福岡大学における公開 NTP サービスの現状と課題

藤村 丞 [1)], 谷崎 文義 [2)]

1) 福岡大学 情報基盤センター

2) 西日本電信電話株式会社

ntp-admin@fukuoka-u.ac.jp

Current status and issues of public NTP service at Fukuoka University

Sho FUJIMURA[1)], Fuminori TANIZAKI[2)]

1) Information Technology Center, Fukuoka University

2) Nippon Telegraph and Telephone West Corporation

概要

福岡大学では、GPS を用いた日本初の公開用 NTP サーバを 1993 年（平成 5 年）10 月から運用しており、今年で 25 年が経過した。この間に、NTP トラフィック（リクエストパケット）が増加していると同時に、直接的、間接的に様々な問題が生じてきている。本稿では、この公開用 NTP サービスに係わる諸問題について、考察していく。

1 はじめに

福岡大学は福岡県福岡市城南区に所在地を置き、学部は 9 学部 31 学科、大学院は 10 研究科 33 専攻、学生数は学部生と大学院生を合わせて約 20,000 人、大学病院 3 病院、附属高等学校 2 校、附属中学校 1 校を有する私立の総合大学である。

この福岡大学では 1993 年（平成 5 年）10 月より、全世界に向けて日本初の GPS を用いた NTP サービスの提供を開始し、25 年が経過した現在もこのサービスの提供を行っている。だが、この 25 年の間でトラフィック量が増加の一途をたどっており、2013 年（平成 25 年）頃からこの公開用 NTP サービスのトラフィックに起因したネットワーク障害が発生し、インターネット接続が行えなくなった。

本稿では、この公開用 NTP サービスに起因した障害事例、現状分析、課題、今後のサービス提供などについて述べていく。

2 サービスの概要

1992 年頃の福岡大学では、大型計算機を学内の各所と同軸ケーブルで結んだ中央集中型（スター型）の構成であった。この頃の計算機は、起動後に正確な時刻を手動で設定する必要があった。ある時この時刻を間違えて設定してしまったことがあり、この時刻設定を自動化する仕組みを整えれば設定ミスを防ぐことができると考え、自動的に時刻同期をする仕組みを整えることにした。当時、郵政省の標準電波を利用した短波受信機では実用に耐えうる精度が出なかったため、GPS 受信機から時刻情報を取り出し、それをコンピュータにて自動化する仕組みを整えた。また、この頃日本国内ではまだ一般向けの NTP サービスが提供されていなかったので、1993 年（平成 5 年）10 月から一般公開し公開用 NTP サービスを運用している。現在運用中の公開用 NTP サーバは、以下の 2 台である。

- 133.100.9.2（clock.nc.fukuoka-u.ac.jp）
- 133.100.11.8（clock.tl.fukuoka-u.ac.jp）

NTP サーバの FQDN と IP アドレスは、サービス運用開始時から現在も変更していない。また、この 2 台の公開用 NTP サーバは、2004 年（平成 16 年）9 月より ntp.org[*1]の Public Time Server Lists [*2]に登録している。

3 ネットワーク構成（2015 年 8 月まで）

福岡大学では、2010 年（平成 22 年）8 月より運用してきた教育研究システム（医療系・事務系・図書館以

[*1] http://www.ntp.org/

[*2] http://support.ntp.org/bin/view/Servers/StratumOneTimeServers

外のシステム、キャンパスネットワーク・ネットワークセキュリティ・PC 教室など）FUTURE（Fukuoka University Telecommunication Utilities for Research and Education）を、2015 年（平成 27 年）8 月に第 5 世代目の FUTURE5（FUTURE 5th Generation）として導入した。この導入と同時に、公開用 NTP システム一式を、FUTURE4 の機器を一部流用して導入した。その導入前（2015 年 8 月まで）の構成を、図 1 に示す。

