運用者からのnetconfへの期待

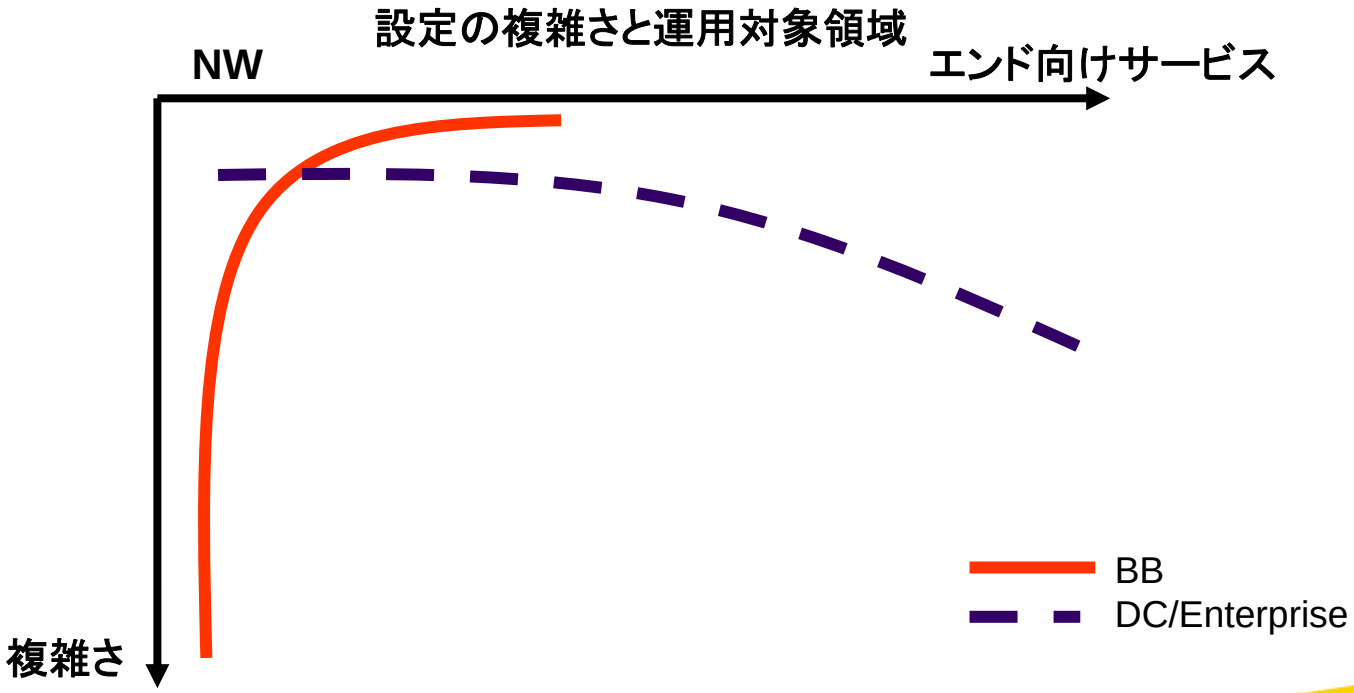
NTTコミュニケーションズ株式会社
桑原　大

Agenda

- BackboneとData Center/企業ネットワークとの違い
- Backbone運用からの視点
  - Backboneオペレーションの現状
  - Backbone運用者のnetconfへの期待
  - Netconfの応用的なUse Case
- DC/企業ネットワークからの視点
  - DC/企業NWオペレーションの現状
  - DC/企業NW運用者のnetconfへの期待
- Netconfへの今後への期待

Backbone NWとDC/Enterprise NWの違い

- Backboneはインフラとしての効率化と安定性を重視した設定・運用
  - 特定の設定が複雑になる
  - ルーティングは超重要
- DC/Enterpriseはエンド向けサービスを意識した設定・運用
  - 運用範囲・対象領域が広範囲にわたる
  - 機器固有の機能は余り必要ない（一般的な設定で事足りる）



