

2023 年度 基幹ネットワーク運用報告

中川 幸子[†], 丸山 広[†], 内野 文貴[†],

抄録 情報メディアセンターでは、青山学院の教育・研究・事務系情報システムの根幹を担う基幹ネットワークの企画・運用を行っている。本稿では、基幹ネットワークの 2023 年度の運用状況と、2024 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, セキュリティインシデント, DNS Firewall

1. はじめに

青山学院における基幹ネットワークは、教育・研究・事務系情報システムの情報通信基盤として中核的な役割を担っている。基幹ネットワークは、情報メディアセンターが主体となり、その企画・運用が行われている。基幹ネットワークの高可用性を確保し、ロバスト性を向上させるために、回線の増強・冗長化や、各種情報システムの分散が進められてきた。運用においては、教職員と基幹ネットワーク担当常駐業者が連携しながら、障害発生への対応、ファイアウォールやVLANなどのネットワーク設定管理を実施している。これらの業務は、定例ミーティングやチケット管理システムを活用し、進捗や課題の可視化と共有を行いながら継続的な改善が図られている[1]。

本稿では、2023 年度（2023 年 4 月 1 日から 2024 年 3 月 31 日）における基幹ネットワークの運用実績として、障害発生やセキュリティインシデントへの対応状況、基幹ネットワークの利用状況、ネットワーク系システムである VPN とメール配送システムの利用状況、チケット管理システムを用いた課題管理について、過去年度との比較をしながら分析し、最後に、2024 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. 基幹ネットワーク運用状況

本章では 2023 年度の障害発生件数、セキュリティインシデント発生件数について述べ、大きな問題が生じていないことを明らかにするとともに、セキュリティインシデント対応の強化について述べる。

2.1 障害発生件数

図 1 は、2019 年 4 月導入以降の障害発生件数を、年別に集計したものである。発生した障害の原因は、以下の 5 つに分類している。

1. ソフト：ソフトウェアバグに起因する障害
2. ハード：機器故障による機能停止やセンサー異常
3. 環境：夜間バッチ処理による CPU 高負荷状態の長時間継続や、センター管理外の機器故障によるネットワークストーム
4. 人災：LAN ケーブル配線ミスによる周辺ネットワークの通信障害や分電盤の誤操作
5. 配線：LAN ケーブルの接続ミスによる当該機器の通信障害

2023 年度の障害発生件数は 96 件であり、特にハード故障の発生頻度が高い。発生件数は昨年よりもやや減少したものの、依然としてハードウェアに起因する障害が多数を占めている。なかでも、無線アクセスポイント（以下、無線 AP）の故障が顕著であり、ハード

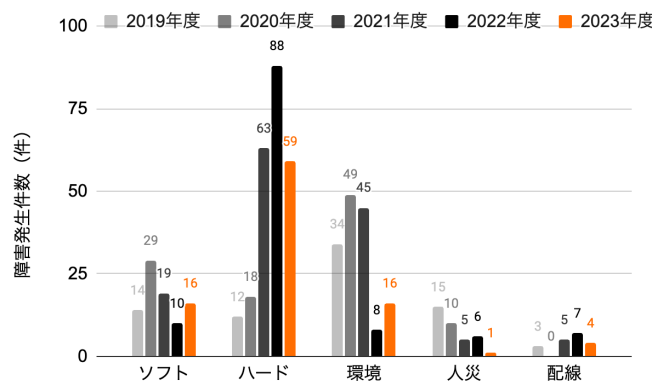


図 1 障害発生件数

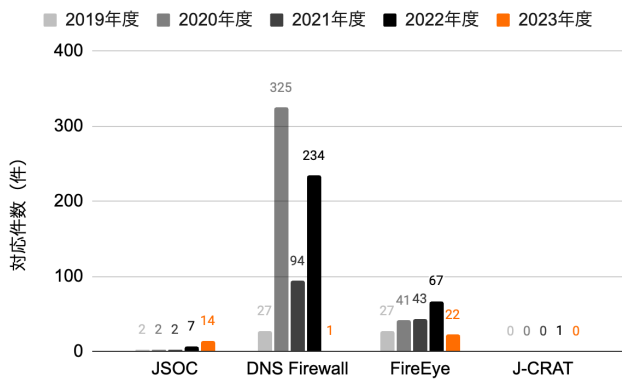


図2 セキュリティインシデント対応件数

ウェア障害の大半を占める結果となった。故障が発生した無線 AP の設置箇所の多くにおいては、近隣にも無線 AP が設置されているため、「予備機と交換が完了するまで無線 LAN の接続が不可能」といった事態は回避されている。しかしながら、2021 年度移行、無線 AP の故障が顕著に増加しているため、その原因究明が急務となっていた。この状況を踏まえ、メーカーへ正式に調査を依頼した結果、特定のロットの半導体部品が故障することが判明したため、対象となる無線 AP の交換対応を実施し、2023 年度 12 月末をもって対応を完了した。

