福岡大学における
公開用NTPサービスの現状と課題

藤村 丞（ふじむら しょう） / 福岡大学 情報基盤センター
谷崎 文義（たにざき ふみのり） / NTT西日本
ntp-admin@fukuoka-u.ac.jp

福岡大學
FUKUOKA UNIVERSITY

目次

福岡大学とは

- 私立大学（創立84年）
  - 所在地：福岡県福岡市
  - 地下鉄七隈線で都心から16分
  - 学部数：9学部（31学科）
  - 研究科数：10研究科（33専攻）
  - 学生数：約20,000名（大学+大学院）
  - 大学病院 2病院 + 1病院（2018年4月より）
  - 附属高等学校 2校、附属中学校 1校
- ネットワーク構成
  - IPv4：133.100.0.0/16　IPv6：2405:be00::/32
  - AS18148（SINET、OCNと接続）

みなさんに質問(1)

- みなさん、様々なサービスやシステムを運用されていると思いますが…
  - 以下のことを最初に想定して開始していますか？
- そのサービス、ちゃんと終了できますか？
- サービスのライフサイクルは？
- そのサービスに対して、ユーザーは提供側が想定した使い方をしていますか？
- サービスのトラフィックや需要の予測は？
- サービスのやめ方は？

みなさんに質問(2)

- 福岡大学が日本初の公開用NTPサービスを提供したという事を知っていた方？
- 設定して使ったことあります？

福岡大学におけるNTPサービス

- 1993年10月に運用開始
- 日本初の公開NTPサービス
  - 133.100.9.2
  - 133.100.11.8
  - 今年で24年目
- 当時の管理者より2005年1月20日トラフィック分散のお願い
  - 毎秒900件ほど

http://pc5.2ch.net/test/read.cgi/linux/1008318869/500-

時刻合わせ総合スレッド

ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

■ このスレッドは過去ログ倉庫に格納されています

時刻合わせ総合スレッド

1 : Stratum1 : 01/12/14 17:34 ID:Acj6d52W
時計の正確さの自慢，および，街で見つけたNTPサーバを
貼り付けるスレです．時刻合わせの運用面における悩みも
どーぞ．

■関連リンク

・The Clock Mini-HOWTO (JF)
http://www.linux.or.jp/JF/JFdocs/Clock.txt
・Experimental NTP Servers
http://www.ist.mfeed.ad.jp/
・NTPサーバリスト
http://pc.spo.to/network/ntp_list.html

500 : 福岡大学のNTP屋 : 05/01/20 13:50:01 ID:u9Qqv67y
早いもので1993年10月に時刻サーバーを公開してから10年を越えてしまいました。
開発時のGPS受信機は190万円も出してアメリカ製を購入しました。
SunOS 4.1.3でドライバーを開発していたり、
古野電気にGPSの受信機を開発してもらったりしたのが夢のようです。
今はFreeBSDでのんびりとサービスを続けています。

ところで、皆さんへお願いですが、出来るだけ負荷を分散したいのです。
今や、clock.nc.fukuoka-u.ac.jpへのアクセスは毎秒900件ほどになります。
引き合いに出して申し訳ないのだけれども、東大のntp.nc.u-tokyo.ac.jpでも
毎秒3，4件程度のトラフィックです。

サーバーとの時刻差を求めるのに
(往路の伝送時間－復路の伝送時間)/2を観測誤差として補正している原理からして、
遠方になるほど観測誤差が大きくなる傾向にあります。

候補となるNTPサーバのそれぞれについてtracerouteなどで遅延時間を求めます。
遅延時間が安定していて、時間が短いのが望ましいサーバです。
ついでに、tracerouteの途中にあるルータを ntpq -p などでチェックしてみます。
Ciscoのルータなどはntpをサポートしているので、案外多くのサーバを発見できます。
念のため ntpqや,ntpdate -q などでまともなサーバかどうかも確認しておきます。

