IIJ
Internet Initiative Japan

Ongoing Innovation

[パネル討論]
NETCONFの現状と今後

新 麗（あたらし れい）
IIJ技術研究所
ray@iijlab.net

Today’s talk

- ネットワークシステムの将来像
- ネットワーク設定プロトコル標準化の背景
- NETCONFの概要
- ベンダの対応状況

IIJ
Internet Initiative Japan

Ongoing Innovation

ネットワークシステムの将来像

ネットワークシステムのコンポーネントの多様化

- ネットワーク機器
  - ルータ
  - スイッチ
  - 無線基地局など
- コンピュータ機器
  - メールサーバ
  - Webサーバなど
- ストレージ

- ポリシー
  - セキュリティ

ネットワーク管理の将来像

- ルータなどネットワーク機器の自動設定
- 運用情報、設定情報の収集と解析
- 一元管理
- サーバ類とネットワーク機器の連携および統合管理

一括管理、自動化による利点

- 一括管理による利点
  - システム全体が把握しやすくなる
  - 関連する情報をリンクできる
  - 作業を一連の流れとして行える
- 自動化による利点
  - 運用ミスが減る
  - オペレータの負担が減る
  - 変更などの対応が早くなる
- 結果として、運用コストが下がり、信頼性が上がる

IIJ
Internet Initiative Japan

Ongoing Innovation

ネットワーク設定プロトコル標準化の背景

IETF IAB Network Management Workshop

- 2002年6月に開催されたネットワーク管理に関するワークショップ
  - ネットワーク運用者とプロトコル開発者が話し合う
  - IETFとして取り組むべきネットワーク管理の課題を抽出
- ネットワーク管理に関係する技術をリストアップ
- 運用者が必要とするものを整理
- RFC3535

ネットワーク管理に関係する技術(抜粋)

- SNMP/SMI/MIB
  - 監視には適当で広く普及している
  - データが多いと検索に時間がかかる
  - 簡単な検索やplaybackがない
- CLI (Command Line Interface)/TELNET/SSH
  - 運用者が慣れていて使いやすい
  - データモデルがない
  - ベンダーごとに異なる
- XML
  - マシン可読で構造が書ける
  - 冗長である

コンピュータ分野での統合管理

- CIM（Common Information Model）
  - DMTF（Distributed Management Task Force）で定義されている、コンピュータデバイスと管理インタフェースの仕様
  - 情報管理にはXMLを利用し、他の管理モデルとの融合がしやすくなっている。
  - スキーマが複雑で、ネットワーク管理にそのまま適用できるかは未知数

ネットワーク設定プロトコルnetconfの登場

- 2002年7月: IETF@横浜にて XML configuration BoF開催
  - xmlconf の名前でJuniperから提案
- 2003年3月: IETF@San Francisco にて netconf BoF開催
- 2003年7月: IETF@Vienna で第1回WG meeting
- 2006年12月: 4本のドラフトがRFCとなり、プロトコルの基本部分が標準化される

NETCONF規定の背景

- キャリア1
  - エンジニアは中央拠点にしかいないので、コアルータの様子を監視、設定する。(TE含めて) 遠隔からSSH/telnetもあるが、もっと安全に柔軟にやりたい
- キャリア2
  - エッジルータつまり顧客収容ルータの各ポートのenable/disableをweb i/f でやり、確認のマークをするなどの従来の交換機の開通業務に近いイメージでできるようにすること
- 運用におけるトラブル対応
  - ファイアウォールルールの一斉書き換え
  - 監視との連携
- 管理コストの削減、人的ミスによるトラブルの防止

