実施(右図)

- マイグレ実施にあたっての課題
  - 数百台分のPEのマイグレ作業
  - 1マイグレあたりの作業量が多い
  - 機器に関するノウハウが限られた人にしかない
  - しかし、マイグレは可能な限り早く終えたい

- そこで、作業負荷少なく・誰でも・正確に・早く
  マイグレができるように自動設定システムを検討



02 内容

本資料はそんな自動設定システムを作ろうとした男の軌跡である…！！

1. 自動化を始める前
   - 自動化を行う範囲の決定
   - 自動化後の業務フローの決定

2. 自動化システムの開発
   - 自動化システムの設計/構築
   - AWXによるAnsible実行環境の構築
   - Ansibleの構成

3. 実際に自動化システムを導入してみて
   - 導入した効果
   - 自動化で苦労したこと/困ったこと
   - ディスカッション

02 自動化システム構築の最初の壁

- どの設定まで自動化するか
- 何を自動化すると効果が高いのか
- そもそも自動化システムの開発がどのくらい大変なのか

全部の装置の
設定ができるの？

自動化システムの
開発ってどのくらいの
期間でできるの？

自動化したら
設定何分くらいで
できるの？

02 自動化する範囲の決定

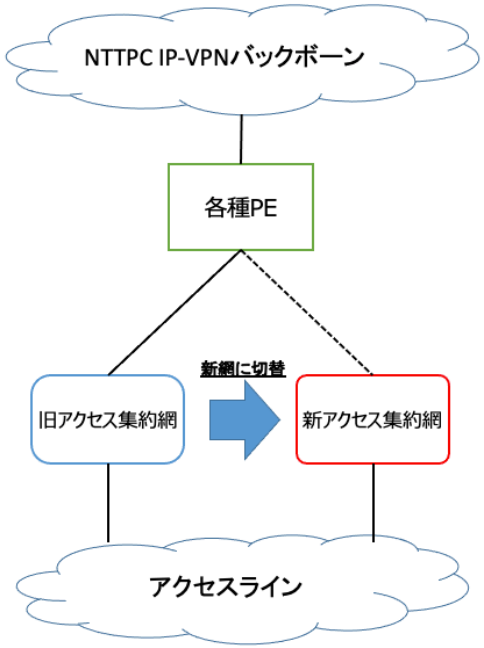
- 開発稼働と効果を考慮し、以下の通り自動化する範囲を決定
- 自動設定と手動設定を組み合わせた半自動化のような形で構築

自動化すること

- 新旧アクセス集約網の論理設定
- 切り戻しのときの論理設定

やらないこと(手動でやること)