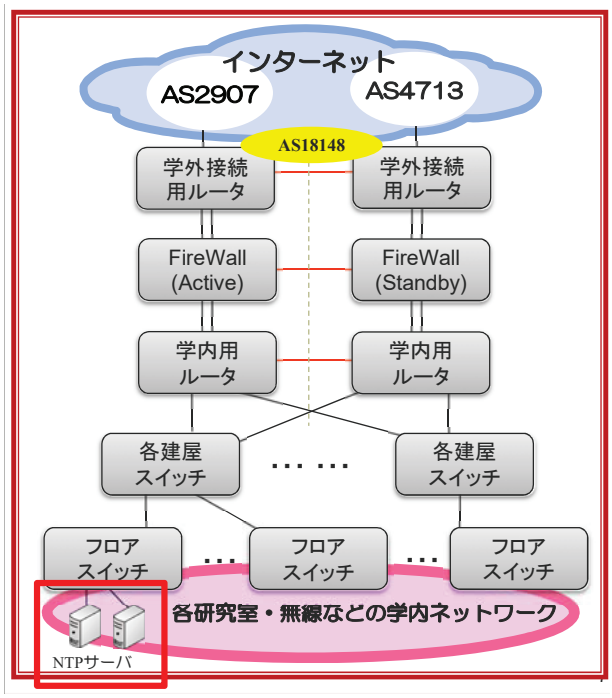

図 1　ネットワーク構成（2015 年 8 月まで）

この構成図からもわかるように本学は AS18148 を取得しており、インターネットへは SINET（AS2907）と OCN（AS4713）とのマルチホームにて運用している。また、学外接続用ルータでは IPv4 と IPv6 の BGP フルルートを受信している。

公開用 NTP サーバは 2015 年（平成 27 年）8 月までキャンパスネットワークの末端に位置し、運用は、学部の一研究室にて行っていた。キャンパスネットワークの末端に位置していたことから毎時 0 分になると極端にアクセスが集中し、同研究室のネットワークへの負荷が大きくなっていた。このため、2005 年（平成 17 年）1 月 20 日に、負荷分散のお願いを当時の管理者より”2 ちゃんねる”の”時刻合わせ総合スレッド”を通じて行った経緯がある。この時のアクセス数は秒間約 900 件、帯域にして約 2Mbps であった。

4　障害事例と復旧手法

2015 年（平成 27 年）8 月までは、第 3 章の構成で運用してきたが、公開用 NTP サーバに対するトラフィックが引き金となった障害が数回発生し、キャンパスネットワークがインターネットに接続できない状態となった。本章ではいくつかの障害事例のうち 1 つを取り上げて、その復旧手法について述べていく。

2014 年（平成 26 年）2 月 14 日（金）に、キャンパスネットワークのインターネット接続が停止した。原因は SINET（AS2907）側から流入した大量の NTP のトラフィックにより、FireWall の有効セッション数（10,000 セッション）を超えてしまったためにセッションを張ることができなくなったからである。この時、以前の障害により OCN（AS4713）用接続ルータには 8Mbps の帯域制限を設定していたが、SINET 接続用ルータにはこれを設定していなかった。このため、SINET 接続用ルータにも OCN 接続用ルータと同様に帯域制限として 8Mbps の設定を行った。これにより、多少遅延は見られたものの、インターネット接続は行えていたのでしばらく様子を見ることにした。

だが翌日の 15 日に、OCN 接続用ルータが停止した。このルータを再起動してみたが、起動はするものの再び停止してしまった。そこで、帯域制限値 8Mbps を 8kbps に変更するなどいろいろと試してみたが、結局この日は OCN 接続用ルータを復旧させることができなかった。この OCN 接続用ルータがダウンした原因は、帯域制限設定である。この設定を入れると大量の NTP のトラフィックを CPU で処理するため、CPU 使用率が 100% となりルータが機能しなくなるのである。よって、この日は OCN 接続用ルータの電源を切った状態で暫定対応することにした。この時、SINET 接続用ルータには 8Mbps の帯域制限が入っていたが、遅延はあるものの動作はしておりインターネット接続は行えていた。SINET 接続用ルータが動作していたのは、OCN 接続用ルータに比べて上位機種であったため、帯域制限処理をかろうじて CPU 処理できていたからである。16 日および 17 日も引き続き様々な対処を行ってみたが、OCN 接続用ルータを復旧させることはできなかった。