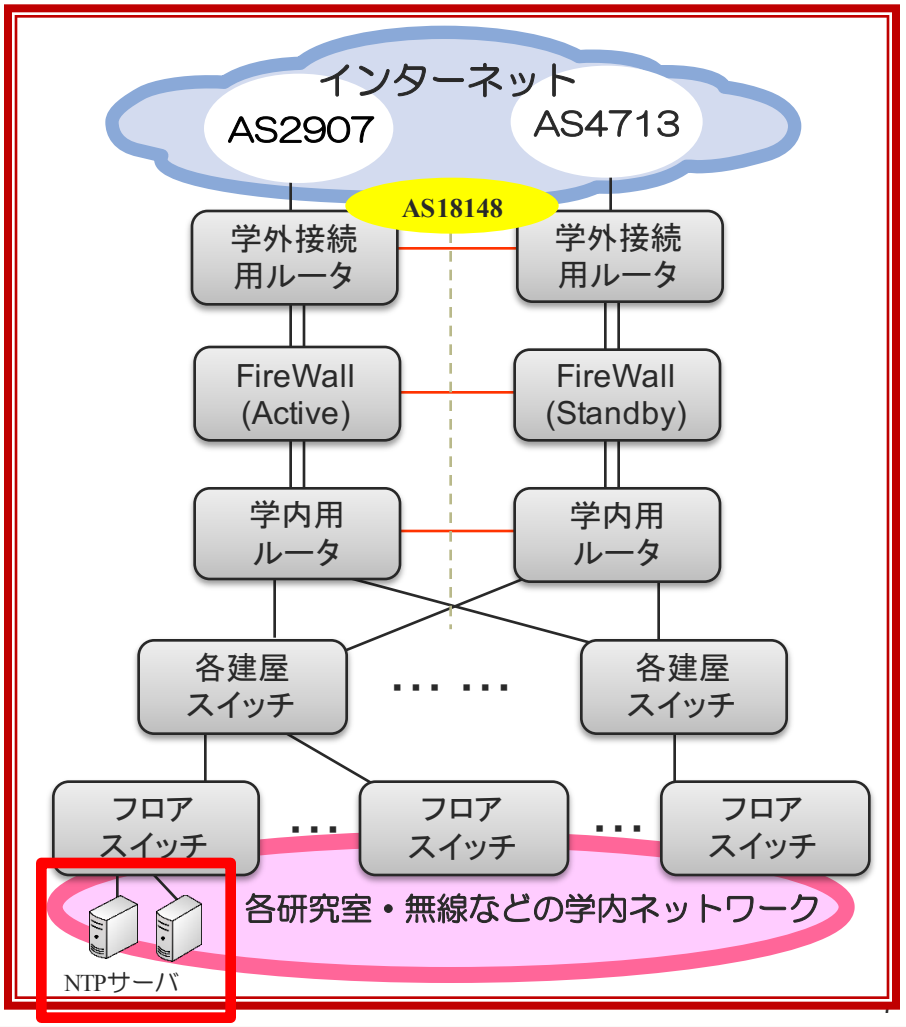
YahooBBなどのISPのユーザは出来るだけISP内で提供しているNTPサーバを参照するようにお願いします。

