

2019 年度基幹ネットワーク運用報告

槌屋 洋亮[†], 丸山 広[†] 大足 恭平[†]

抄録 情報メディアセンターでは、本学院の教育・研究・事務系情報システムの根幹を担うネットワークの企画・運用を行っている。本稿では、本学基幹ネットワークの 2019 年度の運用状況と、2019 年度以降の基幹ネットワークの展望について報告する。

キーワード : 基幹ネットワーク

1. はじめに

情報メディアセンターが企画・運用している基幹ネットワークは、本学院の教育・研究・事務系情報システムの情報通信の根幹を担うネットワークである。情報メディアセンターでは、基幹ネットワークの高可用性の実現及びロバスト性を向上させるために回線の増速や冗長化、各種情報システムの分散、冗長化に取り組んできた。また、その運用面では教職員ならびに基幹ネットワーク担当常駐業者が連携し、障害発生への対応、ファイヤウォール、VLAN などの各種設定などを行っており、定例ミーティングやチケットシステムを通じて進捗を管理している。

本稿では、月次定例の資料ならびに進捗管理システムの統計を元に、2019 年度の基幹ネットワークの運用状況と、2020 年度以降の基幹ネットワークの展望について報告する。

2. 2019 年度基幹ネットワーク利用状況

本章では 2019 年度の基幹ネットワークの運用状況として、障害発生件数およびセキュリティインシデント発生件数、インターネットトラフィックの推移、以上について述べる。

2.1 障害・セキュリティインシデント発生件数

図 1 は、基幹ネットワークにて発生した障害の件数を 2019 年 1 月から 12 月と、2018 年 1 月から 12 月で比較したものである。ネットワーク障害の種類は、

主にハードウェアに関するもの（機器故障など）、ソフトウェアに関するもの（脆弱性に起因するものなど）、ネットワーク環境の障害、配線設備等の不具合、そして人為的な動作による不具合が挙げられる。2018 年 1 月から 12 月の間の障害発生件数は 55 件、2019 年 1 月から 12 月までの障害発生件数は 91 件であり、2019 年は障害発生件数が 2018 年と比べて約 1.6 倍、増加した。具体的にみると、2019 年に最も多かった障害は環境関連によるもので、2018 年の 23 件から 35 件に増加している[1]。ネットワーク環境の障害には、例えば一時的なトラフィック量の上昇とそれに伴うネットワーク機器の異常検出、ストーム検出などが含まれ、それらの原因として利用者自身によるループ構成の作成などがある。また、2019 年は配線不備による障害発生件数が 11 件発生しているが、うち 8 件は 2019 年 3 月の基幹ネットワーク更改にて新しい機器への交換を行った際に起きたものである。

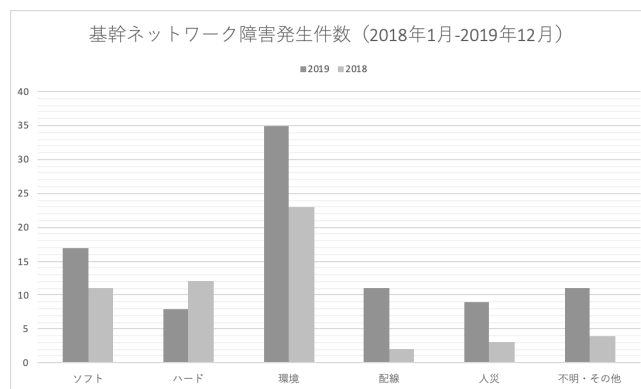


図 1: 基幹ネットワーク障害発生件数

[†] 青山学院大学附置情報メディアセンター

続いて、基幹ネットワークにて発生したセキュリティインシデント件数について述べる。本学基幹ネットワークでは、JSOC (Japan Security Operation Center) によるセキュリティ監視体制を導入しており、基幹ネットワーク上でセキュリティインシデントが発生した場合は、4段階 (Emergency, Critical, Warning, Informational) で検知する。図2は、セキュリティインシデントの Critical の発生件数を、2019年1月から12月と、2018年1月から12月で比較したものである。セキュリティインシデントの Critical は、特定のネットワークに対して外部からの何らかの攻撃が成功した可能性が高いと判断された時に通知される。具体的には、脆弱性を突いた攻撃の成功やマルウェア感染の確認、攻撃成否が不明だが影響を受ける可能性が著しく高い場合、などがある。Critical インシデント発生の際は、該当ネットワークの通信を一時的に遮断する措置が取られ、情報メディアセンターより該当ネットワークの管理者へ攻撃内容について連絡のうえ対処を依頼し、管理者からの対処報告により通信再開の措置を取る。2019年1月から12月までの Critical 発生件数は4件であり、2018年1月から12月の13件から大幅に減少した。