18 日になって、一つの解決策を見いだすことができた。OCN と SINET 接続用ルータの帯域制限は CPU で処理していたため、大量のトラフィックを処理することはできない。だが OCN 接続用ルータの上位に、帯域制限の処理を CPU ではなくハード処理できる

QoS 用スイッチを図 2 のように導入し、このスイッチに帯域制限の処理をさせて OCN 接続ルータの処理を軽減させることができた。この QoS 用スイッチに

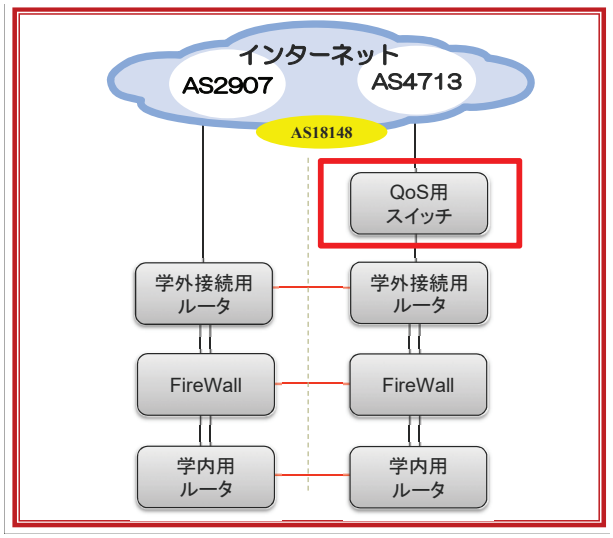

図 2　QoS 用スイッチの導入

帯域制限の設定を行いその帯域を徐々に広げていき、SINET 用接続ルータ、OCN 用接続ルータともに正常復旧することができた。

よって、この QoS 用 L2 スイッチは正常運用のためには必要不可欠と判断し、このまま設置することにした。また最終的には、SINET 用接続ルータと QoS 用スイッチに帯域制限の値として、8Mbps の設定をして運用することにした。8Mbps に設定した理由は、この時 NTP サーバが使用していた帯域が 8Mbps を少し下回っていたためである。

NTP のトラフィックについては、この障害事例のように応答を返すことができない場合、大量のリトライが発生することが判明した。また、後の調査で、SINET 側からの最大流入は、図 3 のように約 900Mbps（通常 150Mbps 程度、閑散期）にも達しており、クライアントの数が大幅に増えてきていることも判明した。

なお、根本の原因であるなぜ SINET 側から大量の NTP リクエストが来たのか、また SINET 接続用ルータに帯域制限を設定した次の日になぜ OCN 側から大量の NTP リクエストが来たのか、これらの原因は不明なままである。だが、いずれにせよ、公開用 NTP サーバがリクエストに返答できない状況が続くと NTP のリトライパケットが増大し、大量のパケットがキャンパスネットワークに押し寄せてくることになる。