一方で、人災による障害の発生件数は、低い件数に抑えられているものの、居室のレイアウト変更などに伴う配線ミスによる障害がしばしば発生している。この障害は、棟全体へ影響を及ぼすこともあり、発生時のインパクトは大きい。特に、無線 LAN ルータの接続ミスはしばしば起きているため、具体的な図を用いた注意喚起を行い、着任時に配布する資料において適切な接続方法について周知を行なっている。

2.2 セキュリティインシデント対応件数

サイバーセキュリティのインシデントの検知方法には利用者自身による申告をはじめ、様々な方法があるが、本節では基幹ネットワークのセキュリティとして導入している侵入検知システム、ウィルス・マルウェア対策システム、DNS セキュリティシステムで検知されるインシデント対応について述べる。

侵入検知システムは、JSOC (Japan Security Operation Center) を導入している。IDS のセンサーが収集した学内外との不審な通信を検知し、脆弱性を利用した攻撃が成功した際や、利用者の端末から学外の不審サーバ

への通信が成功した際は、インターネット通信を自動的に遮断する。この時、学内に設置されているサーバ・機器への通信は遮断されない。

ウィルス・マルウェア対策システムは、FireEye ネットワークセキュリティを導入しており、マルウェアやウィルスに特有の振舞いをネットワーク上で検知した際は、支線ネット管理者や機器の管理者へ通知している。通信の自動遮断までは実施していないため、検知結果を元に利用者を特定し、メールで連絡している。

DNS セキュリティシステムには、DNS サーバとして導入している Infoblox の DNS Firewall 機能を利用している。DNS Firewall は、C&C サーバやマルウェア配布サイト、フィッシングサイトなどの悪意のあるサーバの FQDN をデータベースとして持ち、学内利用者（の端末）が悪意のあるサーバに通信しようとした際に、本来の IP アドレスではなく、ダミーの IP アドレスを応答することで、悪意のあるサーバとの通信を回避する。ダミーの IP アドレスにアクセスすると、警告ページが表示される仕組みを運用しているが、利用者自身がブラウザでアクセスして警告ページを目にするケースはなく、ウィルスやマルウェアがバックグラウンドで通信していることが判明している。

図2に、上述した JSOC、DNS Firewall、FireEye、および J-CRAT で不審な通信を検知した際の対応件数を2019年度から年度ごとに示した。JSOC および J-CRAT におけるセキュリティインシデントの判定は、単なる機械的な検出にとどまらず、人手による詳細な分析も経た上でセキュリティインシデントと確定されるため、アラート発生時の危険度が高いと考えられる。そのため、検知通知が行われるとほぼ同時に、自動遮断により、インシデントの拡大を未然に防ぐ対応を行っている。

他方、DNS Firewall は、2019 年 4 月のシステム更改で導入し、過剰検知や利用者影響を慎重に検証しながら試験的な運用を継続してきた。2020 年度からは本格運用を開始し、とくに検知件数が多いものや、一定のパターンとして注意が必要なものを優先的にユーザーへ通知する対応を進めた結果、DNS Firewall 検知への対応件数が 200 件以上となり急増した。しかしながら、本システムは膨大な数のアクセスを監視する性質上、多数の検知アラートが発生するが、それらすべてのアラートが直ちに危険であるとは限らず、次節 2.3 に述べる通り、影響度の小さいものが含まれている。そこで、2022 年後半より、優先順位を明確化し、影響度が

とくに大きいと判断される場合のみ対応を行う方針へと運用の見直しを行った。その結果、図2のDNS Firewallでは、2023年度の対応件数はほとんど発生していないが、これは検知自体が無くなったことは意味するものではなく、対応対象を限定した運用の結果である点は留意が必要である。

2.3 セキュリティインシデント対応の強化

情報セキュリティ対策を強化したとしても、ネットワーク侵入やマルウェア感染などのサイバーセキュリティインシデントを100%防ぐことはできないため、外部への攻撃通信や感染してしまった際の情報漏洩、二次被害を発生させないことが重要である。