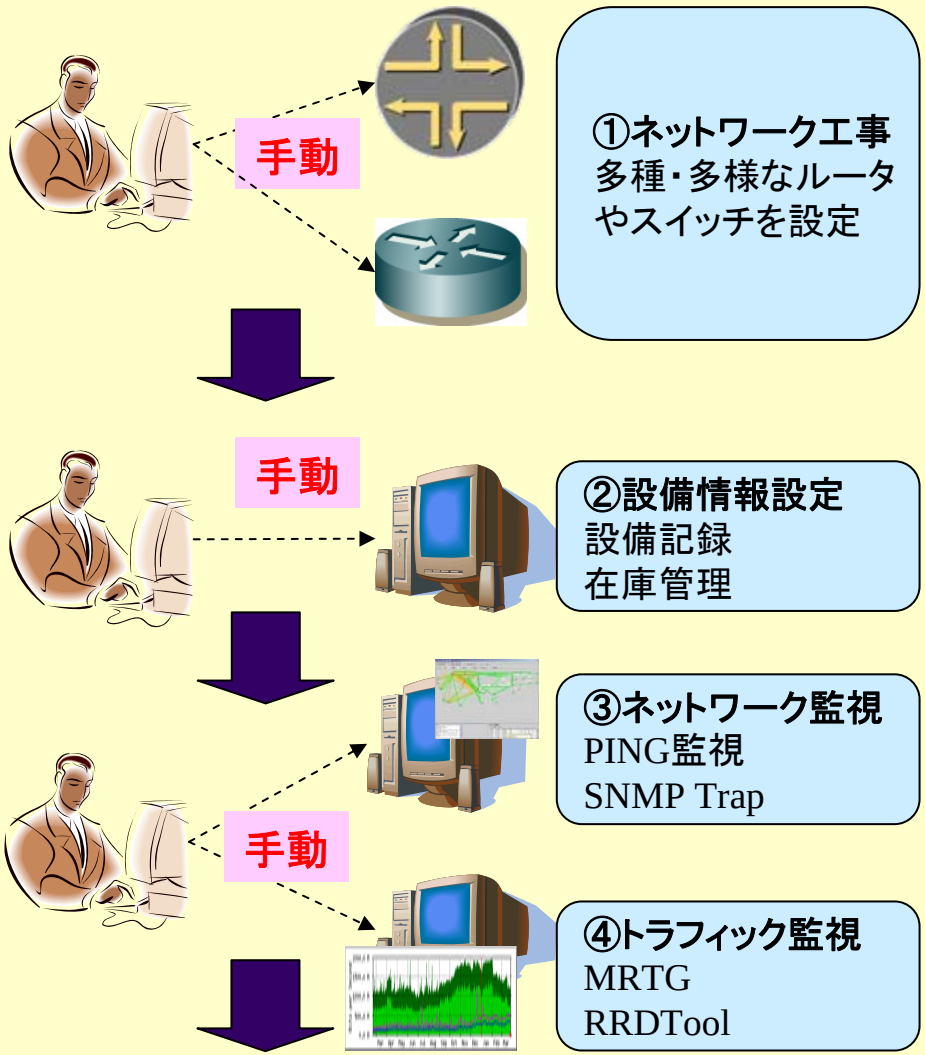
Backbone運用からの視点

Backboneオペレーションの現状

- 多台数のNW機器のオペレーション
- 複数ベンダーの機器で構成されたNW
  - EoL対策としての機器リプレイス
- NW間の接続ポリシーや経路制御を意識した複雑で専門的な設定
- 各種サーバを用いたNW運用
  - トラフィック情報の収集、ping監視、SNMP監視 etc
  - サーバに蓄えられた情報からNW機器の設定の一部を生成（例：IRRを利用した経路フィルタの作成）

