RESTで休めない話！

日本大学
相川成周（あいかわしげちか）

相川成周（あいかわしげちか）

仕事

- エンジニア
- インターネット全般
  - BGP（AS10014）
  - ネットワーク・サーバ・セキュリティ
- クラウド
  - Google G Suite
    - アカウント数10万以上
  - パブリック AWS，GCP
  - プライベート VMware, Nutanix
- ほぼぼっちで設計・運用・管理
  - 絶望的な人不足
  - 運用の自動化が急務

趣味

- 自転車，トライアスロン，オートバイ
- スポーツ観戦

JUNOSと私

- JUNOS歴2年半
  - IOS歴20年超
- 28拠点
  - 約50台
- 推奨バージョン利用
  - 15.1系

JUNIPER NETWORKS

Case Study

全国27拠点、総距離1,700kmをつなぐ
日本最大の学内ネットワーク
シンプルかつパワフルなインフラを実現

サマリー

導入組織：
学校法人日本大学

所在地：
東京都千代田区九段南四丁目８番24号

設　置：
1889年（大学設置1920年）

1889年（明治22年）に前身である日本法律学校を開設。1903年に日本大学へと改称し、1920年に大学令によって大学として設立された。通信教育部・短期大学を含めた学生数は約７万５,000人を数え、卒業生は114万人を超える※1。全国に拠点を持ち、建物延べ面積は1.7平方キロメートル、図書蔵書５万万冊超は私立大学トップ※2。名実ともに日本最大の大学である。

※1：2017年３月現在、※2：2017年４月現在

http://www.nihon-u.ac.jp

学校法人日本大学
本部 管財部
IT管理課 課長
吉田 清氏

学校法人日本大学
本部 管財部
IT管理課
相川 成周氏

日本大学は、16学部９０学科のほか大学院や短期大学、高等学校、中学校などを有し、組織的にも国内最大級の規模を誇っている。同学では、横浜のデータセンターを中心に学部や病院、中学・高校を含む27拠点を接続する「日本大学ネットワーク（日大WAN）」を形成し、インターネット接続などのサービスを提供している。近年、ネットワークパフォーマンスへのニーズが急速に高まり、1Gbps/10Gbpsへのアップグレードを計画。中核となるルーターとして、ジュニパーネットワークスの「MXシリーズ」と「SRXシリーズ」を採用した。

日本大学は、前身である日本法律学校が創設された明治22年より続く長い歴史を持ち、学生数では国内トップ、学部・学科数や建物延面積、図書蔵書数などでもトップクラスを誇り、まさに日本最大の大学である。

2019年に創立130年を迎える同学は、「自主創造」を教育理念として「日本一教育力のある大学」を目標に、さらなる教育環境の整備・強化に注力しているところだ。記念事業の一環として、2016年に危機管理学部やスポーツ科学部を新設。新しい学部教育を通じて「時代が必要とする人材、自主創造型パーソンの育成」を目指している。

これほど多拠点を持つ組織ともなると、一般的な大学とは異なるICT戦略を採っている。日本大学では、学部、病院、高校・中学校はある程度裁量が任せられ、独自性を持って運用されている。そのため、同学の本部IT部門は学内ITコンサルティングの１面を持つ。

特にユーザー数は学生・生徒、教職員等を含めて10万人規模となるため、ソフトウェアライセンスもユーザー数での契約形態ではデメリットと感じられる。そのため、なるべくオープンソースソフトウェアなどを活用し、ユーザー数に依存しないソリューションを選定しているとのことだ。