- PE側の設定変更
- アドレス/VLAN設計
- 物理配線の統制
- End-End通信の確認

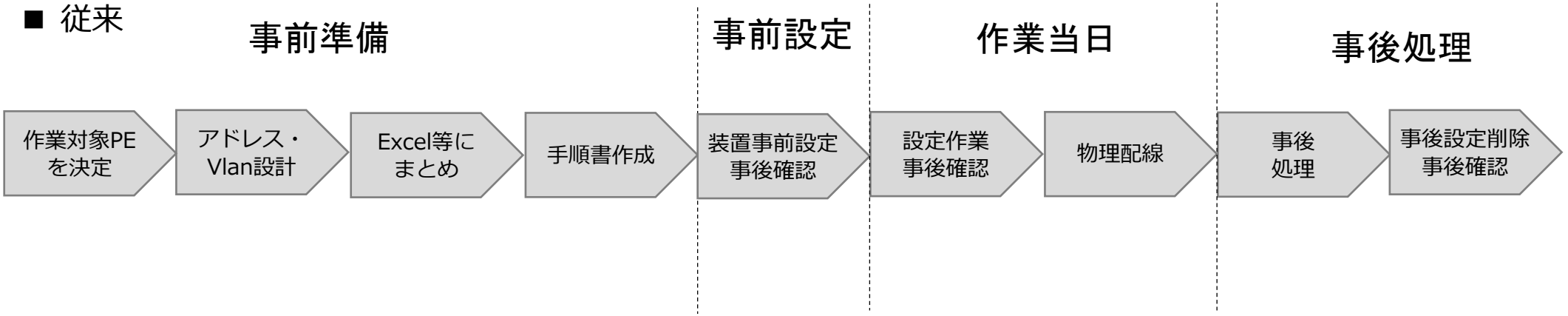


PE毎に機種/設定が異なり種別が多いため、開発が大変
→ 最初のリリースでは見送り

アクセス集約網側はPE向けの設定が共通
→ 使い回しでき設定行数も多いため、効果が大きい

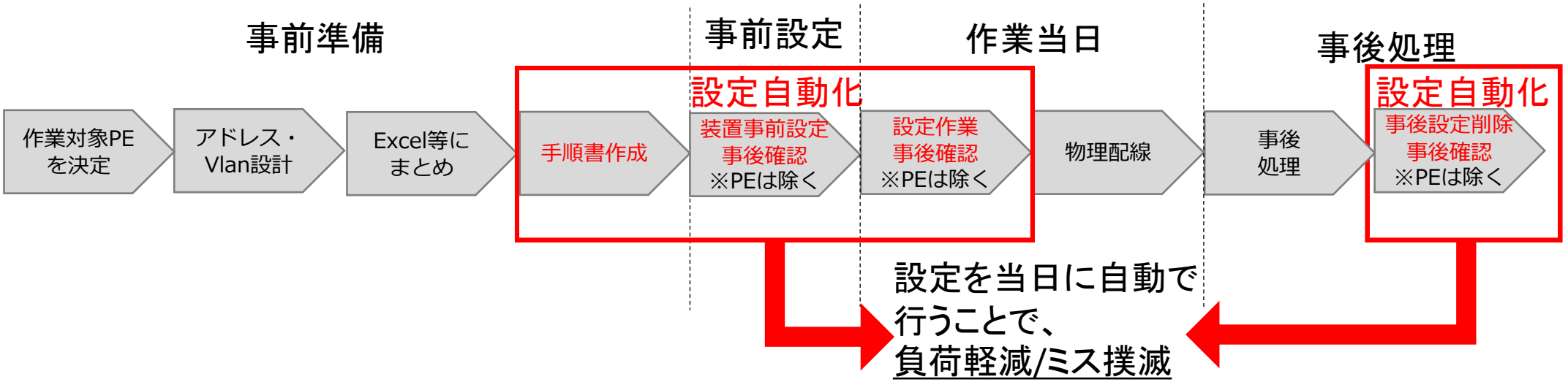
02 自動化前後のフロー比較

■ 従来



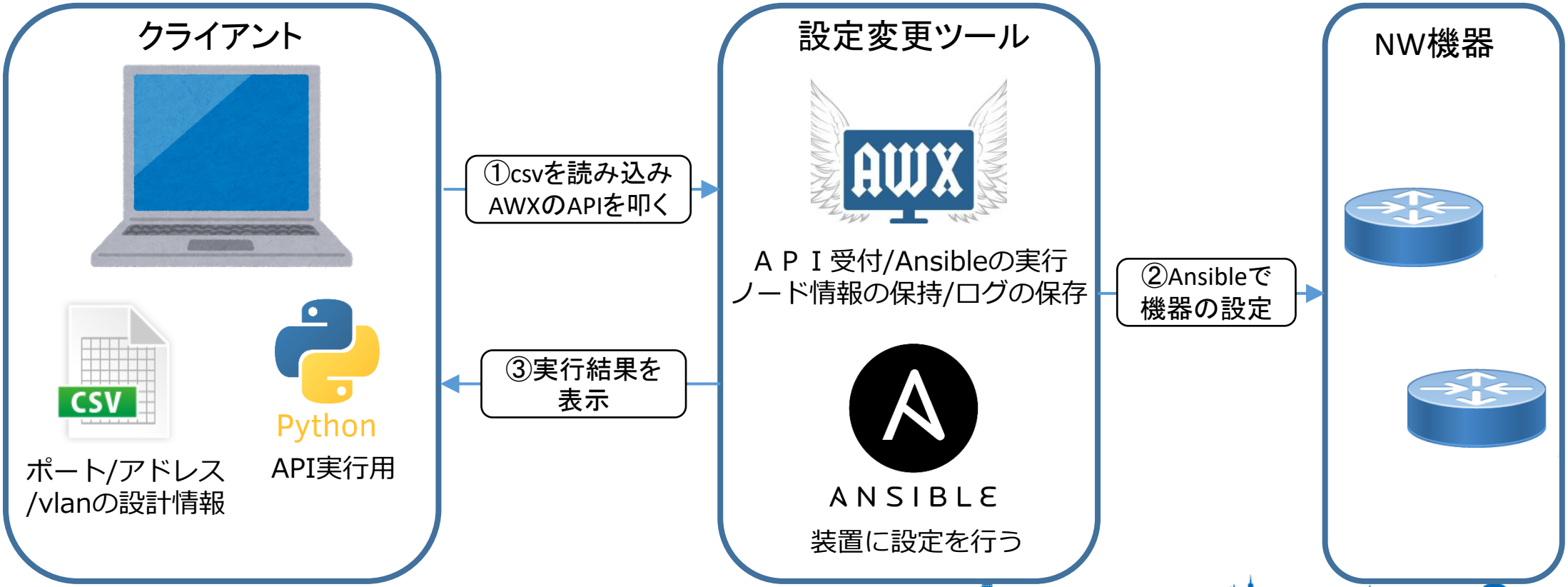
※設定量が多いため、物理作業日に台数をこなすために
事前に設定を行うことや、設定を後日消すことを行っていた