何だか泣き言をいっているようで恥ずかしいのですが、ご協力をお願いします。

鶴岡知昭@福岡大学、電子情報工学科

学内ネットワーク構成図

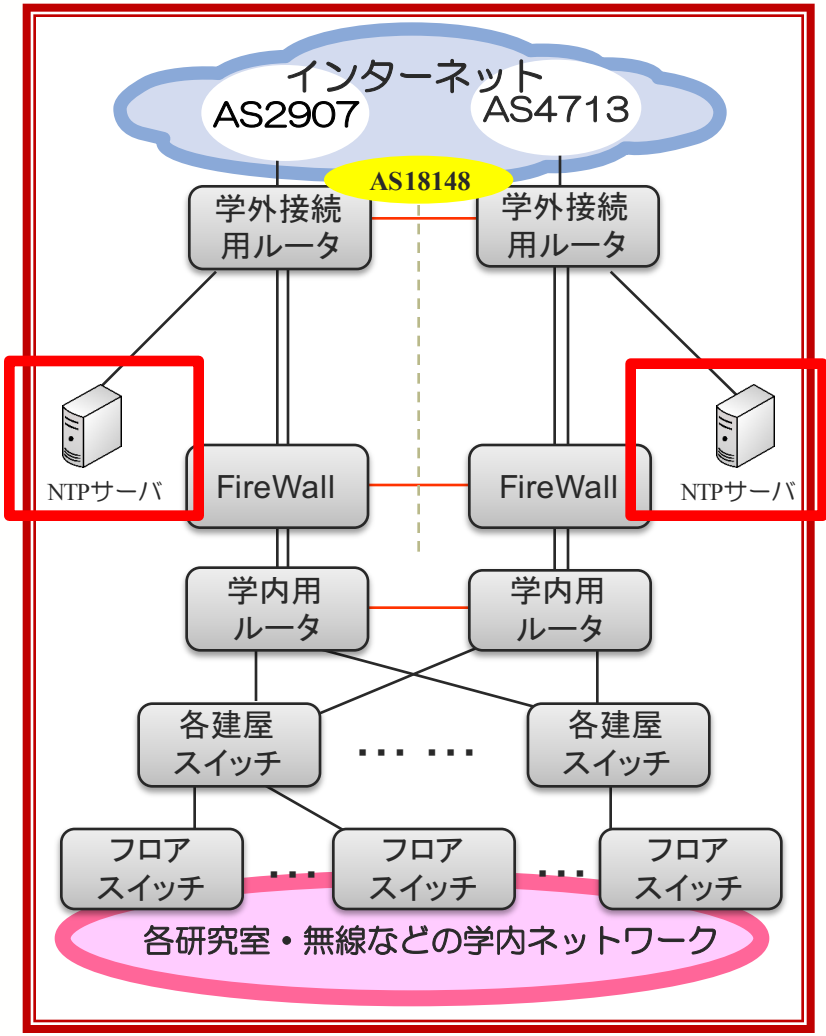
- 2015年8月まで
- NTPサーバは**研究室**での運用
  - ネットワーク的には末端のフロアスイッチ配下
  - 毎時0分に瞬間的なトラフィック増大
- NTPサーバが停止すると、学内のネットワーク機器等が停止することが…（後述）



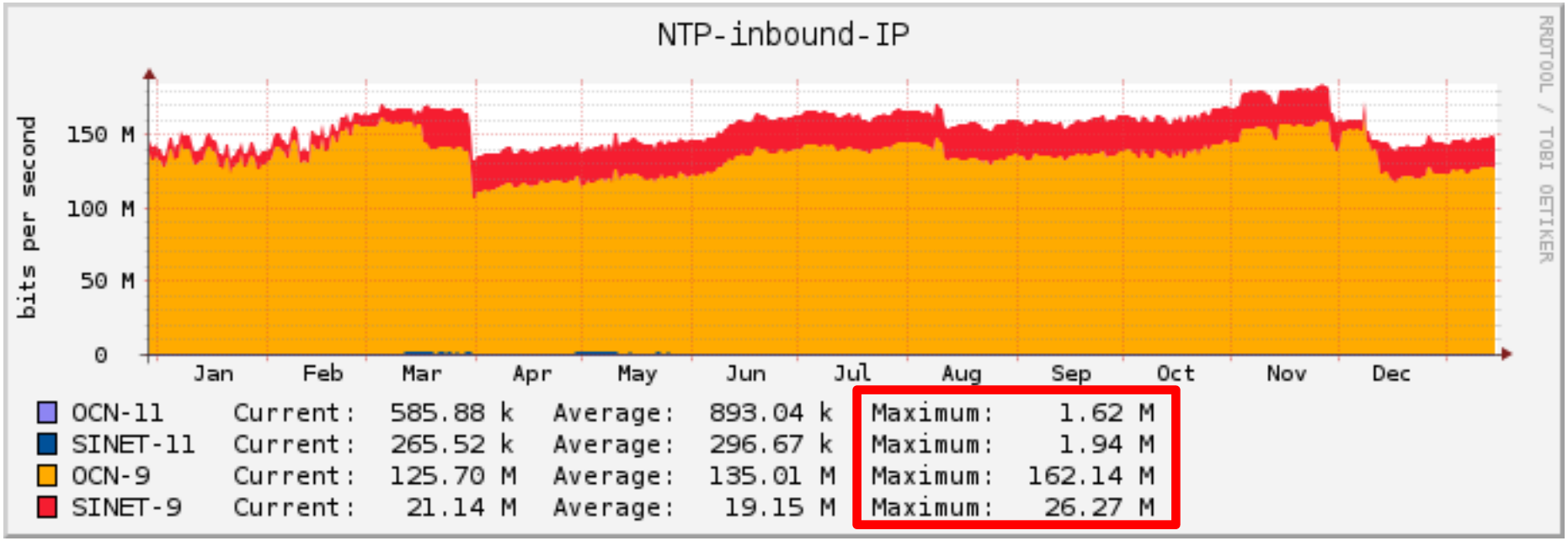
※ AS18148 … Fukuoka University
※ AS2907… Science Information NETwork（SINET）by National Institute of Informatics
※ AS4713 … Open Computer Network（OCN）by NTT Communications Corporation

