

2026.08.28 ENOG91 @ 柏崎

(今さらながら) ルーターに設定を入れる話

さくらインターネット(株)
大久保 修一

自己紹介



さくらインターネット株式会社
サービス統括本部 大久保 修一

ENOG18(2012/12開催)以来、
14年ぶりに登壇させていただきます。
よろしくお願いします！

ENOG18 Meeting を開催しました

by [masakazu](#) • 2012年12月26日 • [0 Comments](#)

2012年12月21日(金)に ENOG18 Meeting を開催しました。
次回 ENOG19 Meeting は 2 月に三条市で開催を予定しています。詳細が決まり次第メーリングリストにてご案内いたします。

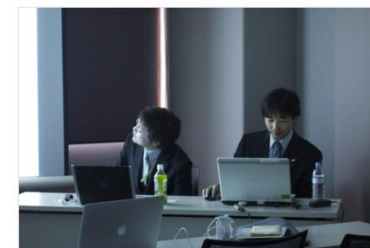
【 ENOG18 Meeting 議事録 】

- 日時: 2012年12月21日(金) 15:00 – 18:00
- 場所: 柏崎市文化会館アルフォーレ 中会議室 (新潟県柏崎市日石町4番32号)

勉強会

- “Netfilter に関するエトセトラ” [\[資料\]](#) – 外山 文規
- “OpenStack かじってみました” [\[資料\]](#) – 田畑 紀彦
- “さくらのクラウドインフラの紹介” [\[資料\]](#) – 大久保 修一
- “Unbound の紹介” [\[資料\]](#) – 高田 美紀
- “JANOG31 Meeting 開催のご案内” [\[資料\]](#) – 金子 康行

会合



検索...

最近の投稿

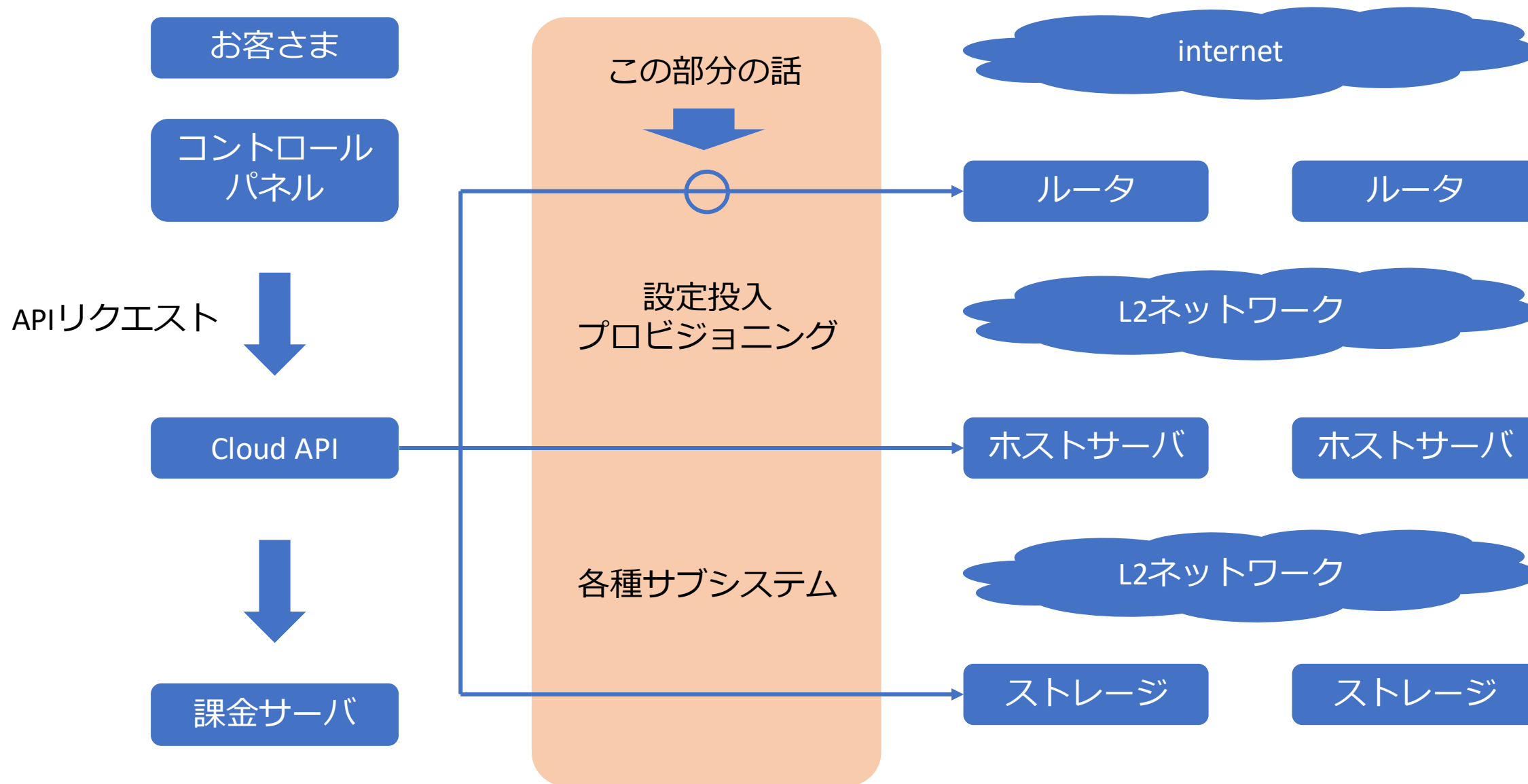
- [ENOG91 Meeting 開催のお知らせ](#)
- [ENOG90 Meeting を開催しました](#)
- [ENOG90 Meeting 開催のお知らせ](#)
- [ENOG89 Meeting を開催しました](#)
- [ENOG89 Meeting 開催のお知らせ](#)