学外からのネットワーク侵入や学外への攻撃通信は、JSOCにより検知された場合、基幹ファイアウォールによる自動遮断を行っている。他方、学内で利用されている端末からの不審な通信は、FireEye および DNS Firewallによって検知されている。ただし、これらのシステムは、検知後の対応に人による調査や連絡、オペレーションを必要とするため、即座に対応ができているとは言い難い。

DNS Firewallについては、DNS クエリを判断基準としているため、ウェブ検索結果の一部サイトや、広告に不審なサイトが表示されたことでも検知することが分かっており、自動的な通信遮断は過剰反応と言える。一方、FireEyeについては一連の通信からウィルス・マルウェアに感染している端末かどうかを判断しているため、その信頼度は高い。しかしながら、検知した後にウィルススキャンをしても何も検知されないケースがしばしば発生している。

FireEye の検知条件を慎重に精査し、自動遮断された端末がインターネット閲覧を試みた際に、当該端末が遮断されていることが分かる仕組みを構築することがもとめられる。これにより、学内ネットワーク環境において自動遮断を適切に機能させ、セキュリティインシデントの拡大を防止する体制の整備が必要である。

3. 基幹ネットワーク利用状況

本章では、2019年4月から2024年3月末までのネットワークトラフィックの推移をもとに、基幹ネットワークの利用状況について述べる。

3.1 インターネットの利用状況

図3に、データセンター（以下、DC）と SINET 間

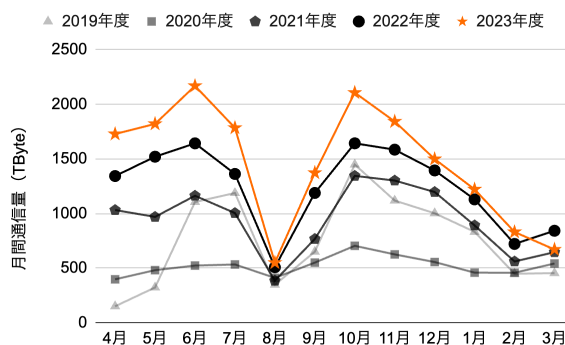


図3 DC-SINET 間の月間通信量推移

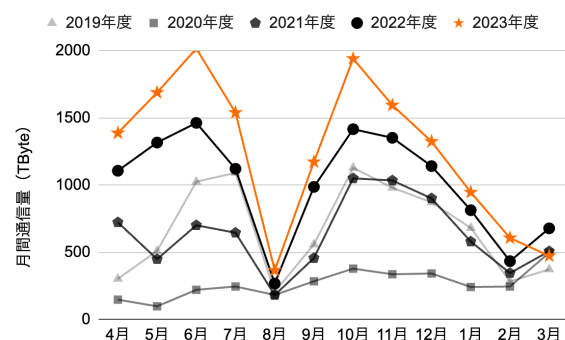


図4 青山キャンパス-DC 間の月間通信量推移

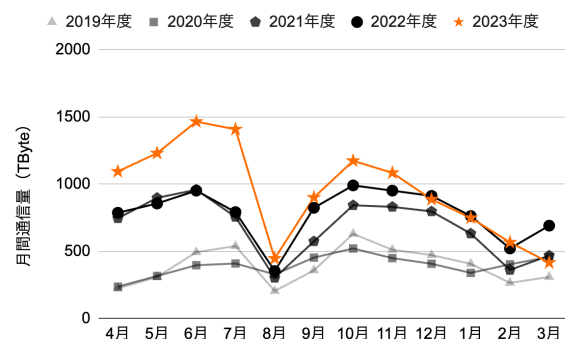


図5 相模原キャンパス-DC 間の月間通信量推移

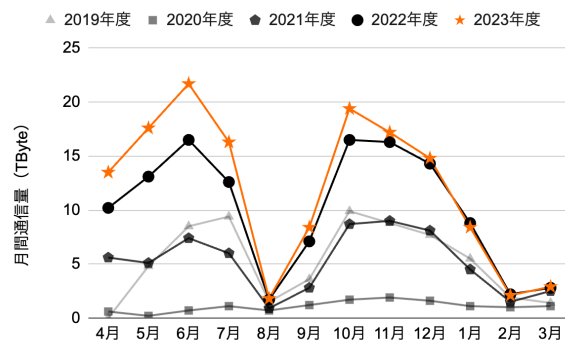


図6 DC-eduroam 間の月間通信量推移

の月間通信量の推移を示す。通信が多い月・少ない月の傾向は例年と同じであるが、一番多い 6 月は約 2200TByte となり、過去最多の通信量となった。

図 4 は青山キャンパス、図 5 は相模原キャンパスから DC への月間通信量である。青山キャンパスからの通信量、相模原キャンパスの通信量とも、前年度と比べると 1.2 倍程度増加している。本システム導入時年度の 2019 年度と比較した場合では、青山キャンパスは 1.9 倍、相模原キャンパスは 2.4 倍に増加しており、両キャンパスともノートパソコンやタブレットなどの情報通信機器を持ち込む学生が倍増していると考えられる。