学内ネットワーク構成図

- 2015年9月以降
- NTPサーバは
  情報基盤センターで運用
  - 過去の障害事例（後述）から、Firewallへの負荷を考慮してFirewallの上段へ移動
- 4台のNTPサーバ
- 2台のロードバランサで負荷分散



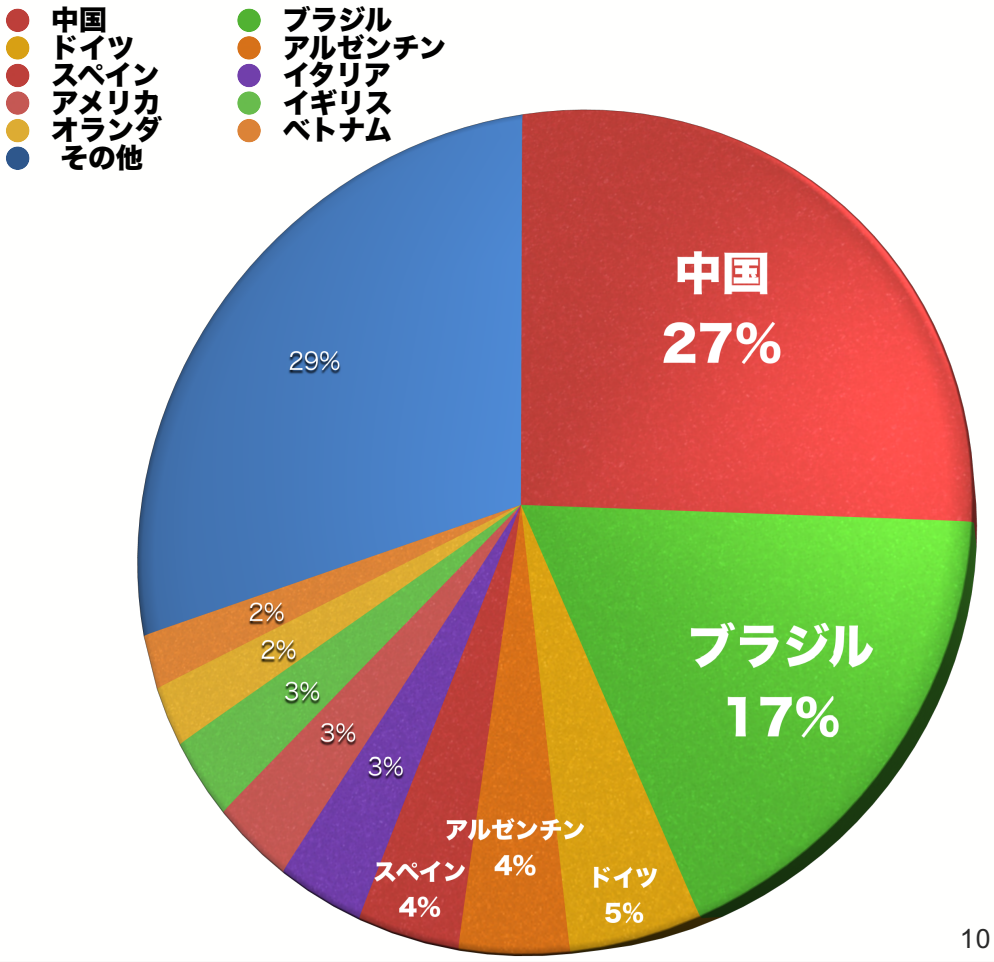
NTPサーバへのトラフィック



- 最大で約190Mbps、21万query/s強
- 133.100.9.2 宛が多い

アクセス元について（国別）

- 調査期間
  - 2018/1/14 - 20
- アクセスしてきた全パケットをIPアドレス別に分類、GeoIPでアクセス元の国をカウント
  - ntopngとElasticSearchで分析
- 239の国と地域からアクセスがある