<https://enog.jp/archives/850>

今回のネタ

- 「さくらのクラウド」のバックエンドの話
- ルータに設定を投入する処理があって、最近改善に取り組んでいる話をしようと思います
- レガシーとどう向き合っているのか、共有できればと思っています

さくらのクラウドのインフラ構成(ざっくり)



ルーター作成画面の例

お客さまがコンパネからインターネット接続ルーターを申し込み可能。
その場でルータ機器に設定を投入し、開通させている。

スイッチ追加

キャンセル 作成

名前

test-router

任意, 1~64文字

説明

任意, 1~512文字

タグ

任意, ENTERキーで追加

アイコン

- ▼

ルータ*

☐ いいえ ☒ はい

プリフィックス*

☒ /28 (16 IP) ☐ /27 (32 IP) ☐ /26 (64 IP)

/25 (128 IP) および /24 (256 IP)をご希望の方は[マニュアル](#)をご参照ください

帯域幅*

500Mbps共有 ▼

帯域プラン毎に月間転送量目安が設けられており、超過した場合トラフィック制限を行う場合がございます。

IPv6アドレス*

☐ 無効 ☒ 有効

開発Yゾーン ▼

リソースを検索...

サーバ

ストレージ ▼

ネットワーク ▲

スイッチ

パケットフィルタ

ブリッジ

ローカルルータ

AWS接続

アプライアンス ▼

グローバル ▼

シンプル通知 ▼

EventBus ▼

スイッチ » test-router

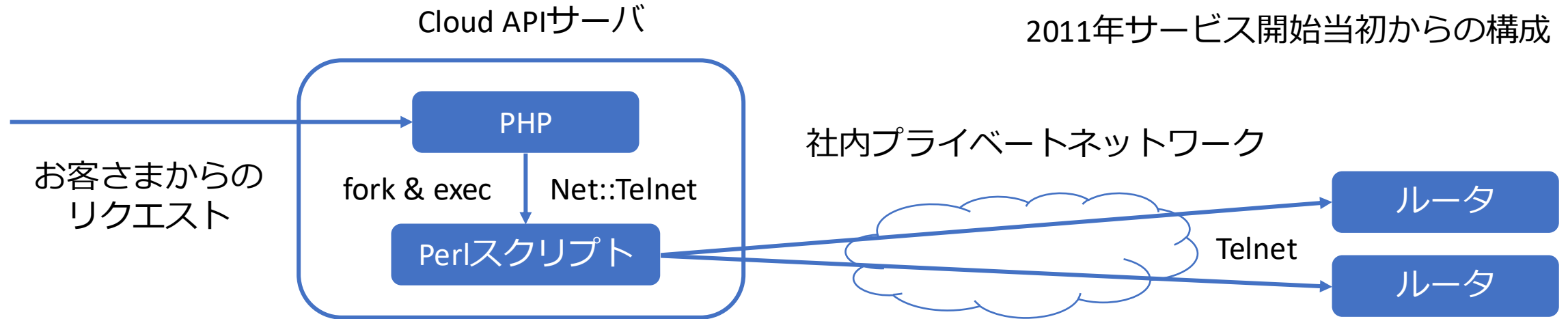
情報 サーバ (0) アプライアンス (0) トポロジ ルータ アクティビティ IPアドレス