特に問題となるのはネットワークだ。各学部等の独自性を認めながらも、組織としては統制を取っていかなければならない。

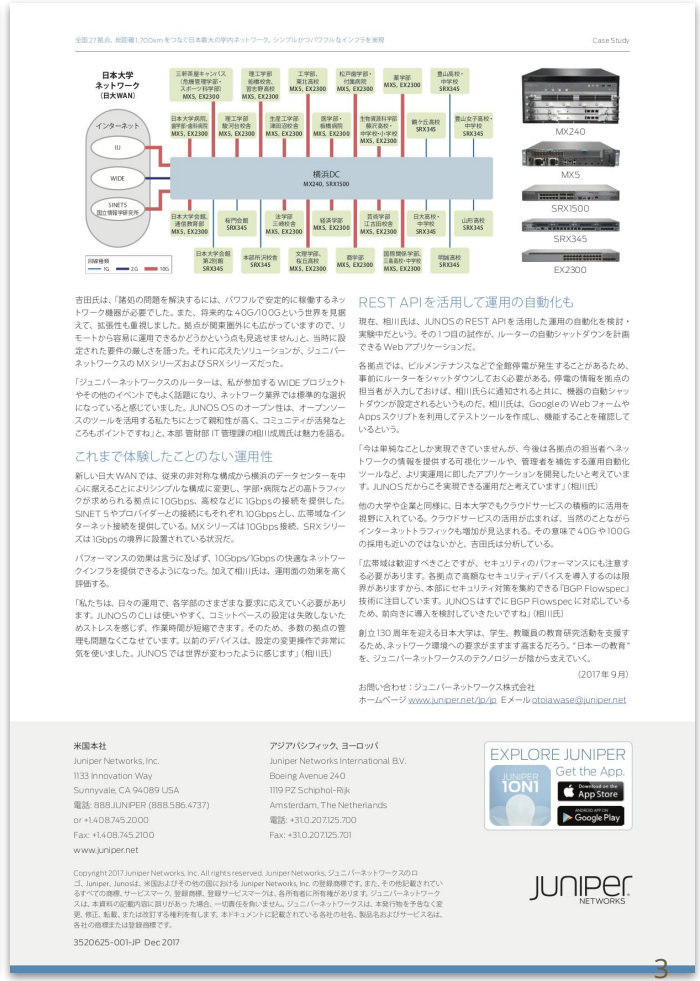
「安定的で快適、かつ自由に利用できるインフラを求められる一方で、安全性も確保しなければなりません。そこで私たちは、各拠点を束ねる“日本大学ネットワーク（日大WAN）”を構築し、セキュリティレベルの均一化を図っています」と、本部 管財部 IT管理課 課長の吉田清氏は説明する。

性能・運用性・安定性の総合力を重視

日大WANは、1994年ごろに構築され、アップデートを繰り返して本日まで運用されてきた。日本大学では、ほぼ学部ごとにキャンパスがあり、病院・高校やデータセンターを含めて27拠点が、日大WANに接続されている。日大WANは横浜に設置されたデータセンターを中心に、SINET５やプロバイダなどにも接続されている。各拠点は、日大WANを介してインターネットと接続する。

日大WANは、最近まで100Mbpsをベースに各拠点と接続していた。しかし、昨今のデバイスやアプリケーションの進化によって、トラフィック強化へのニーズが急速に高まっていた。大学はもちろん、中学・高校ではタブレットを活用した授業が進み、遅延などのトラブルが問題視されつつあった。場合によっては、各組織で独自にインターネット接続を契約し、帯域の問題に対処していた事実もあった。

そこで日本大学では、拠点との接続回線を1Gbpsまたは10Gbpsへと一気に増強、帯域の課題を解決する計画を立てた。魅力のあるネットワークインフラを提供すれば、拠点ごとのインターネット契約を解消し、再び統制を図ることができる。加えて、非対称化していたネットワークトポロジーをよりシンプルなものに改訂し、管理性の向上を図る必要もあった。