■ 自動化後



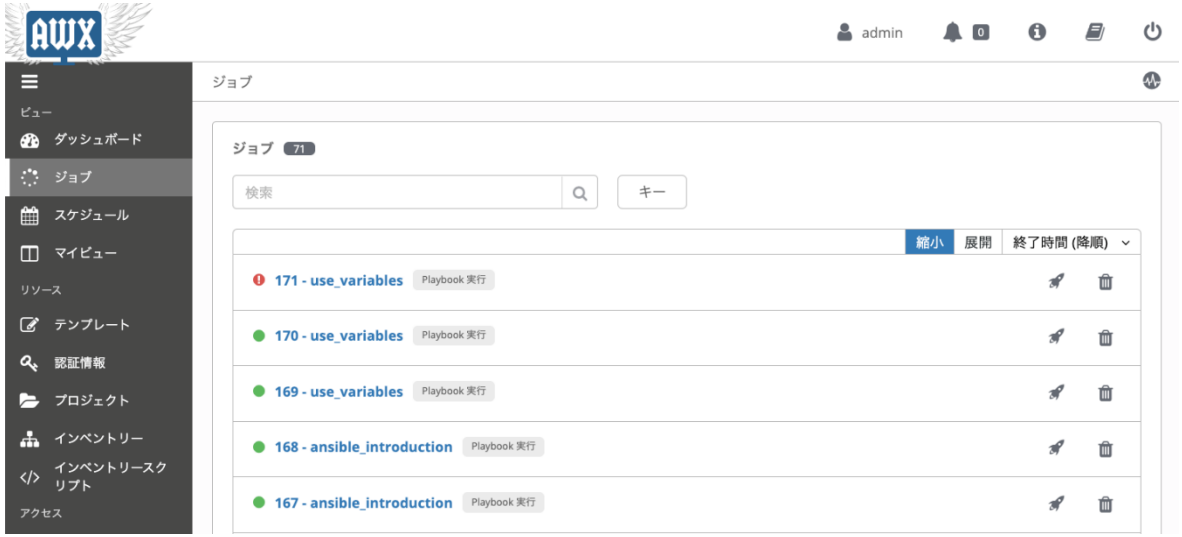
02 自動化システムの概要

- 以下を用いて全て内製で開発
  - クライアントはpythonを用いて作成
  - ワークフローエンジンとしてAWX (Ansible Tower)を利用
  - NW機器への設定はAnsibleを利用