なぜこうなったのか？(1)

- 様々な機器のファームウェアにNTPサーバのIPv4アドレスが埋め込まれている
  - 利用者側での設定変更ができないものがある
  - 最近話題になったのはTP-LINKの無線LAN中継装置
    - 詳しくは資料最後の参考リンクを参照
    - 時刻同期やインターネットへの疎通確認に利用されている
    - 修正されたファームウェアが一部リリースされているが
ユーザーによるファームウェア更新作業が必要
- ファームウェアへの埋め込みは、TP-LINKだけではなく、複数のメーカーの機器でも同様の事例がある
  - 実機を入手し調査・確認済み

なぜこうなったのか？(2)

NTP利用の理由とアップデートの推奨 (スコア:3, 参考になる)

by zhang (48287) on 2017年12月26日 0時16分 (#3335688)

中国深圳に入れる企業である普聯技術は、製品を120を超える国の数千万人のユーザーに売っている。
製品は100%安全で、あなたのプライバシーはセキュリティで保護されています。
しかし、中国の製品は、屡々スパイウェアとバックドアが含まれるという事実無根の冤罪にさらされます。
世界で信頼された日本私立の大学のNTPサーバー (clock.nc.fukuoka-u.ac.jp) と通信しているのは、120を超える国の皆様を安心にする目的です。

> 8.8.8.8にでもなげとけばいい
Googleサービスは中国国内からの金盾工程(全国公安工作信息化工程，Great Firewall)を通れることが保証されていない。
中国国内では政府の管理底でDNS cash poisoningがなされるのでGoogleサービスはDROPされる恐れがあります。

> 自前でサーバ立ててそこへの疎通確認するのが普通
もしそうしたならば、日本人のいくつかの部分は、パケットの内容を捕らえることもなく、「情報を中国のサーバーに送るスパイウェアである」という冤罪をするであろう。中国企業のIPアドレスに通信をするだけでスパイウェアの疑惑がかかる。
日本政府 nict.go.jp のNTPならば日本人は安心だが、中国人は情報を日本政府に送っていると誤解される。
従って、スパイの疑いがかけられる自前や政府のサーバーではなく、世界で信頼された日本私立の大学のNTPサーバー (clock.nc.fukuoka-u.ac.jp) と通信している。

- スラッシュドットの記事より抜粋
  - https://srad.jp/comment/3335688
- 発言者が誰なのか？等、詳細は不明

よくある質問と答え(1)

- Q:今後どうするのですか？
- A:サービスを停止します
  - NTPサービスのトラフィックが多すぎるため、大学ネットワーク運用に無駄なコストがかかっている
  - このままにしておくと、トラフィックが増え続ける恐れがある
  - 1993年当時はNTPで時刻同期することそのものが研究対象であったが、現在では専用アプライアンスが製品販売されていて、研究としては役目を終えている
- 利用されている方は早めの設定変更をお願いします

よくある質問と答え(2)

- Q:NTPサーバを停止する、もしくは大学側のルータでフィルタすれば？
- A:NTPサーバが返答をしないとリクエストパケットが極端に増大することが、過去の事例からわかっています

- 参考:2014年2月上旬の事例
  - 計画停電でNTPサーバを停止させたところ、学外からのNTPリクエストパケット(リトライ)が極端に増大し、Firewallが最大セッション数100万を簡単に超え停止、大学のネットワーク全体が停止した
  - SINETからのIN(最大値): 約900Mb/s
    - 通常時、約150Mbps(入学試験月のため閑散期のトラフィック)
  - OCNからのIN(最大値): 約135Mb/s
    - 通常時、約80Mbps(入学試験月のため閑散期のトラフィック)