図 6 は eduroam の月間通信量推移である。こちらも、前年度と比較して 1.2 倍、2019 年度と比較した場合は 2.3 倍の増加となっており、学会活動などの学外者利用が活発になっていると考えられる。

3.2 ピークトラヒックの推移

各月の通信帯域最大使用量（ピーク）の推移を図 7 と図 8 に示す。図 7 はダウンロード通信のピーク、図 8 はアップロード通信のピークを示している。

3.1 にて述べた月間通信量ほどの変化はないが、ダウンロードのピークは年度ごとに増加傾向にある。現在敷設している回線は 10Gbps の通信が可能であるため、直ぐに逼迫する状況ではないが、5 年後・10 年後に逼迫を生じさせないために、システム更改のタイミングでの帯域の増強を検討している。

3.3 アプリケーションごとの通信量

2023 年度の各月のアプリケーション分類ごとの通信量の推移を図 9 および図 10 に示す。図 9 はダウンロード通信量、図 10 はアップロード通信量をそれぞれ示している。アプリケーションの分類は、オンライン授業・映像配信・SNS・オンラインストレージ・コミュニケーションの 5 つに大別した。各アプリケーション分類の内訳を表 1 に示す。

ダウンロード通信量に関しては、年間を通じて映像配信が最も多く、次いで、オンラインストレージ、SNS の利用が多い傾向が見られる。一方、アップロードの通信量は、オンラインストレージが最も多く、とくに 1 月から 3 月にかけて通信量が突出していることが確認された。この増加は、授業期間終了後におけるデータ移行や整理によるものと推察される。次いで、映像配信のアップロード通信量が多いが、8 月と 2 月に顕著な増加が見られることから、授業以外の用途が活発