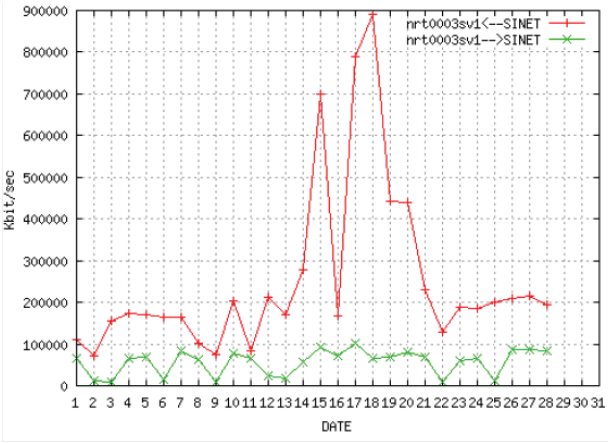

図 3　SINET からのトラフィック

5　ネットワーク構成（現行）

2013 年頃より、公開用 NTP サーバのトラフィック量増加による FireWall 高負荷のため、インターネットに接続できない事象が数回起こっていた。このため、NTP サーバの運用を研究室から情報基盤センターへと変更した。また、教育研究システム FUTURE5（FUTURE 5th generation）を 2015 年 8 月に更新したことに合わせて、公開用 NTP サーバのネットワーク構成を見直した。その構成図が、図 4 である。

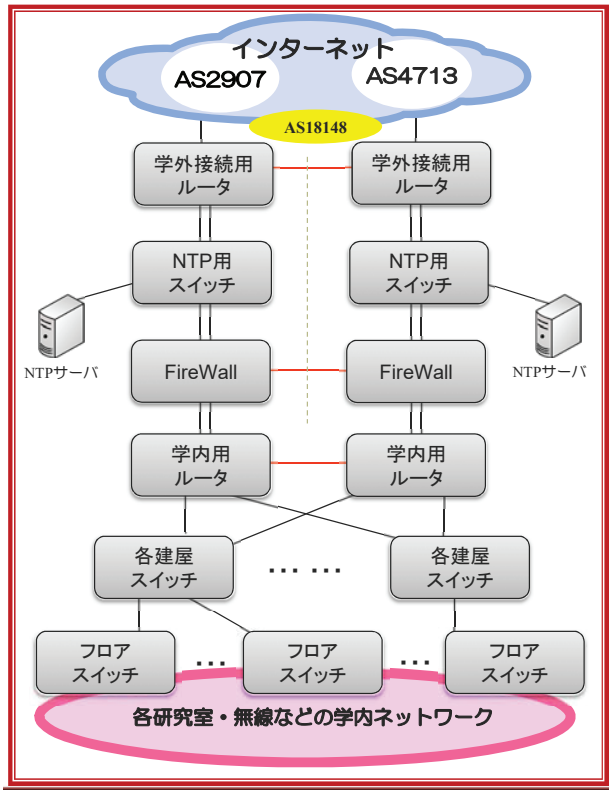

図 4　ネットワーク構成（2015 年 8 月以降）

ネットワーク構成上、エッジスイッチに接続してい

た公開用 NTP サーバを、サービスの安定化を目指して FireWall の上位に移動した。なお、ネットワーク構成を変更したことに加えて、NTP サーバを 2 台から 4 台に増強してリクエスト応答能力を向上させた。前構成での 8Mbps の帯域制限は行なわず、基本的に全リクエストに対して応答を返す事を目指した構成となった。その構成が、図 5 である。