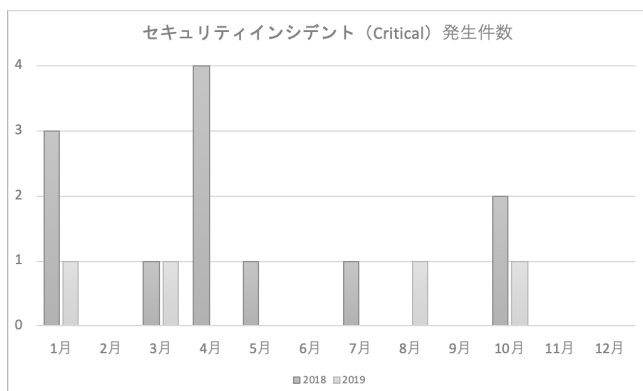


図2: セキュリティインシデント(Critical)発生件数

図3は、セキュリティインシデント Warning の発生件数を、2019年1月から12月と、2018年1月から12月で比較したものである。セキュリティインシデントの Warning は、経過観察が必要と判断された際に通知されるインシデントであり、攻撃の成否を

調査した結果、影響を受ける可能性が無いものや、検知時点で影響を受ける可能性が低く経過観察が必要なもの、等である。Warning に含まれるインシデントの例としては、外部ホストから不審なログインの可能性のある通信を検知した場合や、Web アプリケーションの脆弱性をついた可能性のある攻撃を検知した場合もあれば、単に通常時と比較して突然通信量が増加した場合、などが含まれる。2019年1月から12月までの Warning インシデントの発生件数は10334件であり、2018年1月から12月の9343件よりも増加している。

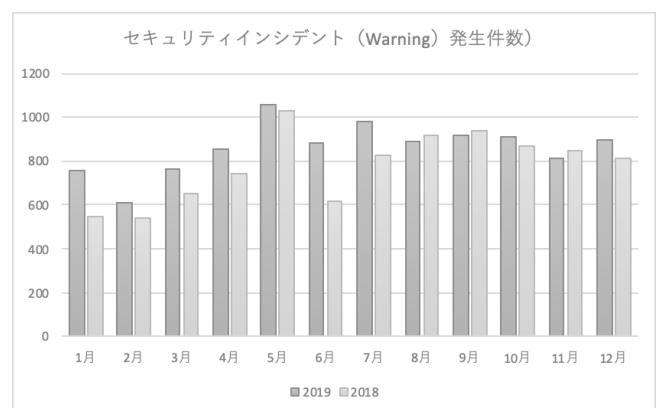


図3: セキュリティインシデント (Warning) 発生件数

2.2 インターネットトラフィックの推移

次に2019年の基幹ネットワークにおけるインターネットトラフィックの推移について述べる。図4は、本学のインターネットルータと SINET 間の、2019年6月から12月末までのトラフィック推移である。本学では2019年度の基幹ネットワーク更改にて、各キャンパスからのそれぞれ最大 10Gbps でのインターネットアクセスが可能となった。2019年度の授業時間帯においては、特に昼から午後帯に一貫して2Gbpsほど利用されていることがわかる。