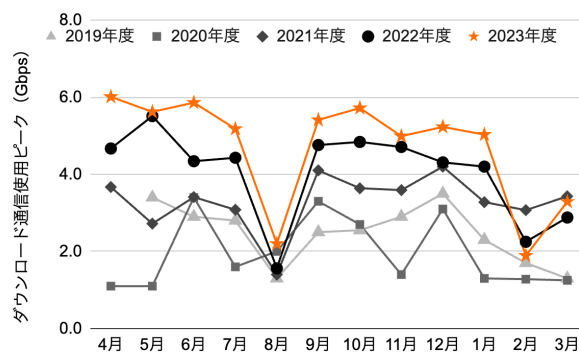


図 7 DC-SINET 間のダウンロード通信
ピークトラヒック推移

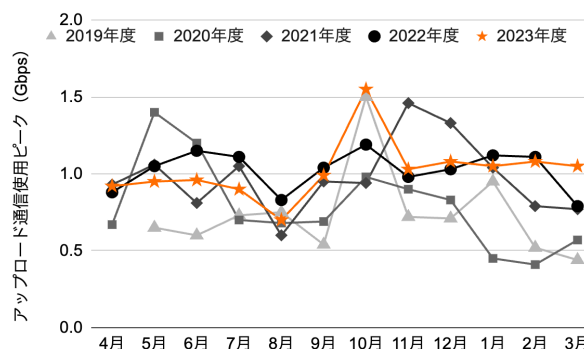


図 8 DC-SINET 間のアップロード通信
ピークトラヒック推移

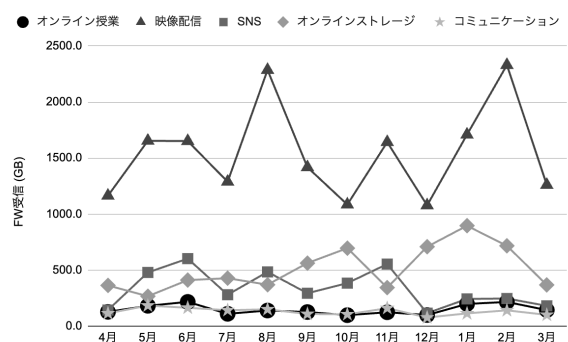


図 9 アプリケーションごとのダウンロード通信量

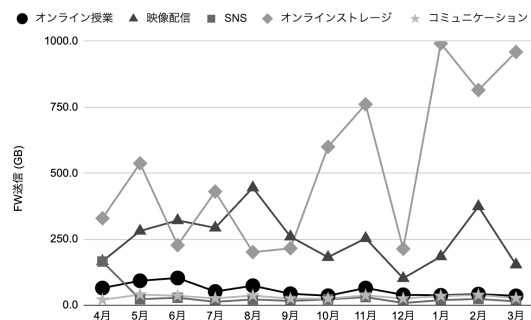


図 10 アプリケーションごとのアップロード通信量

化したと考えられる。

なお、2023 年 4 月に、1 日で 12019.8GB の SNS の利用が観測されたが、1 研究室の 1 端末での利用であることが確認されているため、外れ値としてあらかじめ省いてグラフ化した。

4. VPN とメール配送システム利用状況

本章では、学外から学内ネットワークに接続するための VPN の利用状況と、コミュニケーション手段として重要性が高いメールについて、CoursePower を始めとする学内システムからのメール通知や、自営部局メールサーバが利用しているメール配送システムの利用状況について述べる。なお、職員が利用する事務系の VPN は別システムであり、本章の数値には含まれない。

4.1 SSL-VPN の利用状況

図 11 は SSL-VPN の接続ユーザー数の日別平均をグラフにしたものである。一定して 10 から 30 ユーザーの接続が観測された。サーバを 2 台用いて、500 ユーザーまで同時利用できるサービスとして運用しているが、この利用状況から、脆弱性対応などのメンテナンスの際に、一時的に 1 台での運用を行っても問題は生じない利用状況である。

4.2 メール配送システムの利用状況

基幹ネットワーク系システムが運用しているメール配送システムは、学外から学内メールサーバ（自営部局メールが対象であり、AOYAMA-mail は含まれない）へのメールを中継する外部メールサーバと、CoursePower を始めとする学内システムから送信されたメールを中継する内部メールサーバから構成される。

図 12 は外部メールサーバが受信したメール件数を日毎にカウントしたものである。突発的に 1 万通を超える迷惑メールが届くこともあるが、おおむね 5,000 通のメールを受信・中継しており、増加・減少傾向は見られない。

図 13 は内部メールサーバが受信したメール件数を日別にカウントしたものである。学内システムからのメールは、授業期間中は 5 万通前後で推移しており、今年度は前期と後期で大きな推移の変化は見られなかった。

表 1 アプリケーション分類の内訳

分類	内訳
オンライン授業	webex-base, ms-teams, zoom-meeting
映像配信	http-video, netflix-base, quic, youtube-base, itunes-base
SNS	facebook-base, instagram-base, twitter-base, tiktok
オンラインストレージ	dropbox-base, google-drive-web, ms-onedrive-base
コミュニケーション	naver-line, slack-base