全国27拠点、総距離1,700kmをつなぐ日本最大の学内ネットワーク、シンプルかつパワフルなインフラを実現

Case Study

吉田氏は、「諸処の問題を解決するには、パワフルで安定的に稼働するネットワーク機器が必要でした。また、将来的な40G/100Gという世界を見据えて、拡張性も重視しました。拠点が関東圏外にも広がっていますので、リモートから容易に運用できるかどうかという点も見逃せませんと、当時に設定された要件の厳しさを語った。それに応えたソリューションが、ジュニパーネットワークスのMXシリーズおよびSRXシリーズだった。

「ジュニパーネットワークスのルーターは、私が参加する WIDE プロジェクトやその他のイベントでもよく話題になり、ネットワーク業界では標準的な選択になっていると感じていました。JUNOS OSのオープン性は、オープンソースのツールを活用する私たちにとって親和性が高く、コミュニティが活発なところもポイントですね」と、本部 管財部 IT 管理課の相川成周氏は触れる。

これまで体験したことのない運用性

新しい日大WANでは、従来の非対称な構成から横浜のデータセンターを中心に据えることによりシンプルな構成に変更し、学部・病院などの高トラフィックが求められる拠点に10Gbps、高校などに1Gbpsの接続を提供した。SINET５やプロバイダとの接続にもそれぞれ10Gbpsとし、広帯域なインターネット接続を提供している。MXシリーズは10Gbps接続、SRXシリーズは1Gbpsの境界に設置されている状況だ。

パフォーマンスの効果は言うに及ばず、10Gbps/1Gbpsの快適なネットワークインフラを提供できるようになった。加えて相川氏は、運用面の効果を高く評価する。

「私たちは、日々の運用で、各学部のさまざまな要求に応えていく必要があります。JUNOSのCLIは使いやすく、コミットベースの設定は失敗しないためストレスを感じず、作業時間が短縮できます。そのため、多数の拠点の管理も問題なくなせています。以前のデバイスは、設定の変更操作で非常に気を使いました。JUNOSでは世界が変わったように感じます」（相川氏）

REST APIを活用して運用の自動化も

現在、相川氏は、JUNOSのREST APIを活用した運用の自動化を検討・実験中だという。その1つ目の試作が、ルーターの自動シャットダウンを計画できるWebアプリケーションだ。

各拠点では、ビルメンテナンスなどで全館停電が発生することがあるため、事前にルーターをシャットダウンしておく必要がある。停電の情報を拠点の担当者が入力しておけば、相川氏らに通知されると共に、機器の自動シャットダウンが設定されるというものだ。相川氏は、GoogleのWebフォームやAppsスクリプトを利用してテストツールを作成し、機能することを確認しているという。

「今は単純なことしか実現できていませんが、今後は各拠点の担当者へネットワークの情報を提供する可視化ツールや、管理者を補佐する運用自動化ツールなど、より実運用に即したアプリケーションを開発したいと考えています。JUNOSだからこそ実現できる運用だと考えています」（相川氏）

他の大学や企業と同様に、日本大学でもクラウドサービスの積極的に活用を視野に入れている。クラウドサービスの活用が広まれば、当然のことながらインターネットトラフィックも増加が見込まれる。その意味で40Gや100Gの採用も近いのではないかと、吉田氏は分析している。

「広帯域は歓迎すべきことですが、セキュリティのパフォーマンスにも注意する必要があります。各拠点で高額なセキュリティデバイスを導入するのは限界がありますから、本部にセキュリティ対策を集約できる「BGP Flowspec」技術に注目しています。JUNOSはすでにBGP Flowspecに対応しているため、前向きに導入を検討していきたいですね」（相川氏）

創立130周年を迎える日本大学は、学生、教職員の教育研究活動を支援するため、ネットワーク環境への要求がますます高まるだろう。「日本一の教育」を、ジュニパーネットワークスのテクノロジーが陰から支えていく。

（2017年９月）

お問い合わせ：ジュニパーネットワークス株式会社
ホームページ www.juniper.net/jp/jp Eメール otoiawase@juniper.net

米国本社
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
電話: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