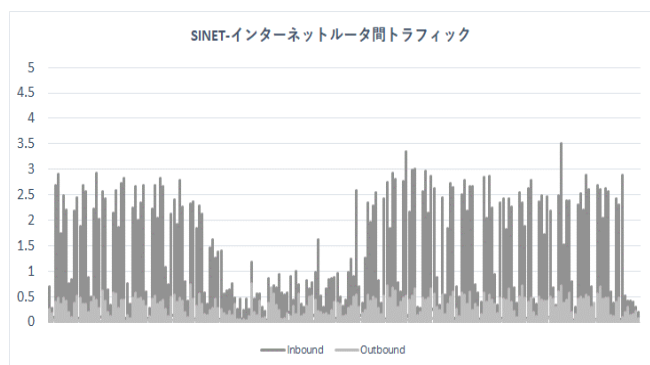


図 4: SINET-インターネットルータ間
トラフィック推移

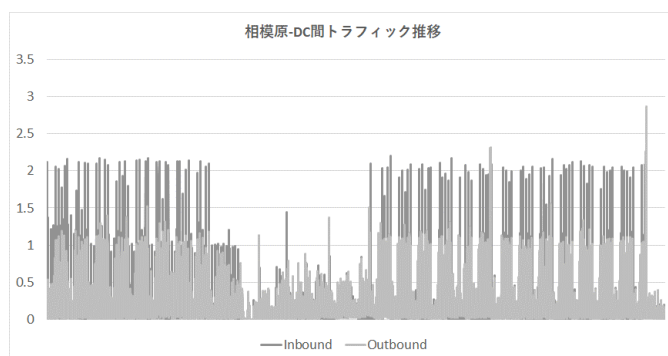


図 6: 相模原-DC 間のトラフィック推移
(2019 年 6 月～12 月)

次に、キャンパスごとのトラフィック推移を示す。2019 年度の基幹ネットワーク更改により、インターネットルータはデータセンター（以下 DC）に設置され、各キャンパスは DC を経由してインターネットへ接続するようになった。図 5 に、青山キャンパス-DC 間のトラフィック推移を、図 6 に、相模原キャンパス-DC 間のトラフィック推移を示す。このトラフィック推移には、インターネットへの通信料の他に、キャンパス間のトラフィック量も含まれる。Outbound（データセンターから各キャンパスへ向かうトラフィック）は、青山-DC 間は概ね 2Gbps で推移している一方で、相模原-DC 間は概ね 1Gbps で推移している。また、Inbound（各キャンパスからデータセンターへ向かうトラフィック）については、青山-DC 間が 1Gbps で推移している一方で、相模原-DC 間が 2Gbps で推移している。

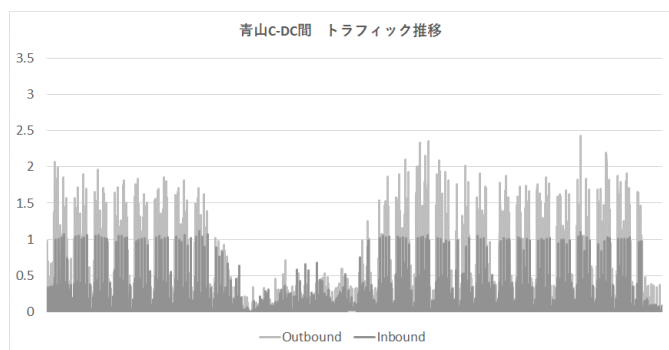


図 5: 青山-DC 間のトラフィック推移
(2019 年 6 月～12 月)

次に、2019 年 12 月 9 日（月）から 12 月 15 日（日）までの間の SINET-インターネットルータ間のトラフィック推移を、図 7 に示す。また、同時期の各キャンパスと DC 間のトラフィック推移を図 8 に示す。両キャンパスともに木曜日のトラフィック量が多く、水曜日のトラフィック量は、他の曜日と比較して少ないことがわかる。特に、青山キャンパスでは通常の PC 教室での授業、公開 PC 室に加え、無線 LAN アクセスポイントからのインターネット利用者が多いことも、両キャンパスの間でのトラフィック量の差異の 1 つの要素であることが推測される。

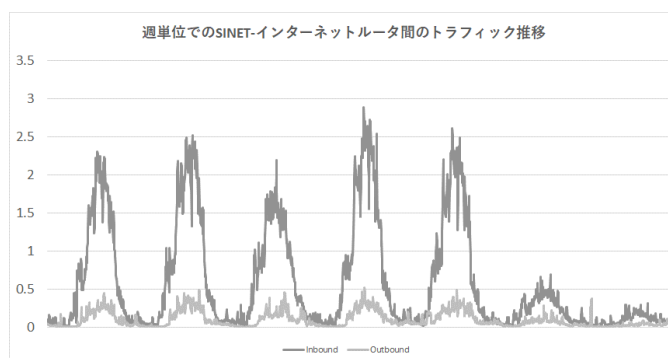


図 7: 週単位での SINET-インターネットルータ間
のトラフィック推移
(2019 年 12 月 9 日～12 月 15 日)