リソースID	113800175924
帯域幅	500Mbps
ネットワークアドレス	133.125.133.32/28
割当可能範囲	133.125.133.36 ~ 46
ゲートウェイ	133.125.133.33
IPv6ネットワークアドレス	2401:2500:108:100f::/64
IPv6割当可能範囲	2401:2500:108:100f::4~
IPv6ゲートウェイ	fe80::1



当初のルータ設定処理構成

2011年サービス開始当初からの構成



- (雑な) Perlスクリプトで実装
 - テストもなく、新機能実装の足かせに (Perlが悪いわけではないです)
- APIサーバに同居している
 - APIサーバにPerlモジュールのインストールが必要。環境依存性
 - APIサーバが神状態 (こいつに脆弱性があると...)
- クレデンシャル管理の課題
 - Telnetパスワードをどう扱うか

他にもいくつか課題が

- 冗長化された2台のルータの設定不整合の可能性
 - 片方のルータの設定が失敗するとそのまま
 - 定期的に整合性チェックを行い、アラートを元に是正作業を実施
- そもそもTelnetがセキュリティ的に...
 - 社内プライベートネットワーク内でも暗号化通信がデフォルトに

改善のゴール

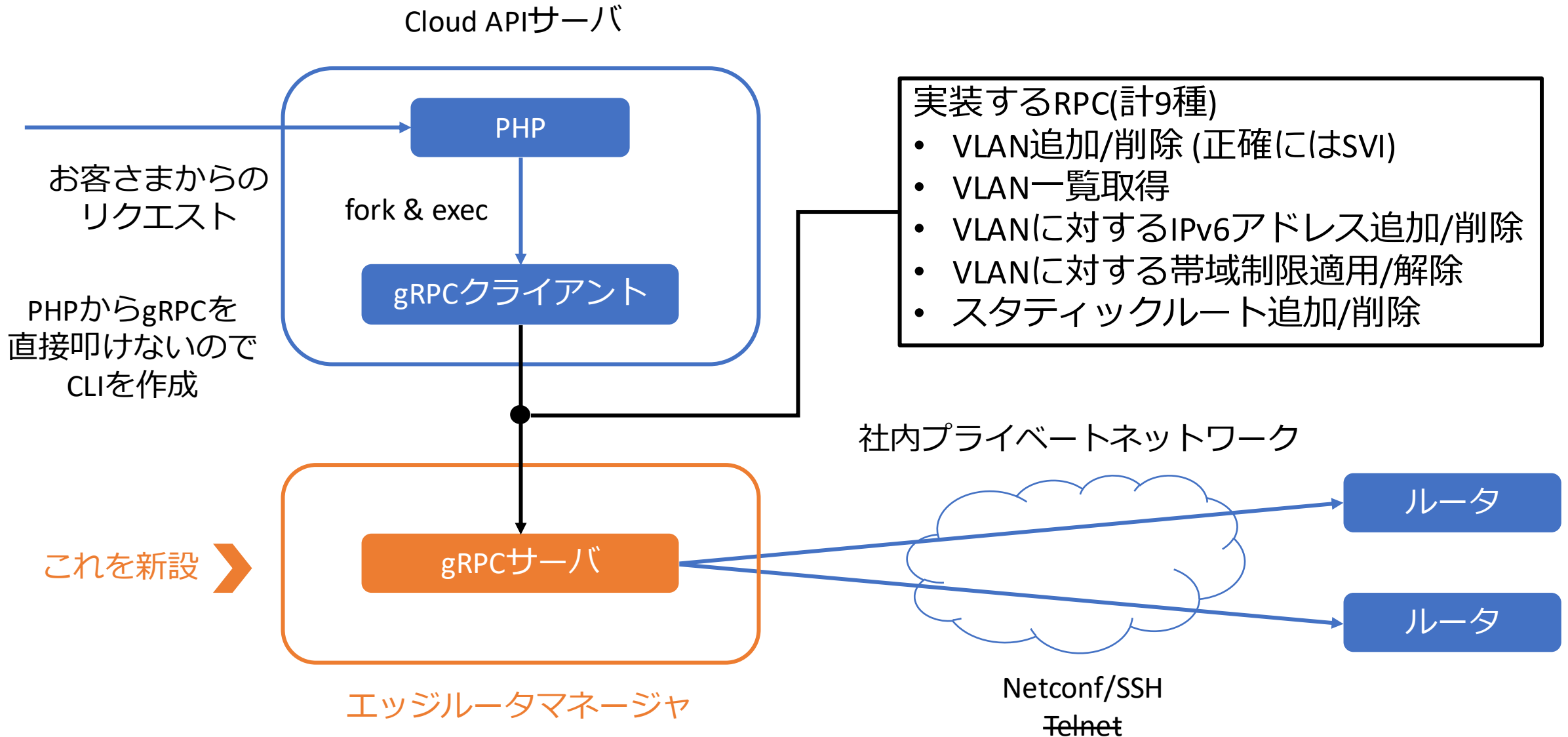
- 継続的にメンテナンスできる状態にしたい
- 責務を分離し疎結合にしたい(単一責任、最小権限の原則)