Backboneオペレーションの現状

一般的な運用フロー



課題①

- ベンダーや機器ごとの知識・ノウハウの蓄積が必要

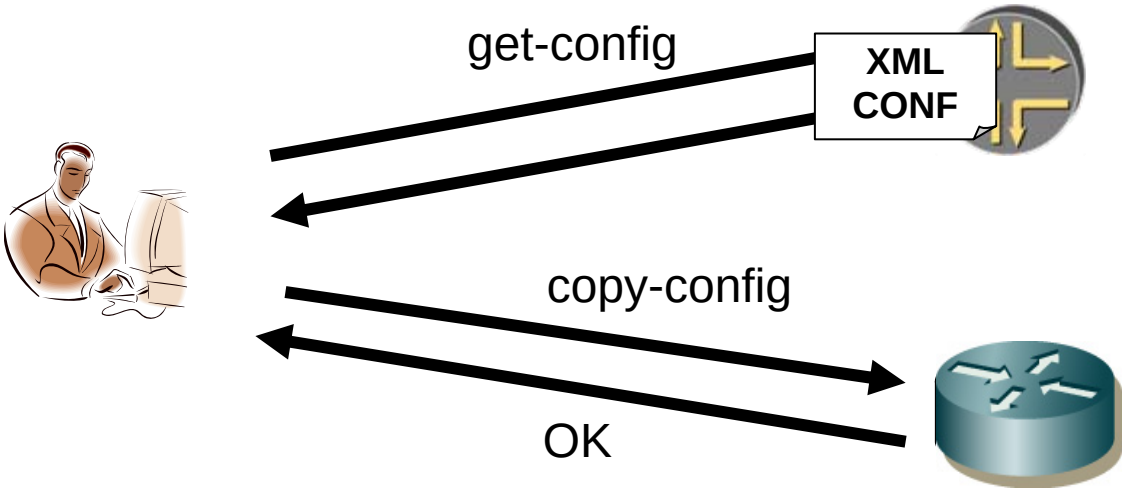
課題②

- 情報を個別に管理・入力する必要がある
  - ネットワーク全体の運用情報の整合性を維持するのが困難
  - 投入漏れも起こりうる
  - 重複データの投入に伴うオペレーション稼動の増加