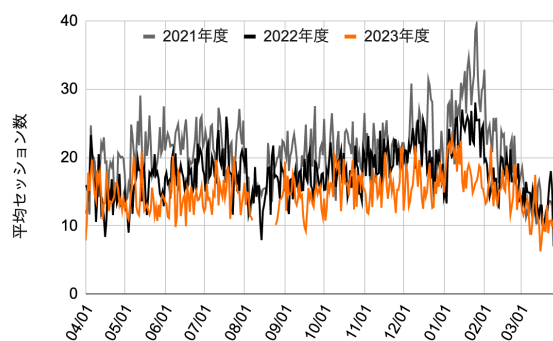


図 11 SSL-VPN 接続 接続数推移

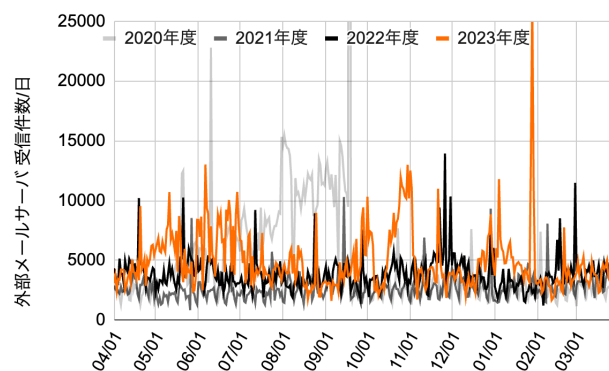


図 12 外部メールサーバ受信件数

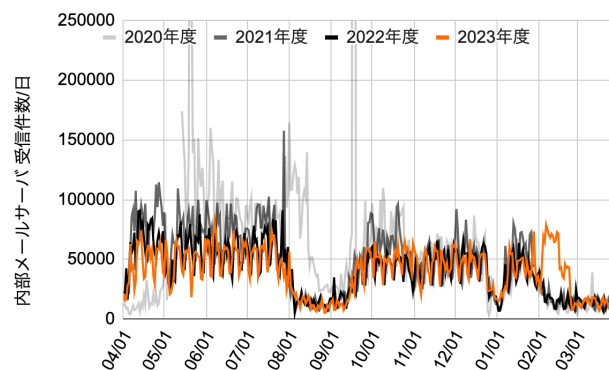


図 13 内部メールサーバ受信件数

5. 課題管理

本学の基幹ネットワークの運用は、情報メディアセンターの教職員 7 名（他の業務と兼務）と常駐業務委託 5 名の協力体制のもと実施されている。ネットワーク運用においては利用者からの申請対応や機器障害への対応に加え、設計変更やポリシー変更を伴う要望への対応、脆弱性対応方針の検討、ならびに運用改善案の策定が求められる。これらの課題は、チケット管理システムを用いて管理し、定例ミーティングにおいて協議が行われている。2021 年 6 月からは、このミーティングを毎週開催しており、継続的な課題管理の強化を図っている。

図 14 は、2023 年度の基幹ネットワークに関する課題チケットの件数の推移を示している。2023 年 4 月 1 日時点で進行中のチケットは 130 件であった。10 月上旬にチケット数が一時的に減少しているが、これは夏季法定点検による停電を利用したシステムメンテナンスの実施により、多数の課題が解決されたことに起因する。この動向は、過去年度と同様の傾向を示している。2023 年度に新規作成された課題は、113 件であり、そのうち 54 件（約 48%）が 2023 年度末時点で完了している。月平均 20 件のペースで、課題が完了している一方で、同程度のペースで新規課題が作成されており、進行中の課題件数は概ね 130 件前後で推移している。なお、この課題件数には、2.2 に前述した SOC 活動における個別のセキュリティインシデント発生への対応件数は含まれていない。

2023 年度においては、山積する日々の課題に加え、2024 年度実施を目標とした大学無線 LAN のセキュリティの対策強化に向けた運用体制の構築に取り組んだ。本施策は、不正な通信や不正なプログラムの挙動を検知した際に、当該端末を自動的に学内ネットワークから遮断することを目的とする。この施策の実施には、単なるシステム設定の変更にとどまらず、ユーザーへの周知や窓口対応と連携したサポートラウンジの運用

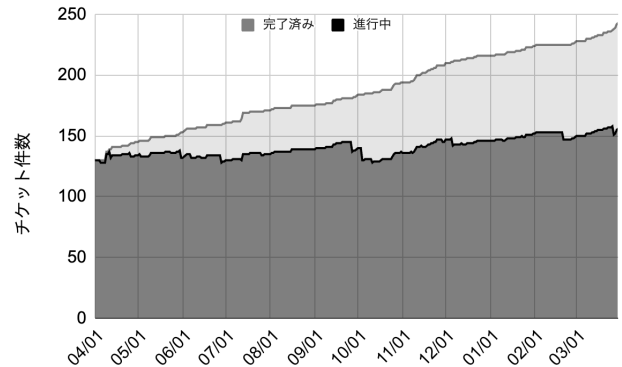


図 14 課題管理チケット数・完了数推移

体制の整備が不可欠である。これらの対応を含め、1 年間をかけて次年度施策実施に向けた体制を構築した。

6. おわりに

本稿では、基幹ネットワークの利用状況と現状の課題、今後の展望について報告した。基幹ネットワークは、教育・研究・事務系と性質の異なる目的を持った情報システムおよび利用者によって活用されており、それに伴い求められるネットワークの要件も多様化している。とくに、最近のオンライン授業の普及や BYOD（Bring Your Own Device）の増加など、利用形態の急激な変化が進む中で、基幹ネットワークがこれら変革の阻害要因にならないよう、その運用と設計を適応させる必要がある。今後も、通信速度などの性能面のみならず、利便性と安全性のバランスを考慮しながら、継続的な改善を進めていく。

参考文献

- [1] 丸山広, 中川幸子, 内野文貴「2022 年 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.51, No.1, 2023, pp.38-42.