よくある質問と答え(3)

- Q:上流のISPでフィルタしてもらえば？
- A:技術的には可能ですが、ISPで長期に渡りそのフィルタを維持し続けてもらうことが難しいと思っています
  - 様々な製品のファームウェアにアドレスが埋め込まれていることから、リクエストパケットは長期に渡り送られ続けると予想しています
  - 例えば数年後にそのフィルタが意図せず削除された場合、福岡大学に向けて多量のリクエストパケットが流入してくる恐れがあります

よくある質問と答え(4)

- Q:今後のスケジュールは？
- A:サービス停止にむけた技術的検証を2018年4月以降に行う予定です
- 停止する際は事前にアナウンスします

よくある質問と答え(5)

- Q:どのように停止するのですか？
- A: BGP等の経路制御でリクエストパケットを自ネットワーク内の特定の場所に集めて、ネットワーク機器のブラックホールに落とすことを検討しています
  - また、そのトラフィックを継続的に計測・分析する予定です

よくある質問と答え(6)

- Q:お手伝いできることがありますか？
- A:福岡大学のNTPサーバを使わないでください
  - この問題を多くの人に知らせてください
  - もしご存知だったら…
    - www.ntp.orgのサーバリストから、福岡大学のNTPサーバを消す方法
      - 指定されたコンタクト先(webmaster@ntp.org)に連絡しても返答がない…
    - ブロードバンドルータなどのファームウェアを作っているメーカー(特に中国や台湾)をご存知でしたら紹介してください