Backbone運用者のnetconfへの期待

課題①に対するNetconfの適用

- ベンダー／機器固有の知識・ノウハウとの決別できる？
- 究極的には、Configuration Fileでの互換性

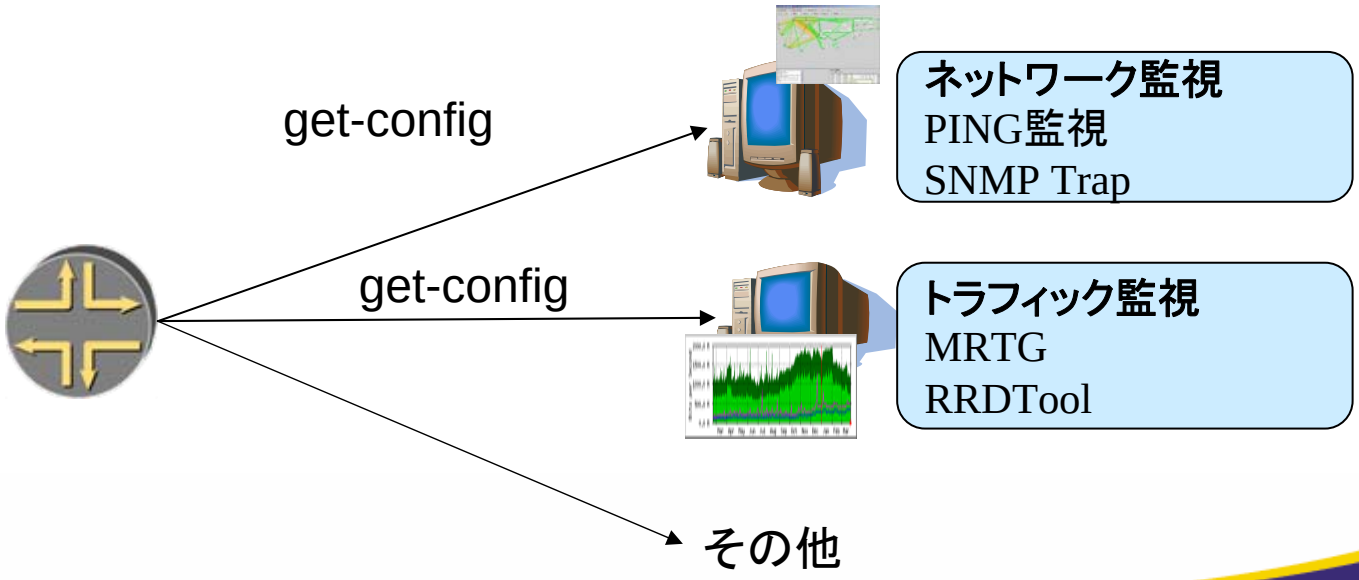


Content Layerが標準化／統一されれば実現可能？

Backbone運用者のnetconfへの期待

課題②に対するNetconfの適用

- NW機器から直接ネットワーク情報を取得
- XML ⇒ 各種管理システムの設定にマッピング
  - NW機器からの情報抽出で、データ投入の稼動削減
  - NW機器自体を情報の源泉とした管理