基本的な方針

- Go言語でリライトする
- ルータ設定処理用のサーバをAPIサーバから分離
- gRPCを用いてインターフェイスを明確化

改善後のアーキテクチャ



実装第一フェーズ

- 一旦動作は変えずにTelnetを維持しつつ移植
 - 早期に古いコード(Perlのコード)を捨てたい
 - Netconf/SSH対応は追って実施
- 同時期、新ゾーン開設が決まり、新機種への対応を実施
 - それまで：Cisco IOS(IOS-XE), Juniper QFXシリーズの2種類
 - 新機種：Juniper MXシリーズ 🎉
- 要検討事項
 - Goでの対話シェルクライアント実装
 - Juniper MXシリーズへの対応
 - サーバ分離に伴うクレデンシャル管理方法再検討

Goでの対話シェルクライアント実装

- Goで実装された“expect風”のモジュール
 1. <https://github.com/google/goexpect>
 2. <https://github.com/netflix/go-expect>
- (選択肢がほぼない。他にご存じの方いらっしゃったら教えてください)
- 1はアーカイブされており、メンテは終了しているもよう
- 2を導入することに
 - 若干クセがあったんですが、
 - うちのチームの方が使いやすいようにラッパーを作っていた

Juniper MXシリーズへの対応

- QFXとMXの違い
 - ほぼ一緒なんですが、
 - VLAN単位(お客さま毎)で帯域制限をかける際、
 - MXシリーズはlayer2 policerが利用できる
 - QFXは利用できず、苦肉の策としてaddress family毎の帯域制限をかけていた

QFXとMXの帯域制限設定の違い

QFXの場合 (VLAN毎にIPv4/IPv6, in/outのポリサーを作成し適用)

```
set groups tenants firewall family inet filter policer-vlan300-ipv4-in term 1 then policer 500M
set groups tenants firewall family inet filter policer-vlan300-ipv4-out term 1 then policer 500M
set groups tenants firewall family inet6 filter policer-vlan300-ipv6-in term 1 then policer 500M
set groups tenants firewall family inet6 filter policer-vlan300-ipv6-out term 1 then policer 500M
set groups tenants interfaces ae0 unit 300 family inet filter input policer-vlan300-ipv4-in
set groups tenants interfaces ae0 unit 300 family inet filter output policer-vlan300-ipv4-out
set groups tenants interfaces ae0 unit 300 family inet6 filter input policer-vlan300-ipv6-in
set groups tenants interfaces ae0 unit 300 family inet6 filter output policer-vlan300-ipv6-out
```

MXの場合 (L2ポリサーを利用可能。とてもシンプルに！)

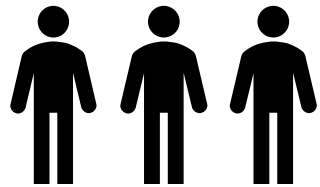
```
set groups tenants interfaces ae0 unit 300 layer2-policer input-policer 500M
set groups tenants interfaces ae0 unit 300 layer2-policer output-policer 500M
```