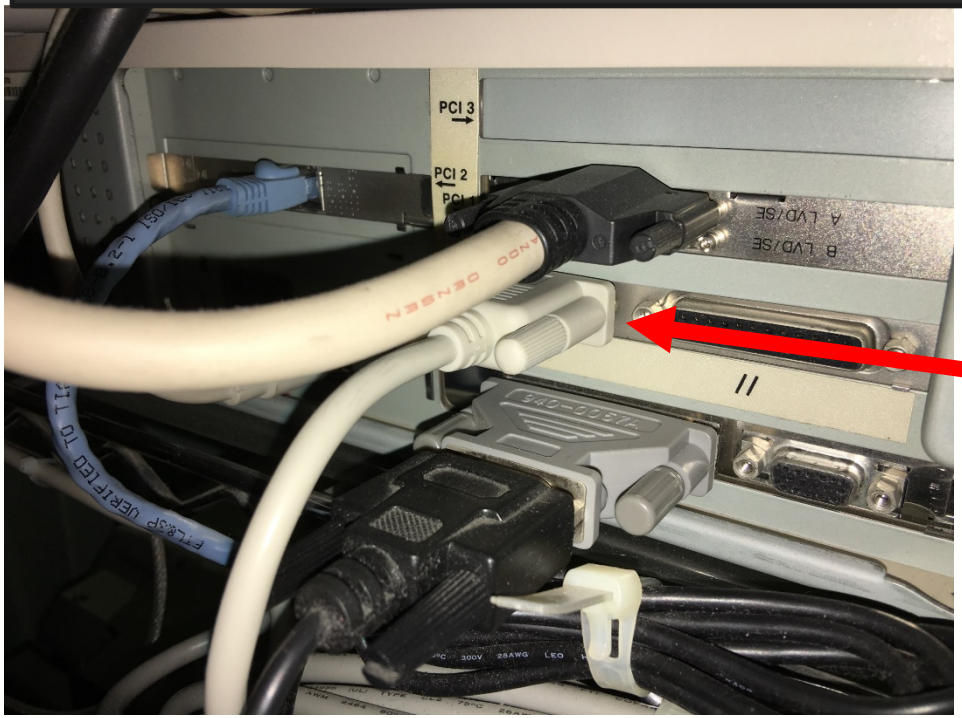
今回の事例から見えてくる事柄

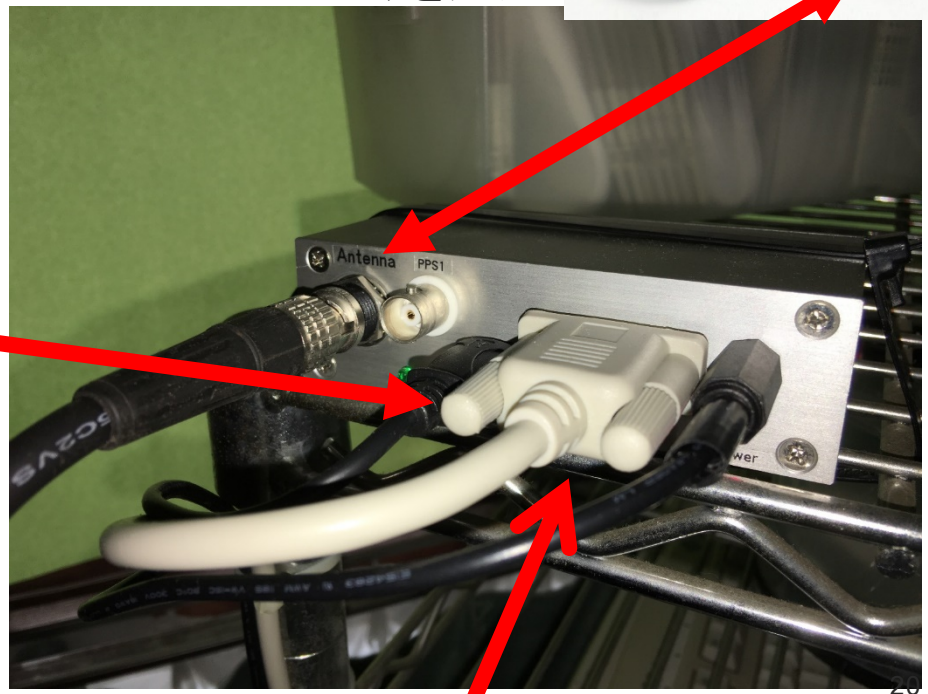
- サービス開始時に、そのサービスの終わらせ方をザックリでも考えておくべきである
  - インフラ化すると止められない場合も？！
- 提供側が想定していないサービスの利用のされ方をする場合がある
  - まさか疎通確認に使われるとはw
- コンシューマ向け機器のファームウェアアップデートをどうするか？という問題はとても根深い
  - 自動アップデート or 手動？告知方法は？
- システムにとって重要な要素である『時刻』を他組織が運用する『公開NTPサーバ』だけに任せてもいいのか？
  - 『正確な時刻と周波数は、情報通信の基盤であるとともに、学術、産業、安心安全な社会生活の基盤です。』
    - 国立研究開発法人 情報通信研究機構 電磁波研究所 時空標準研究室
    - http://www2.nict.go.jp/sts/lab/

Stratum 1作ってみませんか？(1)

