L-022

福岡大学公開 NTP サービスへのトラフィックの調査・分析
Traffic Investigation and Analysis of Fukuoka University Public NTP Service

財津 玲奈[1)]　神屋 郁子[2)]　奥村 勝[3)]
Rena Zaitsu　Yuko Kamiya　Masaru Okumura
藤村 丞[3)]　谷崎 文義[4)]　下川 俊彦[1)]
Sho Fujimura　Fuminori Tanizaki　Toshihiko Shimokawa

1　はじめに

時刻同期はネットワークにおいて欠かせない要素であり，特に分散システムではデータの整合性確保に重要な役割を果たす．NTP（Network Time Protocol：ネットワーク時刻プロトコル）[1] は，ネットワーク接続されたコンピュータや電子機器の時刻同期に用いられる標準プロトコルである．

福岡大学の公開 NTP サービス [2] は，1993 年 10 月に日本で初めて運用を開始し，30 年以上にわたり国内外の多くのユーザに利用されている．しかし，近年の IoT 機器普及により，2020 年頃から急激なトラフィック増加が発生し，サーバへの通信負荷は一時期約 400Mbps を超え，ネットワーク障害を引き起こしている．

公開 NTP サーバは，その性質上外部からの大量アクセスを受けやすく，異常トラフィックの検出とその特性把握は，安定運用に不可欠である．従来研究では単一観点（パケット数のみ，地域のみ等）からの分析が主流であったが，複合的な特徴の把握には限界があった．

本研究の目的は，福岡大学公開 NTP サービスへの膨大なトラフィックを複数の分析軸（送信元 IP アドレス，AS（Autonomous System：自律システム），TTL（Time To Live：生存時間），ポート番号，NTP 仕様等）から統合的に分析し，トラフィックの特徴を明らかにすることである．

2　調査方法

福岡大学公開 NTP サービスのサーバが受信するトラフィックを tcpdump でキャプチャし，pcap 形式で保存したデータを分析対象とした．調査期間は 2024 年 4 月 24 日 0 時から 5 月 24 日 0 時までの 30 日間である．

調査項目は，トラフィック量，送信元 IP アドレス，送信元 AS，TTL，宛先 IP アドレス，リクエストパケット長，送信元ポート番号，宛先ポート番号，NTP バージョン，NTP 動作モードである．

分析処理では，各調査項目について，パケット全体，NTP パケット，NTP 以外の UDP パケット，ICMP パケット，TCP パケット，その他パケットに分類して集計した．分析には Python3 と Scapy 等を使用し，プロトコル別の統計的分析を実施した．

3　調査結果

3.1　トラフィック量

30 日間の総パケット数は 331,125,016,610 パケット，データ量は 33.4TB であった．表 1 に示すように，NTP パケットが全体の 93.7%を占め，NTP 以外の UDP が 6.2%で続いている．

表 1　プロトコル別パケット数と割合

プロトコル	パケット数	割合 (%)
NTP	310,314,972,025	93.7
UDP(NTP 以外)	20,513,872,169	6.2
ICMP	188,094,610	0.1
TCP	108,061,990	0.0
その他	15,816	0.0

表 2　上位送信元 AS 別パケット分布

AS 番号	国・地域	パケット数	割合 (%)
AS-A	ブラジル	71,490,834,576	21.6
AS-B	中国	61,860,555,202	18.7
AS-C	ドイツ	33,433,601,675	10.1
AS-D	イラク	16,556,300,830	5.0
AS-E	アメリカ	9,933,750,498	3.0

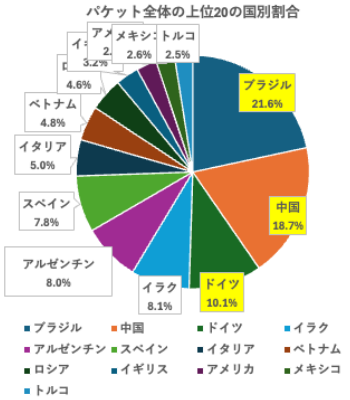

図 1　送信元国別パケット分布（全体）

表 2 に示すように，上位 5 ヵ国の AS が全体の 58.4%を占めている．図 1 は全パケットの送信元国分布を示しており，ブラジル，中国，ドイツの 3 ヵ国で全体の約 50%を占めることが分かる．

5 月 22 日と 23 日の 2 日間でパケット数が増加しており，その原因が NTP パケットであった．表 3 では通常期間と比較して最多 85%の異常増加を示している．

1）　九州産業大学. Kyushu Sangyo University.
2）　福岡女子大学. Fukuoka Women's University.
3）　福岡大学. Fukuoka University.
4）　西日本電信電話株式会社. Nippon Telegraph and Telephone West Corporation.