※ アドレスファミリーやVLAN毎にポリサーを作成する必要がない

GoのTemplateを用いて差異を吸収

クレデンシャル管理の改善

ソフトウェア開発のチーム



私は今ここに所属

ソースコードや
バックエンドサーバのメンテナンス



デプロイ

レポジトリ

エッジルータ
マネージャ

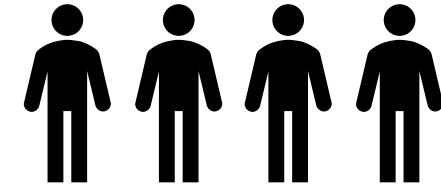
ログインパスワードは
知らされない



Telnetログイン・設定処理

このパスワードを
どう管理するか？

インフラ開発のチーム



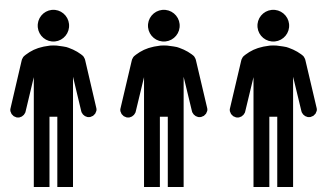
インフラの管理、オペレーション



ルータ群

クレデンシャル管理の改善

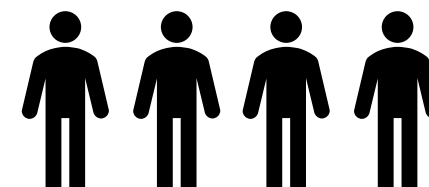
ソフトウェア開発のチーム



私は今ここに所属

ソースコードや
バックエンドサーバのメンテナンス

インフラ開発のチーム



インフラの管理、オペレーション

ログインパスワードは
知らされない



レポジトリ

デプロイ

エッジルータ
マネージャ

Telnetログイン・設定処理

ルータ群

このパスワードを
どう管理するか？



暗号化した
パスワード

yamlファイル中のシークレット情報を暗号化して格納



SOPS: Secrets OPerationS

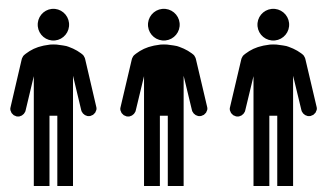
<https://github.com/getops/sops>

実装第二フェーズ

- TelnetからSSHへの移行
 - 対話シェル操作は一旦そのまま
- 並行処理と分散トランザクションの実装

クレデンシャル管理(SSHの場合)