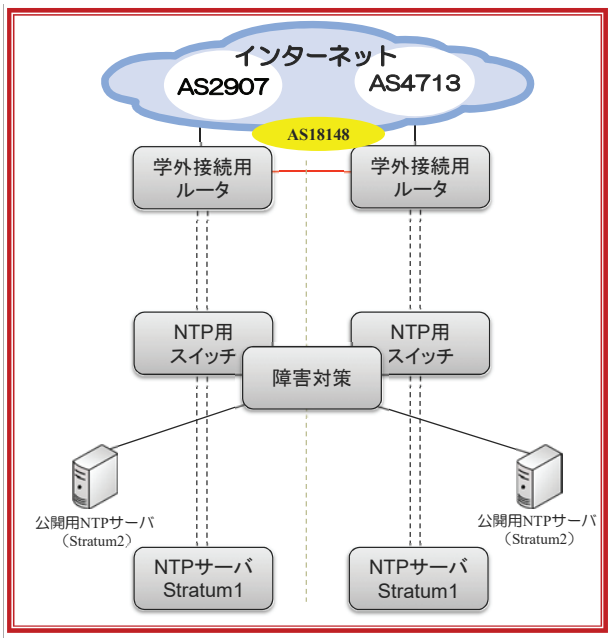

図 5　NTP サーバ構成

公開用 NTP サーバをキャンパスネットワークの上流に設置し、教育研究システム（FUTURE5）とは完全に独立させ、可能な限りキャンパスネットワークへの影響を少なくした。また障害対策を施し安定したサービス提供を行うとともに、NTP サーバ停止時には NTP クライアントから大量の NTP リトライパケットが発生してしまうため、可能な限りサービスが停止しないことを一番の目標として、この構成とした。

この公開用 NTP サーバは Stratum2 として運用しており、Stratum1 は学内に設置している NTP サーバ（Stratum0 として GPS と CDMA、学内専用）から正確な時刻を取得している。

6　トラフィック

第 4 章の障害時に、SINET、OCN 双方から NTP サーバへの帯域制限を 8Mbps としていた。設定後しばらくしてその制限を超えてしまったが、どの程度のトラフィックが発生しているのか、システム構成の制約上 2015 年 8 月までは測定することができなかった。

だが、第 5 章のように構成変更したこと、また、新たなキャンパスネットワークとして教育研究システム FUTURE5 を導入したことにより測定が可能となった。それが、図 6 である。

公開用 NTP サーバで使用している帯域は約 210Mbps、パケット数でみると約 270,000 リクエスト/秒にものぼる。瞬間的には、約 300,000 リクエスト/秒を超えることもある。ちなみに、2016 年 2 月時点では約 120,000 リクエスト/秒であった。よって、現在も少しずつトラフィックが増加している状態である。

7　アクセス統計

トラフィックは右肩上がりで増加の一途をたどっている。また、サービスを停止したとしても、リトライパケットでさらにトラフィックが増加すると推測されるため、まずはトラフィックの傾向を分析することにした。ある一ヶ月間ほど NTP サーバへの全リクエストを分析し、それを国と地域別にグラフ化した。分析には、ntopng と Elasticsearch というソフトウェアを用いて分析した。図 7 が、その結果である。

この図からもわかるように、約 3 割のトラフィックが中国から、1 割半がブラジルから、続いてアルゼンチン、アメリカ、ドイツ、スペイン、イタリア、イギリス、オランダ、ポーランドと続いている。ちなみに、日本は 15 位であった。合計としては、239 の国と地域からのアクセスがあった。よって、公開用 NTP サーバは、世界中にある多くの国と地域からアクセスされていることが判明した。

8　トラフィック増加の原因

第 7 章のアクセス統計を見ると、世界中の多くの国と地域から公開用 NTP サーバへのリクエストパケットが届いている。これらから推測すると、利用者が手入力で公開用 NTP サーバの設定を行っているとは考えづらく、なんらかの機器や初期設定、利用例などに、公開用 NTP サーバが指定されていることが推測される。

図 8 は、海外で流通している比較的安価な、とあるブロードバンドルータに対してパケットダンプを行った結果である。購入して電源を投入しただけで、公開用 NTP サーバにリクエストを出していることがわかる。また、WebGUI から各種設定変更を行うが、NTP サーバについては変更することができない仕様となっている。