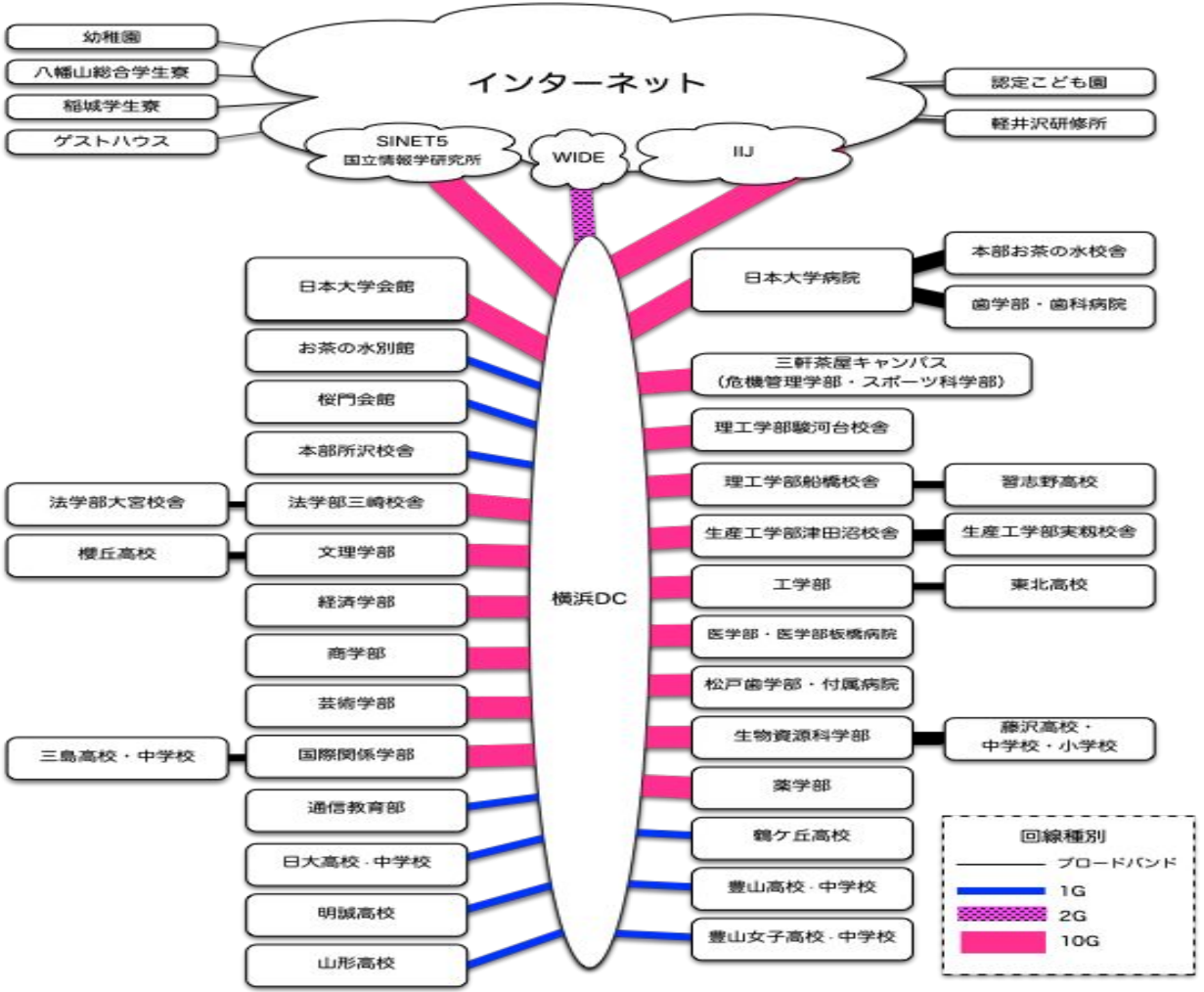
アジアパシフィック、ヨーロッパ
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
電話: +31.0.207.125.700
Fax: +31.0.207.125.701