表 3　5 月 22-23 日の異常トラフィック

日付	パケット数（億）	増加率
5/22	145.7	+42%
5/23	189.3	+85%

3.2　送信元 IP アドレス

5 月 22 日と 23 日の 2 日間のパケット数増加が NTP パケットの特定の IP アドレス（以降 A01 と呼ぶ）によるものであった．A01 からのパケット数が約 600 万倍に急増した．A01 からのパケットは NTP クライアントモード以外の動作モード（モード 7 等）も含んでいた．

3.3　送信元 AS 分析

プロトコル別地理的分析では，NTP はブラジル（21.6%），中国（15.9%），ドイツ（11.9%），NTP 以外 UDP はイラク（AS-D，約 15%），中国（約 12%）が上位を占めた．特に AS-D からの UDP トラフィックが大部分を占め，特定地域からの集中的アクセスが確認された．

3.4　TTL 分析

TTL 分析では，NTP・UDP 初期値 64，TCP 初期値 255 が主流で，約 74%のパケットが 9 ホップ以上を経由し国際的アクセスが多数を占めた．特定 TTL 値（64，128，255）への集中から多様なクライアント環境が確認された．

3.5　ポート番号分析

AS-D からの UDP パケットで 512 番起点 32 間隔の特異な周期性が確認された．図 2 は送信元ポート番号 0-1023（123 除く）におけるパケット数分布を示しており，512 番から 32 番間隔でピークが現れている．この規則的なパターンは，AS-D からのトラフィックが 56.6%（512 番），37.1%（544 番）などの高い割合を占めていることが特徴的である．

表 4　AS-D 発ポート番号の 32 間隔パターン

ポート番号	パケット数	512 からの差
512	1,245,678	基準
544	1,198,432	+32
576	1,187,291	+64
608	1,176,543	+96

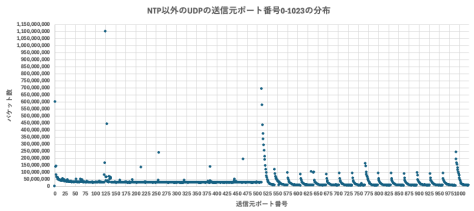

図 2　UDP 送信元ポート番号の周期性（0-1023）

宛先ポート番号については，プロトコルごとに指定するポートが異なっている．

3.6　NTP バージョンと動作モード

NTP バージョンの分析では，バージョン 3 が約 65%，バージョン 4 が約 30%を占めた．これは多くの古いシステムや IoT 機器が依然として NTPv3 を使用していることを示している．

動作モードでは，クライアントモード（モード 3）が約 98%で，正常なクライアント-サーバ通信が大部分を占めた．

しかし，残りの 2%には未定義モードや不正な組み合わせも含まれており，正規の NTP クライアント以外の通信も一定数存在することが確認された．これらの異常な動作モードを持つパケットの大部分は，先述の異常トラフィック源と地理的・AS 的に関連しており，正常な NTP クライアント以外からの通信も含まれていた．

3.7　トラフィック増加の詳細分析

5 月 22-23 日の異常なトラフィック増加について詳細調査を実施した．A01 からの日毎パケット数推移では，4 月 24 日から 5 月 21 日まで 100 パケット以下の正常な通信パターンを示していたが，5 月 22 日から 23 日にかけて約 12 億，約 31 億パケットへと異常な急増を記録した．この期間における時間あたりパケット数は約 608 万パケットに達し，平常時の約 600 万倍という極端な増加率を示した．

このような短期間での急激なパケット数増加が確認された．

4　まとめと今後の課題

本研究では，福岡大学公開 NTP サービスの 30 日間トラフィック（総計 33.4TB）を分析し，複数の分析軸を統合的に組み合わせた包括的なトラフィック特性解明を実施した．

本研究により，公開 NTP サービスへのトラフィックには以下の特徴が明らかになった：(1) プロトコル分布では NTP が 93.7%を占め，時刻同期サービスとして正常に機能している．(2) 地理的分布では特定地域への偏重が確認され，ブラジル・中国・ドイツの上位 3 ヵ国で全体の約 50%を占める．(3) 特定の IP アドレスから 5 月 22-23 日に約 600 万倍のパケット増加が発生した．(4) AS-D からの UDP パケットで 32 間隔の特徴的なポート番号周期性が確認された．(5) NTP バージョン 3 が約 65%を占め，多くの古いシステムが現在も稼働している．(6) TTL 分析から約 74%が国際的アクセスであることが判明した．

今後の課題として，これらの特徴を踏まえた適切な対策の検討が必要である．例えば，レート制限の導入，特定パターンの検知システムの構築，プロトコル検証の強化などが考えられる．

また，引き続き調査分析を継続し，トラフィックの流れや傾向をより詳細に把握する必要がある．特定の送信元 IP アドレスの追跡や，NTP 以外の UDP パケットの詳細調査，送信元ポート番号の周期性のさらなる分析などが今後の課題である．

参考文献

[1] Jim Martin, Jack Burbank, William Kasch, Professor David L. Mills, “RFC 5905: Network Time Protocol Version 4: Protocol and Algorithms Specification,” https://datatracker.ietf.org/doc/html/rfc5905, 2025 年 1 月 30 日参照.

[2] 福岡大学情報基盤センター, “公開 NTP サービス,” https://www.itc.fukuoka-u.ac.jp/i/service/special/public_ntp, 2025 年 1 月 30 日参照.