このような安価なブロードバンドルータや無線中継

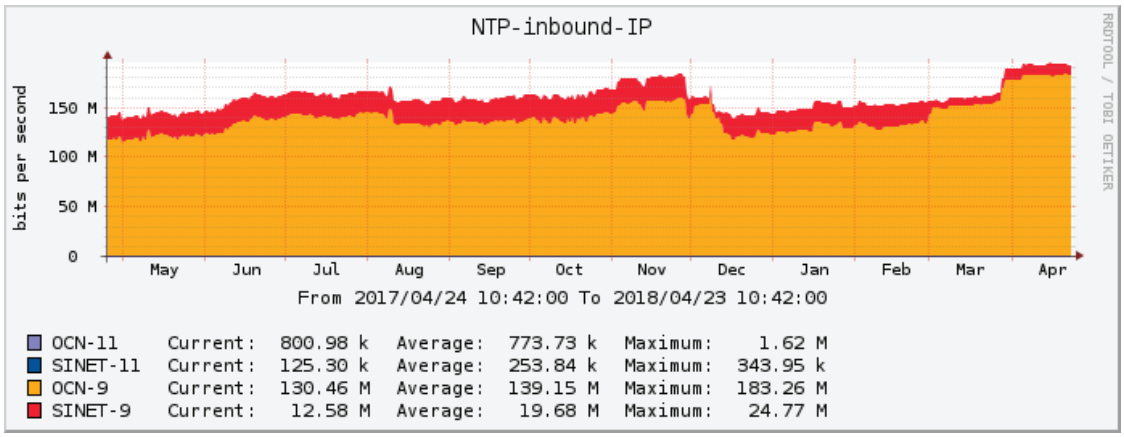

図 6　NTP サーバトラフィック

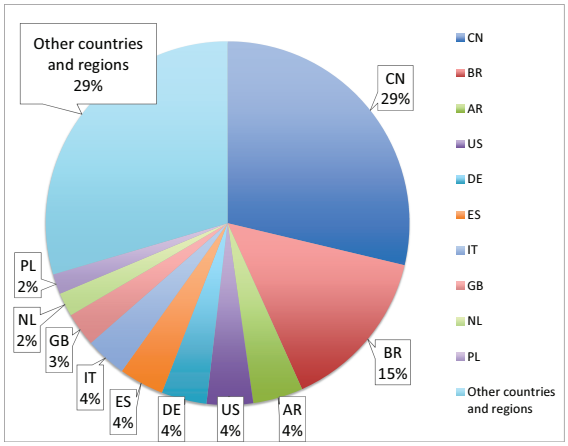

図 7　アクセス分析（国と地域別）

器などが世界中で販売され、その結果、公開用 NTP サーバに対して世界中からリクエストをしていると推測できる。

9　サービスの今後について

これまで述べてきた公開用 NTP サーバの障害事例、トラフィック量やその増加傾向などから考えると、公開用 NTP サーバを維持するためには今後も大規模な投資が必要になる。また、キャンパスネットワークの安定運用にも、同じように大規模な投資が必要になる。よって、この公開用 NTP サービスを停止した方が、最善であると考える。

公開用 NTP サービスを開始した 1993 年頃、NTP サービスを公開している組織は数少なかったが、現在では多くの組織で NTP サービスが公開されており、福岡大学における公開用 NTP サービスとしては、一定の役目は終えていると判断している。また、仮にこのままの状態で公開用 NTP サービスを提供すると、トラフィック量はさらに増え続けるであろう。よって、トラフィック量を減らし、最終的にはサービスを停止する方法を模索していく必要がある。

9.1　サーバ（サービス）停止時の考察

第 4 章にあるように、公開用 NTP サーバを停止すると大量のリトライパケットが発生すると推測している。これを確認するために、一定期間リクエストを破棄してリトライパケットが増加するかどうかの実験を行った。ただし、キャンパスネットワーク全体に影響が及ぶといけないので、リクエストの破棄は一部のアクセス元（比較的アクセスが多い AS の一つ）に絞って行った。また、公開用 NTP サーバは 4 台で運用しているので、一部のリクエストの破棄は、まず 4 台全てで破棄を、その後 2 台解除、最終的には 4 台解除という手順で行った。その結果が、図 9 である。