ネットワーク機器に求められる機能

- 遠隔で制御できること
- 設定情報を一括管理できること
- セキュアに設定ができること

IIJ
Internet Initiative Japan

Ongoing Innovation

NETCONFの概要

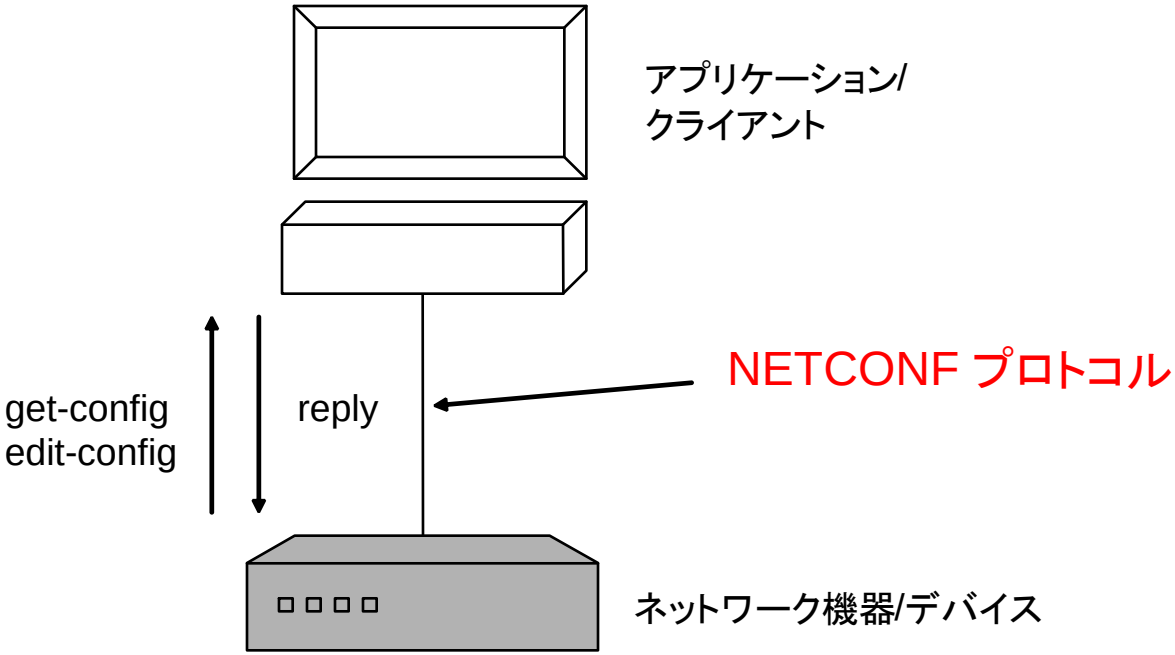
NETCONFの目的と特徴

- ネットワーク機器の設定を行うプロトコル
  - 遠隔制御
  - 自動化
- XMLベースのプロトコルである
  - Webと親和性がよい
  - データベースで設定情報を管理できる
  - 他のXMLベースの情報と相互交換がしやすい

XML採用の利点

- データとフォーマットの分離により再利用性が高まる
- 異なる種類のデータをXMLで保存しておくことで、既存のXMLツールを利用して解析が可能となる
- 関係付け、意味づけなどのモデル化を追加していくことが可能となる
- プロトコルやログより抽象度の高い解析が可能となる