誰もが持っているSun ULTRA5で簡単にできる！

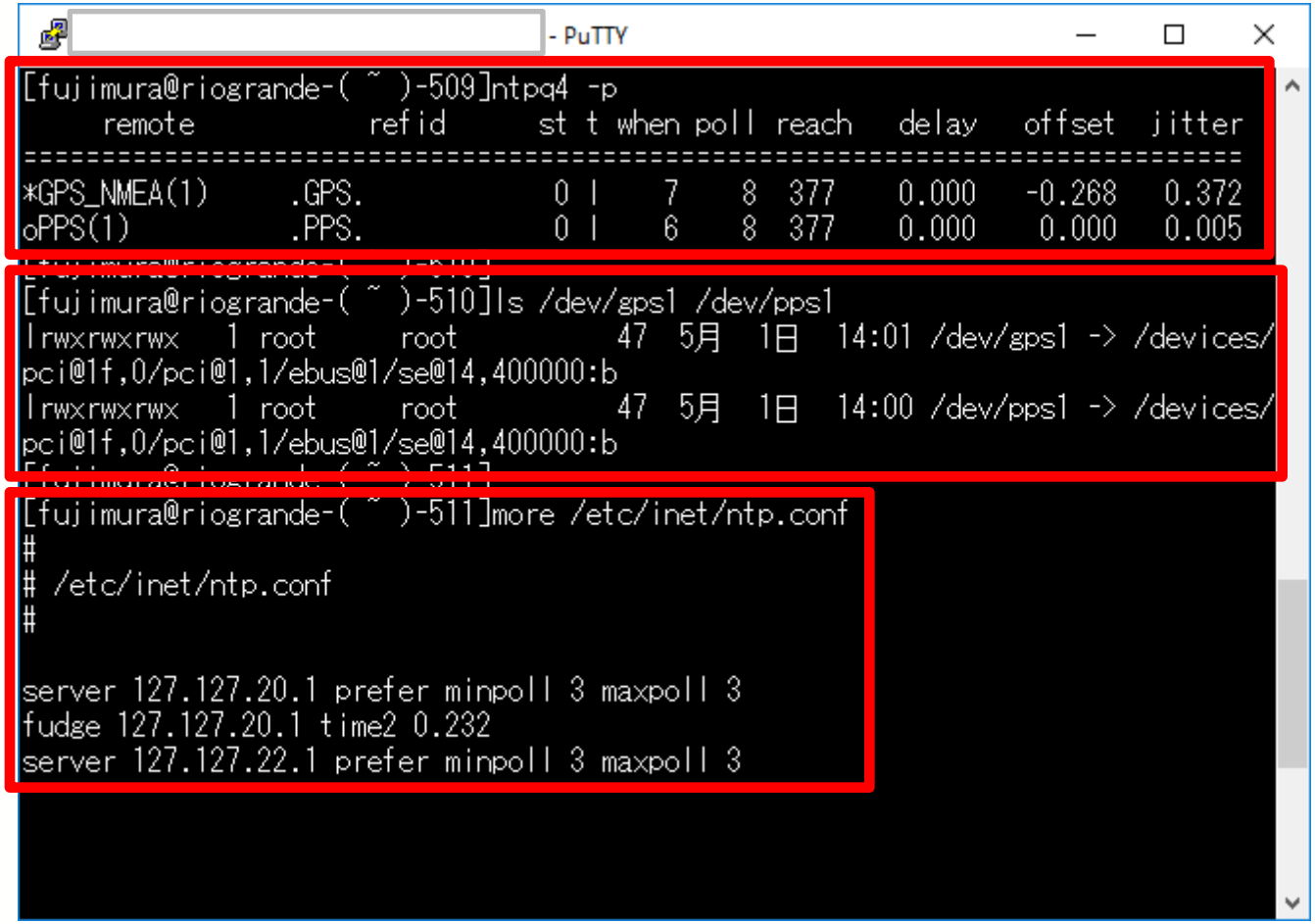
シリアルから、時刻の文字列とPPS(Plus Per Second)を入力





GPSレシーバー 兼 Plus per Second(PPS)出力機（時刻同期専用）

Stratum 1作ってみませんか？(2)



最後に

福岡大学の
NTPサーバは
停止します！

参考リンク

- Column 情報の糧 楽しかりし年月
  - 1993年当時の福岡大学の様子が書かれたコラム
  - https://www.ipc.fukuoka-u.ac.jp/column/y2008/m10/
- Fukuoka University Public NTP Service Deployment Use case（APRICOT 2017）
  - https://www.slideshare.net/apnic/fukuoka-university-public-ntp-service-deployment-use-case
  - https://www.slideshare.net/fujimura_sho/ntpapricot-2017（日本語訳）
- 公開NTPサーバの運用と課題（ENOG47）
  - http://enog.jp/wp-content/uploads/2017/10/20171027_ENOG47_tanizaki.pdf
- 福岡大学の公開NTPサーバに関するまとめ
  - https://togetter.com/li/1182233
- TP-Link repeater firmware squanders 715 MB/month
  - https://www.ctrl.blog/entry/tplink-aggressive-ntp
- ＜更新＞TP-Link製無線LAN中継器によるNTPサーバへのアクセスに関して
  - http://www.tp-link.com/jp/news-details-17792.html
- TP-Linkの無線LANルータなどで高頻度でNTPサーバにリクエストを投げる設定が発覚し問題に
  - https://it.srad.jp/story/17/12/25/0813230/

人をつくり、時代を拓く。

福岡大學