一部リクエストの破棄を図 9 の「1」の時点で始めた。始めた直後から徐々にリトライパケットが増加し、約 6 時間後にピークに達した。増加帯域は、おおよそ 160Mbps であった。リクエスト数にして、約 210,000 リクエスト/秒増加したことになる。次に、一部リクエストを破棄している 4 台の NTP サーバのうち、2 台の NTP サーバについて破棄の設定を解除した。それが、図 9 の「2」の時である。解除後は NTP クライアントがリクエストを受信したためリトライパケットは減っていき、最終的には 4 台の NTP サーバ全てで破棄の設定を図 9 の「3」の時点で解除したが、「2」の時点とリクエスト数は変わらず、最終的にトラフィックは元の状態に戻った。結果として、ある一定のリクエストを返答すれば、元の状態に戻ることが判明した。だが同時に、この公開用 NTP サービスを停止するとリトライパケットが増大し、インターネット接続の帯域を占有してしまう恐れがあることがわかっ

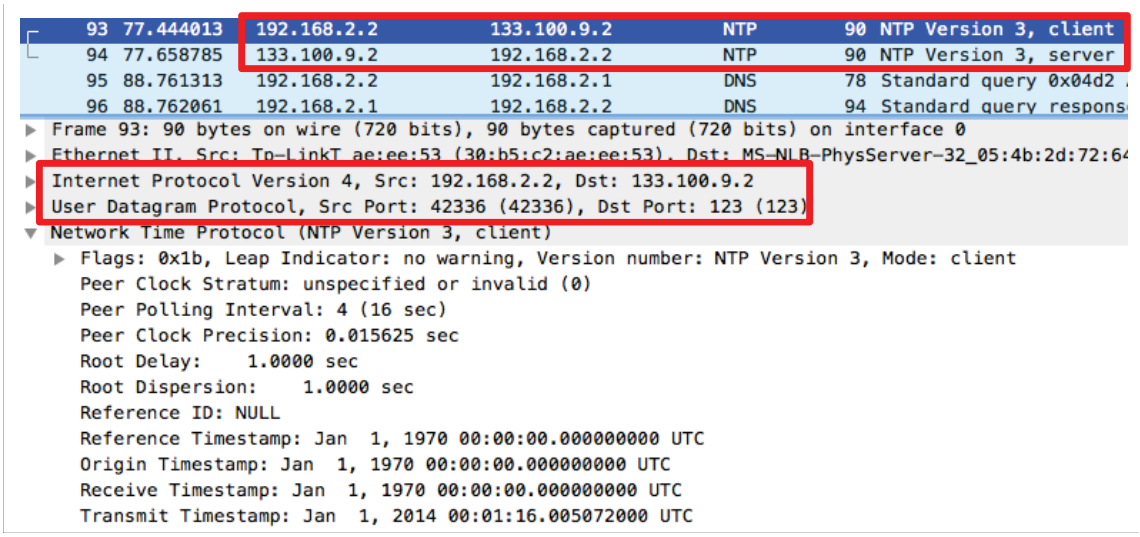

図 8　とあるブロードバンドルータのパケットダンプ

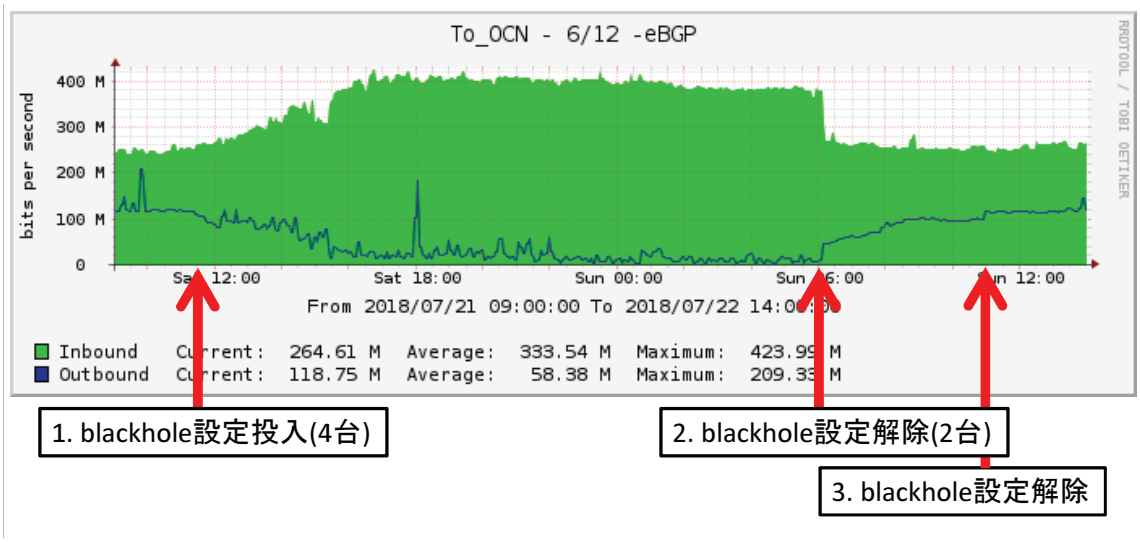

図 9　リトライパケット確認試験

た。また、各ネットワーク機器が処理能力を超える状態になり、インターネット接続ができなくなることも判明した。

よって、単純にサーバ（サービス）を停止するだけでは、解決にならないことが判明した。

9.2　アクセスフィルタ設定時の考察

では、キャンパスネットワークの上位、ISP にて NTP リクエストをフィルタすることはどうだろうか。技術的には可能な選択肢であると考える。ただし、公開用 NTP サーバへのリクエストはブロードバンドルータなどに設定されていることを考えると、長期に渡って続くであろうと推測できる。仮に上位の ISP でフィルタをした場合、そのフィルタを長期に渡って維持・管理してもらわないと行けない。機器移行時や運用者の変更などのタイミングでフィルタが外された場合には大量の NTP リクエストが押し寄せ、キャンパスネットワークのインターネット接続が停止してしまうであろう。