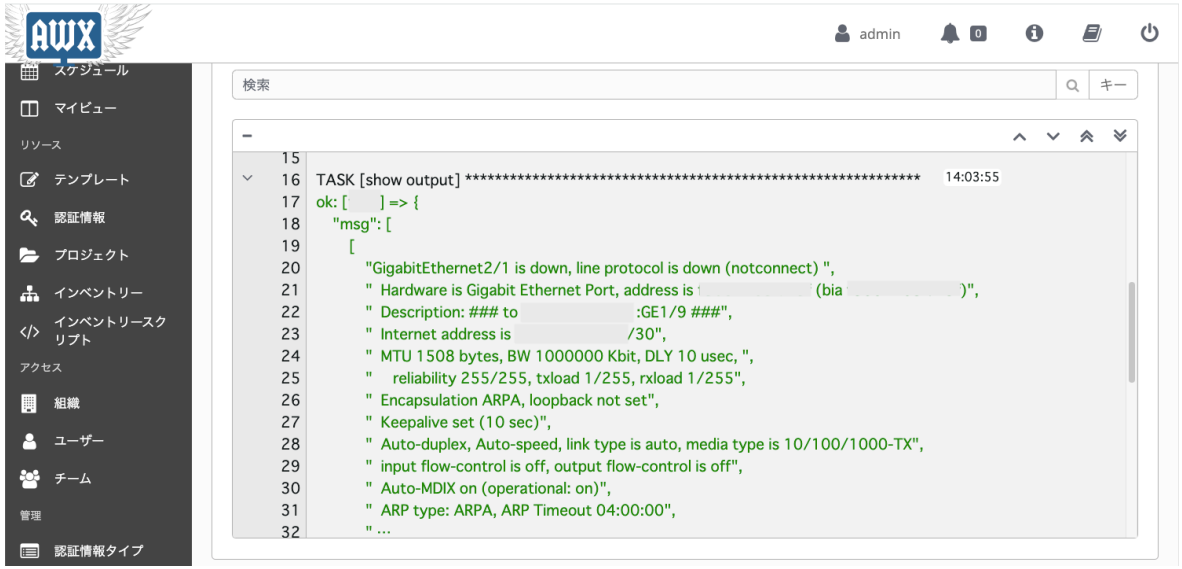
02. AWXによるAnsible実行環境の構築

- AWXを用いてAnsibleのplaybookをAPIで呼び出せるように構築
- Playbookの実行ログを保持/参照できるように



AnsibleのPlaybookを登録し、
GUIやAPIから実行できる

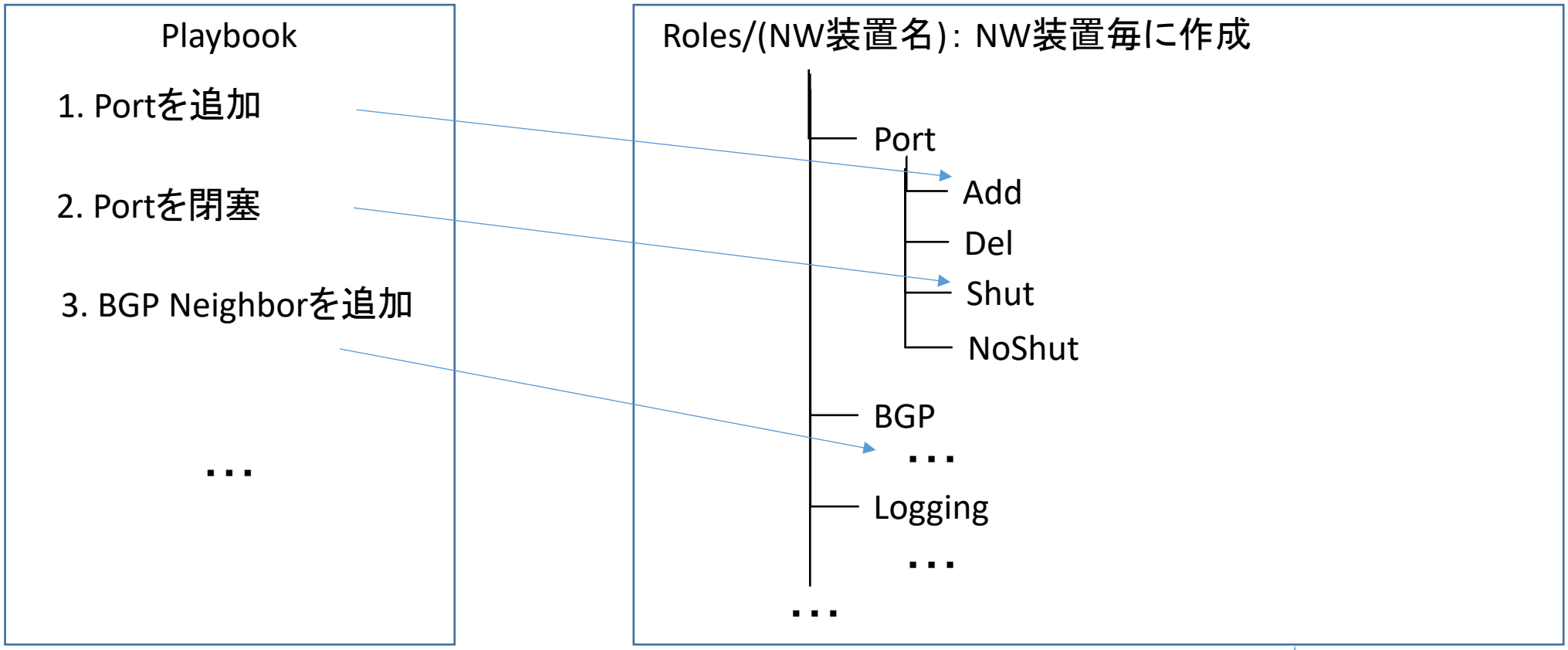
Playbookの実行履歴や、
実行の成功/失敗の確認ができる



Playbookの動作ログについて、
左図のような形で確認可能

02 Ansibleの構成

- 設定を記述する部分(Role)と手順を記述する部分(Playbook)を分離
- RoleはNW装置毎に作成し、その下に具体的な設定毎にRoleを作成
- Roleの単位でUnit試験を実施し、正しく設定できることを担保
  (1設定、1確認コマンド毎にテストを行う)
- PlaybookからはRoleを順々に呼び出すことで設定できるように



02 自動化による効果

- 自動化により以下の通り作業負荷軽減や作業品質向上を達成

Before

作業負荷

- 1マイグレあたりの作業量多い
  時間も多くかかる
- 装置も多く、画面をいったりきたり

作業品質

- 手動でコピー&ペースト
- 熟練の技術者による作業

その他

- 暗黙の手順が存在
- マイグレ作業や機器に関する
  ノウハウの属人化

After

作業負荷

- 手動設定の分量は半分以下に
- 作業時間も▲30分/台の削減
- python実行の1画面で作業可能