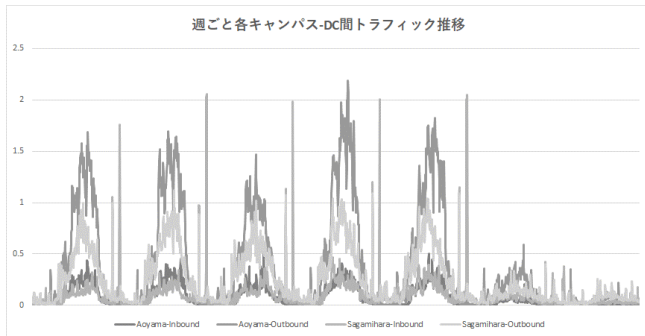


図 8: 週単位での各キャンパス—DC 間のトラフィック推移 (2019 年 12 月 9 日～12 月 15 日)

最後に、インターネットルータ～eduroam でのトラフィック推移 (青山・相模原の合計値) を、図 9 に示す。本学では 2017 年度の教育研究システム更改により eduroam を導入し、学外関係者もインターネット接続を利用できるようになった。eduroam のトラフィック推移は一貫して 300Mbps 程度あり、学外関係者による一定したインターネット利用があることが推測される。

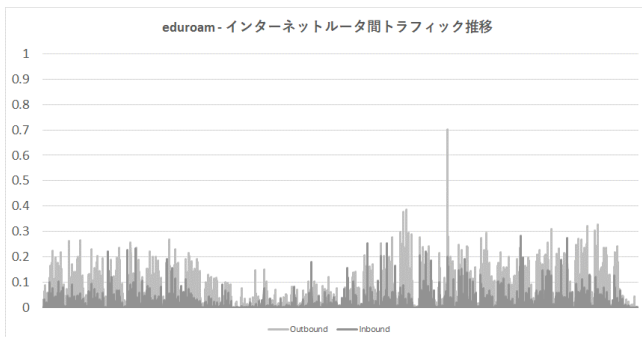


図 9: eduroam – インターネットルータ間
トラフィック推移

インターネットトラフィックについては、2018 年 9 月より両キャンパス合計で 1Gbps の環境であり、相模原キャンパスにおいてはアクセス状況に改善が見られたが、全体としては逼迫状態が継続していた。2019 年度基幹ネットワーク更改により、両キャンパスおよび本学—SINET 間の接続環境が 10Gbps へ改善された。特に、青山キャンパスからのインターネット接続が解消された。

3. 基幹ネットワーク運用状況

基幹ネットワーク運用では、通常運用業務とは別に、イレギュラーな課題や運用改善案などについて、課題管理システムを用いて管理し、2 週間に一度の定例ミーティングにて進捗把握を行っている。検討課題としては、基幹ネットワークで導入している機器の OS 更新、不具合・脆弱性への対応に加えて、サービス申請フローの検討2019年度基幹ネットワーク更改に伴う運用課題の検討などがある。

図 10 では、2019 年 1 月から 2020 年 1 月までの間に起票された課題の進捗状況をまとめたものである。この期間に起票されたチケット数は 116 件である。そのうち 2020 年までに終了もしくは解決しているのは 75 件であり、チケットが起票された時期にもよるが、2019 年 1 月から 2020 年 1 月までの間の消化率は 67%であった。