3520625-001-JP Dec 2017

https://www.juniper.net/assets/jp/jp/local/pdf/case-studies/3520625-en.pdf

日本大学ネットワーク（日大WAN）

- 横浜DC
  - MX240 x 2
  - SRX1500
- 大学(学部)
  - MX5 x 17
  - EX2300 x 17
- 高校等
  - SRX345 x 10



Googleフォームで運用自動化

- みなさんご存知Googleフォーム！
- Google Apps Scirpt（GAS）と連携
  - Google Apps ScriptはGoogle APIを内包したJavaScript
  - GASはRESTが使える→正確にはHTTPアクセスができる
  - JSONの処理も得意→正確にはJavaScriptの機能
- JUNOSはREST API対応
- 停電や脆弱性対応に応用
  - キャンパスが多いので管理しきれない
  - 法定停電時のshutdown予約
    JUNOS更新後のreboot予約
    - 管理権限なくても運用可能に！

REST APIのフロー

REST API
HTTPS

submit

Google
フォーム

Google
Apps
Script

カレンダー
投入

Calendar

キャリアへ
監視停止

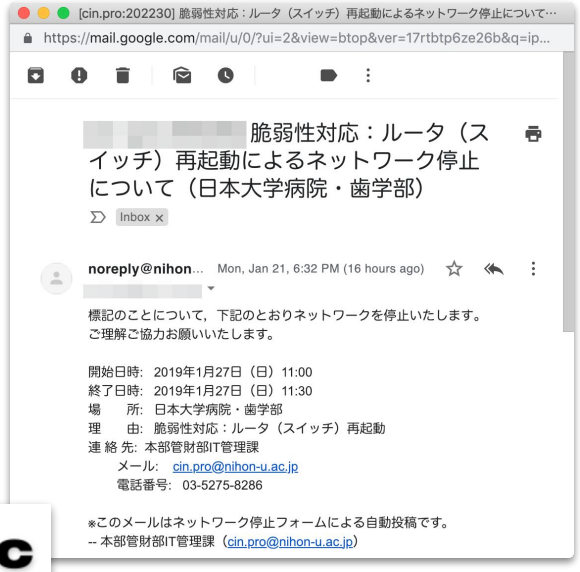
Gmail

管理者MLへ
告知

Groups

実行例

- 管理者MLへ周知
- キャリアへはサービスコード・回線 IDを添えて監視停止を通知
- 投稿者ならびに関係者カレンダーにスケジュール投入
- ルータ（スイッチ）にコマンド投入
- 投稿者チェックあり