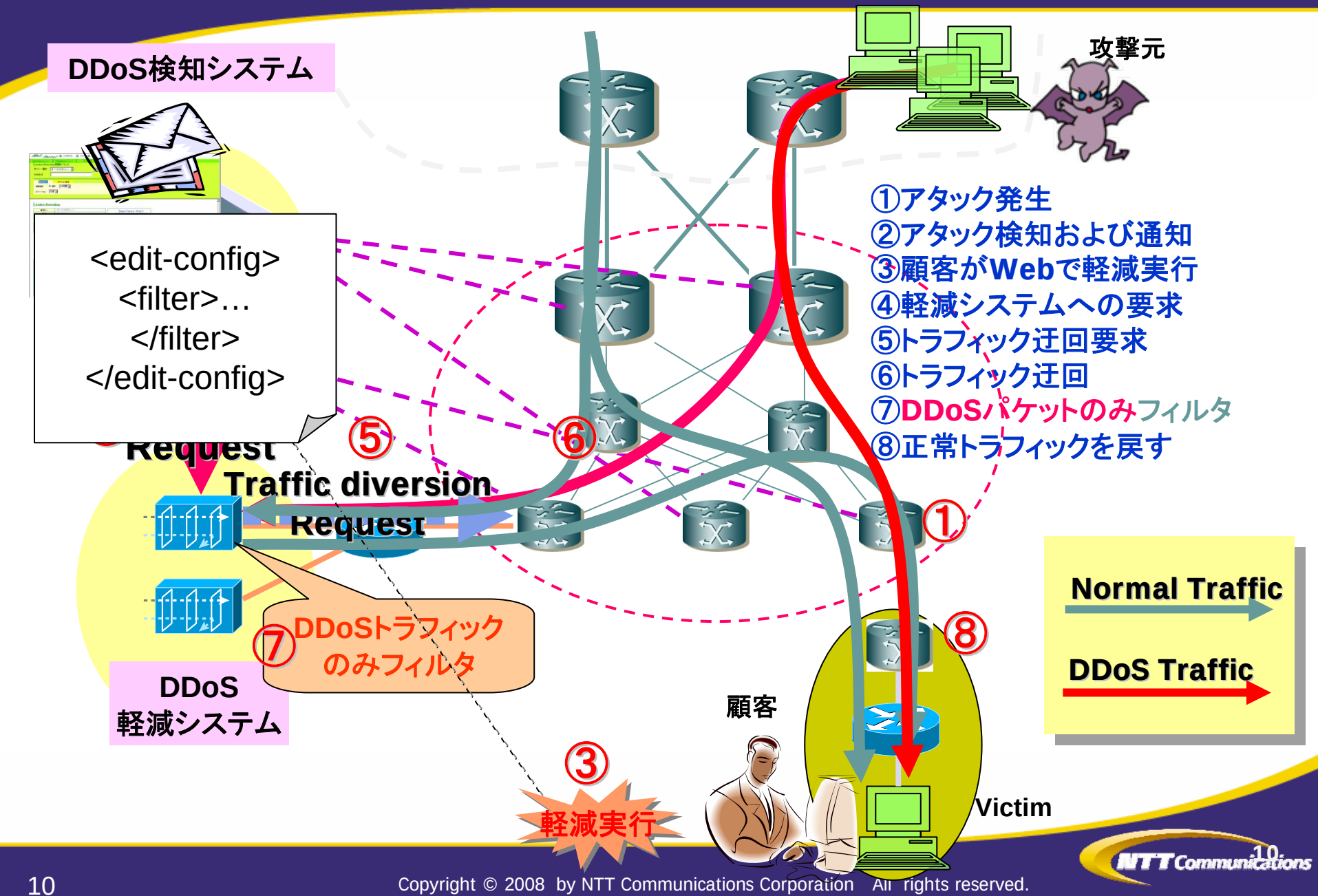


Netconfの応用的なUse Case

Machine-to-Machine Interfaceとして利用

- System⇔NW機器で人手を介さないやりとりが可能
- 部分的Configの即時投入が可能（例：Attackへの対処）
  - netflowやsflowを用いたDoSなどの異常トラフィックの検知技術は開発・商用化されつつある。
    - 検知後にルータへのフィルターの設定や、Traffic shaping等の緩和処置の設定を投入するMachine-to-Machineのインタフェースとしてnetconfを利用する
  - IRRに登録された情報と、実際のBGPの経路情報とを比較することにより、経路ハイジャックを検知
    - 経路フィルターの投入や、longer prefix経路をルータに投入するためのインタフェースとしてnetconfを利用する