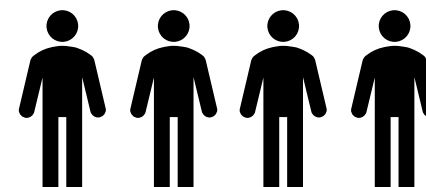
ソフトウェア開発のチーム



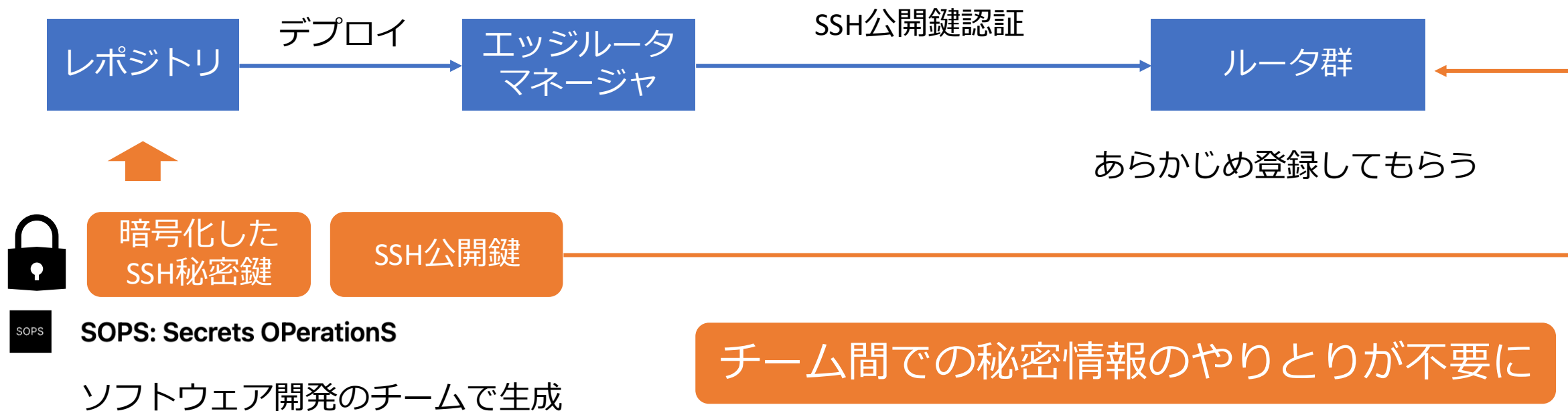
私は今ここに所属

ソースコードや
バックエンドサーバのメンテナンス

インフラ開発のチーム

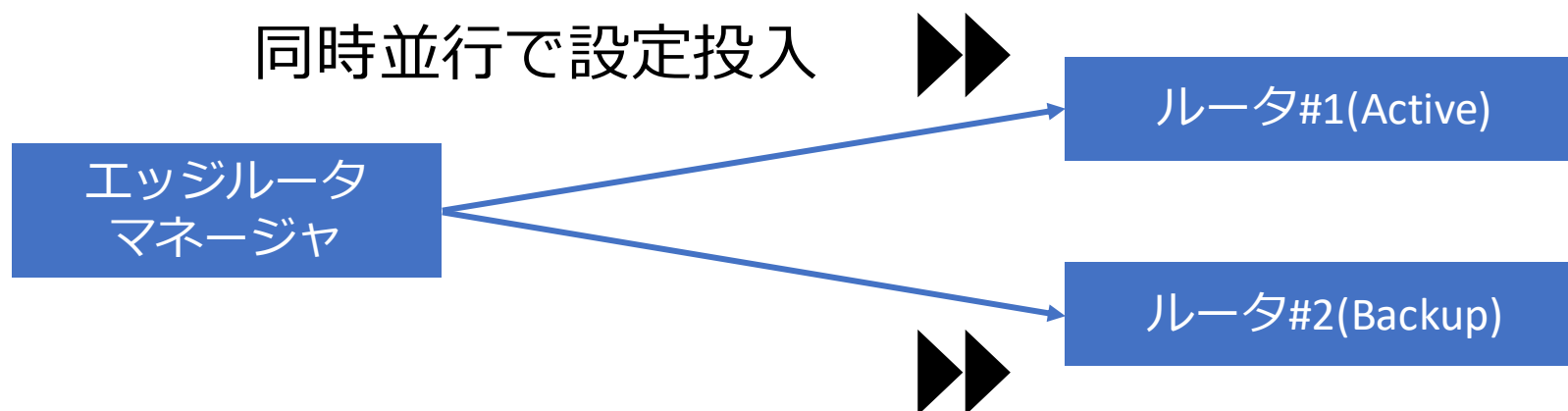


インフラの管理、オペレーション



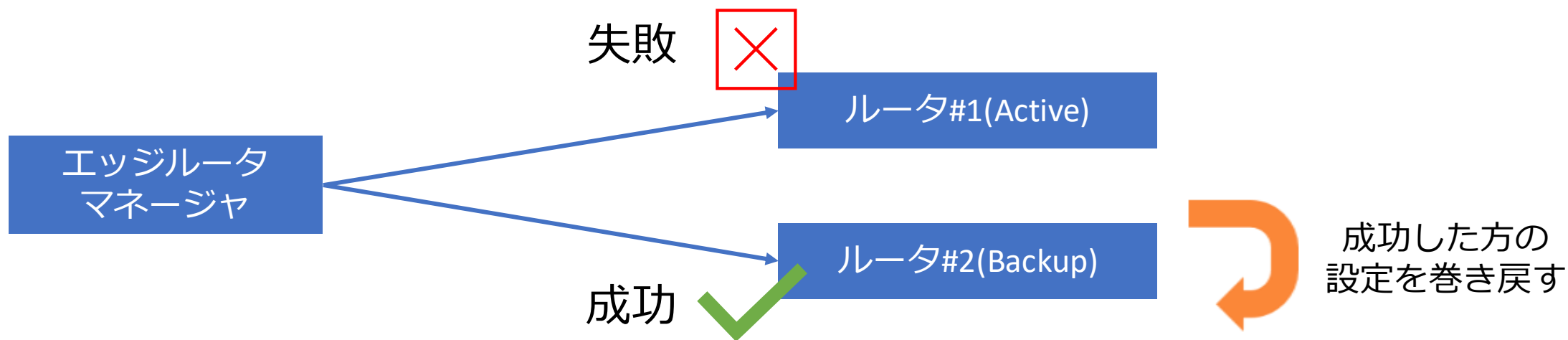
並行処理と分散トランザクションの実装

- 冗長化された2台の装置に対して、同時並行で設定処理を走行
 - 以前は2台をシリアルに実行していた
 - goroutineで並行処理を実装
 - コンパネ/API操作に同期実行となっている
 - お客さま操作をなるべくお待たせしないようにする効果