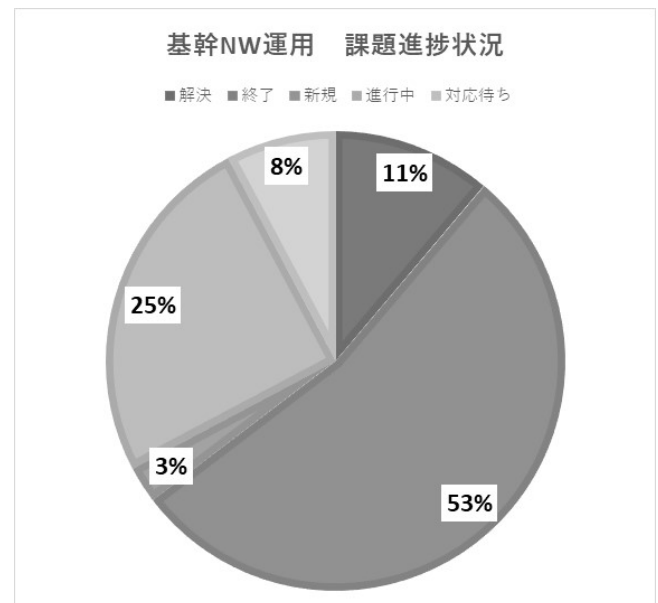


図 10:課題の進捗状況

また、表 1 に、終了したチケット 62 件について、起票日から終了するまでにかかった日数を集計した結果を示す。チケットの消化にかかった日時は、平均 91.7 日であり、概ね 3 か月程度平均して掛かっている。

表 1：チケット終了に要した日数

日数	件数
7 日未満	4
30 日未満	14
60 日未満	15
90 日未満	7
120 日未満	2
150 日未満	5
150 日以上	15

今年度は、運用方針に関わるものとしては、2019 年度の基幹ネットワーク更改によって導入されたシステムの運用フロー検討、それに伴う申請書の改定、2018 年度までの運用フローの改定などがある。2019 年度の基幹ネットワーク更改により、DNS ファイアウォール、リスクベース認証の導入など、ネットワークセキュリティ面での強化が図られた。一方で、これらは利用者への影響も大きいので、前述の定例ミーティングにて運用フローの検討を慎重に行い、利用者への周知を徹底した。

前年度に引き続き今年度もインシデント対応の行われていないネットワークへの対応の検討を行ってきた。具体的には、脆弱性への対処報告がなされないままインシデントが発生し続けるケースに関しては、基幹ネットワーク運用にて該当ネットワークへの通信遮断措置を行う場合のフローについての検討を行った。脆弱性への対処フローについては引き続き検討を続け、改善に努めたい。

その他、今年度は、無線 LAN 増設要望への対応の基本方針についても検討した。昨今のスマートフォン、ノート PC の普及に伴い、無線 LAN への増設要望が各所から絶えない。増設要望へ対応するための条件と、他部署との連携もとりながら増設する際の手順について検討を行った。さらには、NII が提供する eduroamJP 認証連携 ID サービス[2] の導入について検討し、2020 年 4 月以降の提供開始に向けて運用フローについてまとめた。来年度も、他部署とも連携をとりながら、ネットワークの利便性の向上を目指す

して、基幹ネットワークの運用に努めてゆきたい。

4. おわりに

本稿では、情報メディアセンターが提供する基幹ネットワークと今後の展望について報告した。本学院に求められるネットワークは一般的な企業等の組織に求められるネットワークと大きく異なる点がある。まずは、その用途の多様さである。先にも述べた通り、教育・研究・事務系と様々な目的を持った情報システムが基幹ネットワークを利用するため、求められるネットワーク像は利用者により異なる。

そのため、様々な利用者が期待する利便性と安全性のバランスを併せ持つ基幹ネットワークの実現は、情報メディアセンターが今後も継続して検討していかなければならない課題の一つである。2020 年度以降も急速に変化していく技術や本学院を取り巻く状況を視野に入れながら、柔軟かつ頑強なネットワークを実現することが必要である。情報メディアセンターは、そのようなネットワークが本学院の教育・研究活動を一層充実させる礎となると考え、技術基盤や組織体制の改善に今後も継続して取り組んでいく所存である。

参考文献

- [1] 槌屋洋亮, 丸山広, 大足恭平, 櫻井淳, 根本貴弘
「2018 年度基幹ネットワーク運用報告」青山インフォメーション・サイエンス, Vol.46, No.1, 2019, pp.80-84.
- [2] eduroamJP 認証連携 ID サービス <https://federated-id.eduroam.jp/> 2020 年 2 月 29 日アクセス