作業品質

- ツールによる実行で、
  コピペ間違いやノード間違いなし
- 誰が行っても高品質に作業できる

その他

- コードに落とす過程で、
  手順/判断の整理や標準化できた

02 自動化で苦労したこと/困ったこと

- 監視部門・監視システムとの連携
  - 作業前後でsh logを確認するが、どのログがあると問題？
  - 対象装置に監視アラートがでたときのエスカレ対応は？, etc…
  - 今回は上記は人で対応としたが、本来は監視システムと連携すべき

- 設計情報がDBできちんと管理されていないこと
  - アドレス/VLAN/構成情報が、APIで取得できる形で管理できていなかったため、都度Config等で調査し、Excelでの管理という形になっていた
  - 現在Netboxで管理できないか検討中

- Ansibleのテスト環境の構築やテストについて
  - Ansibleテスト専用の検証用環境が用意できず、検証装置を共用して使用
  - 他の検証とバッティングしてテストが通らなくなることも
  - 仮想ルータ等で専用の環境を用意すべき？
    皆さんどうしていますか？

ディスカッション

03 ディスカッション

- 自動化用の設定データの管理はどうしていますか？
  - 構成情報をモデル化 / 装置設定をモデル化 / その他
  - 設計DBとしてこのOSS/製品を利用している等あれば
- 手続き型ですか？宣言型ですか？
  - メリット / デメリット / 苦労したことなど
- 監視、テスト関係どうしていますか？
- 物理作業を伴う自動化をやっている方いますか？