よって、ISP にてフィルタを契約などで維持する仕組みが必要になってくる。これらの商品や仕組みなどは今のところなく、長期に渡ってフィルタを維持してもらうことは難しいのが現状である。

10　サービス停止に向けた考察

このように本学の公開用 NTP サーバについてはアクセス数が今でも増加しており、2018 年 4 月現在で約 270,000 リクエスト/秒までになっている。また、アクセス元については世界中の国と地域からである。

本学にとってこれ以上のアクセス増加（NTP サービスによる帯域の占有）は、教育研究環境の安定提供や

機器・回線の費用、人的負担などの面から見ても好ましくない。また公開用 NTP サーバが停止すると、世界中の NTP クライアントから大量のリトライパケットが送られ、本学のサービスに何らかの支障をきたすことは、実験から明らかである。よって、現時点では公開用 NTP サービスを停止させることはできず、最大限に優先する事項は、NTP リクエストに対して一定量返答し続けることである。

将来的にこの公開用 NTP サービスを問題なく終了させるためには、キャンパスネットワークに影響がないように NTP リクエストを破棄することと、トラフィック量を減らすことである。NTP リクエストの破棄については、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る。トラフィック量を減らすことについては、有効な手段を見いだすことができていない。ブロードバンドメーカへの現状説明や各国の NOG（Network Operators' Group）への状況報告などを行い、世界各国の関係者にご協力をいただくのと同時に、技術的な解決策を模索していく必要があると考える。

11　参考文献

参考文献

[1] 鶴岡 知昭「楽しかりし年月」、Column 情報の糧、福岡大学情報基盤センター Web ページ、2008 年 10 月
https://www.ipc.fukuoka-u.ac.jp/column/y2008/m10/