並行処理と分散トランザクションの実装

- フェイル時の設定ロールバック処理を実装
 - 片方のルータの設定が失敗した場合に、設定が成功したもう一方のルータの設定を巻き戻すように
 - 可能な限り設定の不整合を発生させない仕組み
 - ただし、ルータ自身にrollbackの仕組みがない機種もある
 - 補償トランザクションを実行するような動作とした



補償トランザクションの例

例：Cisco IOSで、VLAN設定の削除

- VLANの削除を実行

no int vlan 300	<= SVIの削除
no vlan configuration 300	<= 帯域制限設定の削除
no vlan 300	<= VLANの削除

- もう一方のルータの設定が失敗した場合、VLAN設定を復活させる(追加操作を行う)

interface Vlan300
ip address 192.0.2.2 255.255.255.0
ip helper-address vrf mgmtVrf 10.0.0.1
no ip redirects
no ip proxy-arp
standby version 2
standby 1 ip 192.0.2.1
standby 1 timers 10 30
standby 1 priority 255
standby 1 preempt
no shutdown

vlan configuration 300
service-policy input rate-limit-500M
service-policy output rate-limit-500M

設定を復活させるために、設定削除前にIPアドレスや帯域制限値を確認しておく必要がある
(地味にめんどくさい)

実装第三フェーズ

- 対話シェルからNetconfへの移行
- Junosの場合、CLIと同じsetコマンドやshowコマンドがそのままNetconfでも使える！
- xmlで書かなくてよい。我々オペレータとしてはわかりやすい
- プロビジョニングの仕組みを変えずに、対話シェルの部分のみをNetconfに置き換えが可能

show configコマンドをNetconfで叩く例

```
<rpc>  
<command format="text">  
show configuration interfaces | display set  
</command>  
</rpc>
```

リクエスト

```
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns:junos="http://xml.juniper.net/junos/22.4R0/junos">  
<configuration-information>  
<configuration-output>  
set interfaces et-0/0/0 description XXXX  
set interfaces et-0/0/0 vlan-tagging  
set interfaces et-0/0/0 unit 95 vlan-id 95  
set interfaces et-0/0/0 unit 95 family inet address 192.168.254.1/24  
set interfaces et-0/0/0 unit 2501 vlan-id 2501  
set interfaces et-0/0/0 unit 2501 family inet mtu 1500  
set interfaces et-0/0/0 unit 2501 family inet address 169.254.0.2/24 vrrp-group 1 virtual-address 169.254.0.1  
set interfaces et-0/0/0 unit 2501 family inet address 169.254.0.2/24 vrrp-group 1 priority 100  
set interfaces et-0/0/0 unit 2501 family inet address 169.254.0.2/24 vrrp-group 1 advertise-interval 5  
set interfaces et-0/0/0 unit 2501 family inet address 169.254.0.2/24 vrrp-group 1 accept-data  
</configuration-output>  
</configuration-information>  
</rpc-reply>  
]]>]]>
```