DDoS軽減システム



DC/企業ネットワークからの視点

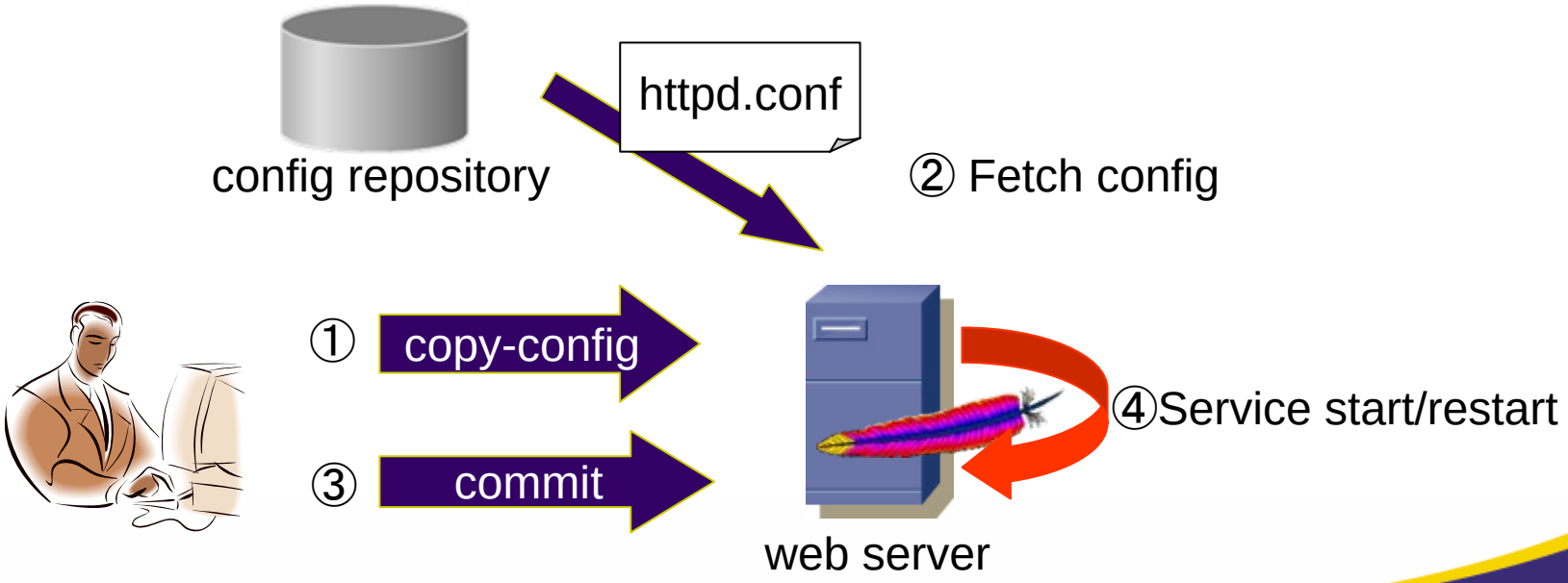
DC/企業NWオペレーションの現状

- Backbone以上に多様な機器／サービスを管理
  - Firewall, LB, WAF, IDS/IDP etc…
  - DNS, WWW, SMTP/POP/IMAP, File Server etc.
  - → 課題①：管理情報や設定情報の分散
- 運用者はオペレーションの専門家とは限らない
  - CUIやCLI に慣れていない
  - NW機器の全ての機能を利用するわけではない
    - 機能の全てを用いた“職人芸”は要求されない
  - → 課題②：利用しやすいユーザインタフェースが必要
- オペレーションをアウトソースする場合も
  - → 課題③：権限委譲による効率化とセキュリティ確保

DC/企業NW運用者のnetconfへの期待

課題①に適用：サービス管理

- 設定情報の一元管理と遠隔運用
- 多様なサービスを個別にXMLで管理するのは困難
  - inetdのような、Super Daemonを制御するのが現実的か？
  - Config RepositoryからのfetchとServiceの起動制御をnetconfで



DC/企業NW運用者のnetconfへの期待

課題②に適用：GUIからnetconfを利用する

- NetconfをGUIオペレーションの基盤として用いる
  - GUIからnetconfの処理を呼び出す
- GUIによる簡易なオペレーションを提供する
  - 家庭用BBルータを設定する感覚でNW機器を制御
- 複数のNW機器を統合されたGUIから制御
  - 少なくとも同じベンダー／機種であれば実現可能
    - Content Layerが統一されればマルチベンダーも？

DC/企業NW運用者のnetconfへの期待

課題③への適用：NW機器のセキュリティ強化

- サーバ（アプリケーション）を介したオペレーションにより、NW機器単位ではなく、より粒度の細かいAuthorization Modelを実現
  - NW機器の貧弱なAuthorization Modelを補完
    - 例：
      - 特定のインタフェースとVLANに限定された設定権の付与
      - 特定のIP Filterルールの設定変更権限の付与

Netconfへの今後の期待

Netconfへの今後の期待

- 効率的で統合的な運用の基盤となりうるNetconf
  - Content Layerの標準化／統一化が課題
    - SNMPにたとえると、Standard MIBが無い状況
      - 標準的なデータモデルが確立すれば利用用途が広がる
  - Configに表現されない値や設計思想の違いをどのように吸収するかも課題
    - システムのdefault値
    - NW機器による経路数の上限
  - ユーザレベルのAPIの充実
    - 運用ツール類の開発環境として充実したAPI
    - 複数のコンピュータ言語のサポート
    - ユーザレベルのAPIの統一
      - 機器やベンダーによって用いるAPIが異なると効果は半減
  - 運用ツールの開発基盤としての色が濃い
    - 運用者にとって直接的なメリットが提示されることを期待
      - 対応機器の増加、オペレーションツールの実装の普及