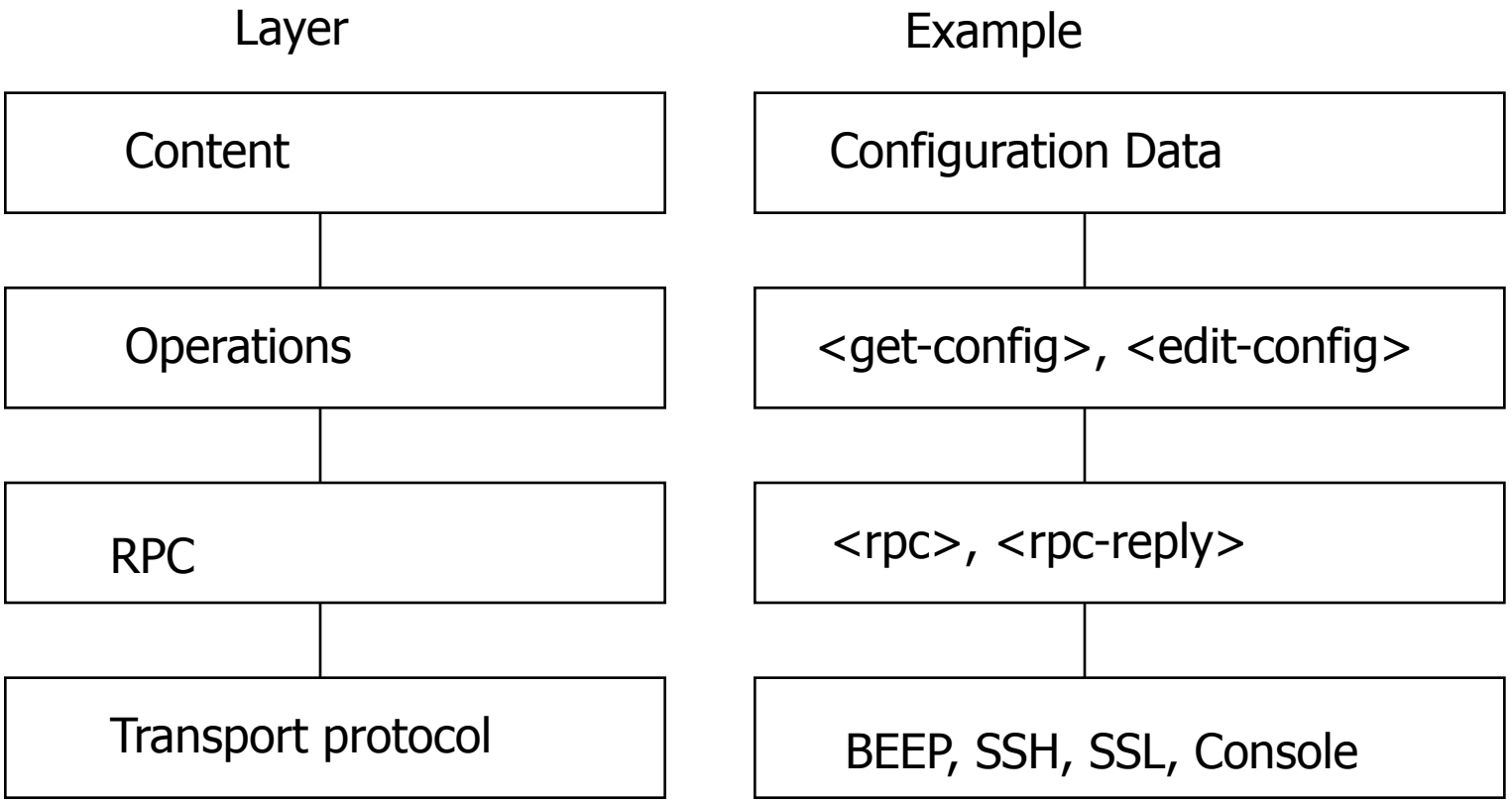
NETCONF プロトコル



Netconf のRFC（Request For Comment）

- RFC4741
  - NETCONF Configuration Protocol
- RFC4742
  - Using the NETCONF Configuration Protocol over Secure Shell (SSH)
- RFC4743
  - Using the Network Configuration Protocol (NETCONF) Over the Simple Object Access Protocol (SOAP)
- RFC4744
  - Using the NETCONF Protocol over Blocks Extensible Exchange Protocol (BEEP)

NETCONFプロトコルレイヤ



Transport Protocol

- 設定情報を送るトランスポートプロトコル
- 新しいプロトコルは作らず既存のものを使う
- NETCONF では以下のように規定されている
  - SSHは必ずサポートする (MUST)
  - SOAP, BEEPは必須ではないが、サポートしてもよい

RPC layer

- NETCONF インタフェースの呼び出し手続きを記述
- RPCを利用する
- <rpc>, <rpc-reply> などが規定されている

Operations layer

- ネットワーク機器に対する操作を規定する
- 主な操作は以下の通り
  - <get-config>: 設定情報の取得
  - <edit-config>: 情報の書き換え
  - <copy-config>: 設定情報のコピー
  - <delete-config>: 設定情報の削除
  - <lock>,<unlock>: 設定情報の書き換え禁止とその解除

Content layer

- 実際の設定内容を規定する
- IETFではまだ正式には議論されていない
  - データモデルとして、WGにならないレベルでいろいろ活動はある
- ベンダごとに異なるため、標準化は難航すると思われる

NETCONFプロトコルの例

```
<rpc message-id="101"
    xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <get/>
</rpc>

<rpc-reply message-id="101"
    xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <data>
 <!-- ... entire set of data returned ... -->
    </data>
 </rpc-reply>
```

netconf WGの動向

- 最初の目標は終了しRFCを4件発行、1件が最終段階
  - NETCONF event notification
- 2008年3月に目標を再設定しchairも交代
- 新しい目標として4件の項目を設定
  - Fine-grain locking
  - NETCONF monitoring
  - Schema advertisement
  - NETCONF over TLS

netmod WG

- NETCONF Data Modeling Language
- 2008年3月に発足
- NETCONF Data Model を記述するための言語を決める(作る)ことが目的

ベンダの対応状況

ベンダの動き

- NETCONFプロトコルは Juniper ベース
- netconf WG の元Chair の一人は元Cisco
- 2006年頃から、キャリア向け大型ルータから対応が始まっている
- 日本では AlaxalA Networks が初期から標準化に関わり、エンタープライズ向け製品も提供している

ベンダの対応状況

- AlaxalA
  - ON-API (Open Networking-application programming infetface)
  - JAVA API と SDK
- Cisco
  - NX-OS 4.0
- Juniper
  - **JUNOS (XMLインタフェース)**
  - **netconf API Perl Client**

今後の動向

- ネットワーク機器本体のNETCONF対応は進みつつある
- 機器よりもAPIの柔軟性が今後の可能性を左右する
  - 管理の自動化やシナリオベースの連携プログラムが書きやすい
- XMLベースであることでデータ処理の可能性
- 標準化動向については、データモデルの標準化がカギ