レスポンス

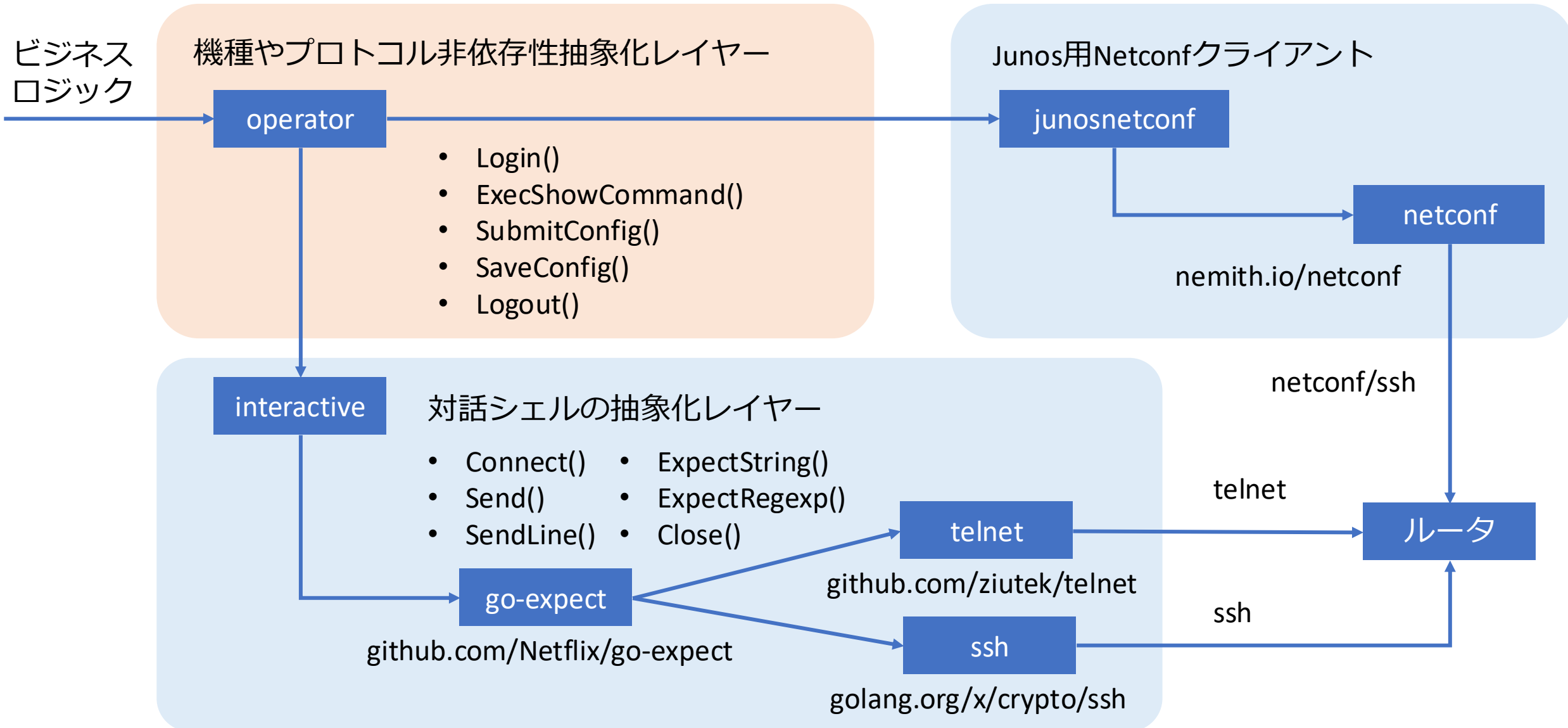
setコマンドでconfigをNetconfで流し込む例

```
<rpc>
<load-configuration action="set">
<configuration-set>
set interfaces et-0/0/0 unit 2502 vlan-id 2502
set interfaces et-0/0/0 unit 2502 family inet mtu 1500
set interfaces et-0/0/0 unit 2502 family inet address 169.254.1.2/24 vrrp-group 1 virtual-address 169.254.1.1
set interfaces et-0/0/0 unit 2502 family inet address 169.254.1.2/24 vrrp-group 1 priority 100
set interfaces et-0/0/0 unit 2502 family inet address 169.254.1.2/24 vrrp-group 1 advertise-interval 5
set interfaces et-0/0/0 unit 2502 family inet address 169.254.1.2/24 vrrp-group 1 accept-data
</configuration-set>
</load-configuration>
</rpc>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns:junos="http://xml.juniper.net/junos/22.4R0/junos">
<load-configuration-results>
<ok/>
</load-configuration-results>
</rpc-reply>
]]>]]>
```

リクエスト

レスポンス

Goのパッケージ構成 - ルータ設定処理部分



終わりに

- 長らく運用しているサービスについて、レガシーなシステムとどのように向き合っているか、弊社事例を紹介しました。
- 何かの参考になれば幸いです。
- ところで、
- 新しいネットワークサービスを開発中です。
- その話は合田さんからあるはず。中途採用も募集中です
- **ソフトウェア開発エンジニア（仮想ネットワーク基盤）**
- <https://www.sakura.ad.jp/recruit/midcareer/634/>



ご清聴ありがとうございました