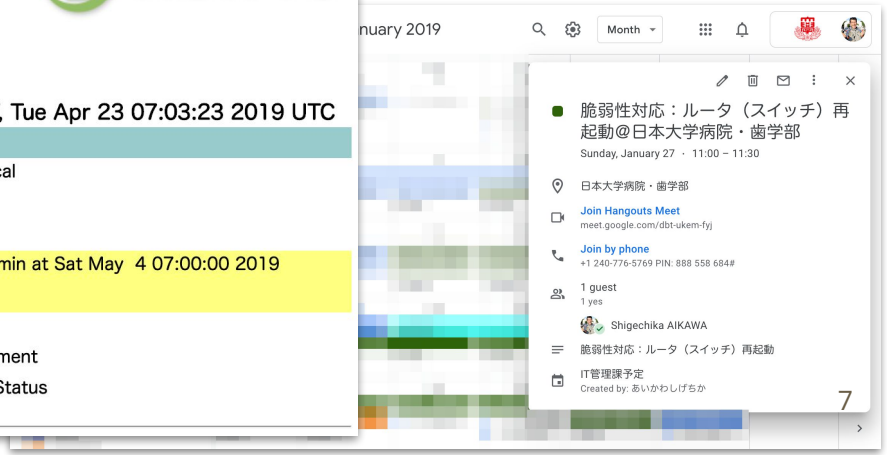


Diff of /wan/configs/chs-rt.nihon-u.ac.jp

viewvc

Parent Directory | Revision Log | Patch

#	revision 14255 by *rancid*, Thu Feb 21 04:03:26 2019 UTC Line 1	revision 15911 by *rancid*, Tue Apr 23 07:03:23 2019 UTC Line 1
1	#RANCID-CONTENT-TYPE: jlocal	#RANCID-CONTENT-TYPE: jlocal
2	#	#
3	# chs-rt> show system reboot	# chs-rt> show system reboot
4	# No shutdown/reboot scheduled.	# shutdown requested by nuadmin at Sat May 4 07:00:00 2019
5		# [process id 97828]
6	#	#
7	# chs-rt> show chassis environment	# chs-rt> show chassis environment
8	# Class Item Status	# Class Item Status



REST使ってわかったこと

- 認証はBASIC認証
  - HTTPじゃ不安すぎる→HTTPSにするよね
  - ブルートフォースには無力
- HTTPSの実装ががが
  - CTサーバー証明書がオレオレ証明になる仕様
    - 中間証明書が抜けるバグ →直すらしい
- RESTを使うにはインターネットからのHTTPSアクセスフルオープン
  - Google Apps Scriptを受けるためにSRC IPを縛れない
  - クライアント証明があればだいぶ安心！？
- Juniper EXシリーズ（L2SW）はREST未実装※

思ったより楽できない…

NETCONF（PyEZ）への改宗

- JUNOSはNETCONFも動く
  - 言語はPython
- NETCONFはEXシリーズも対応
- JuniperはPyEZ（junos-eznc）というライブラリを出してる
  - https://github.com/Juniper/py-junos-eznc
- PythonはGoogle APIも充実してる（oauth2client, gspread）
- REST処理部分をNETCONF（PyEZ）へ書き換え
  - 定期的に動かしフォームの更新をチェック
  - Pythonからフォームと共に更新されるスプレッドシートにアクセス
    - 更新があればPyEZでコマンド投入

NETCONFの場合

NETCONF
(SSH)

定期的に
更新チェック

EZ

CentOS

Google
フォーム

submit

Google
Apps
Script

カレンダー投入

Calendar

キャリアへ監視停止

Gmail

管理者MLへ告知

Groups

NETCONF使ってわかったこと

- ssh鍵認証できない→パッチはありそう
- SW.reboot()には引数at=YYMMDDHHMM（日時指定）できるが，SW.poweroff()はin_min=（何分後）しかなく不便
  - at=対応パッチ作りPR
  - コミッターとのやりとりの末，3月19日にマスターにマージされた。
    しかし4月21日リリースのv2.2.1に含まれず😭
- RESTより楽できるようになったけどサーバ必須なのがが
  - サーバレスにしたい←イマココ
    - サーバレスでPython動かしたい。
    - NETCONFアクセスはSRC IP固定で受けたいたい。

JUNOS REST API vs NETCONF

	REST API	NETCONF
Serverless	YES	NO※
Transport	HTTP/HTTPS※	NETCONF（SSH）
MX Series	YES	YES
SRX Series	YES	YES
EX Series	NO※	YES

QFXシリーズは未検証

※個人の感想です

まとめ

- REST API動いた
  - HTTPSオレオレ証明直して欲しい
    > JUNOS
  - クライアント認証対応して欲しい
    > JUNOS・GAS
  - EXシリーズ18.1系にREST APIが載ったらしいので検証せねば > 俺
- NETCONF動いた
  - SSH鍵認証したい
  - サーバーレスにしたい
    - Function as a Service
    - SRC IP固定したい

みなさんの知見を共有していただけると幸いです