

## 2022 年度 基幹ネットワーク運用報告

丸山 広<sup>†</sup>, 中川 幸子<sup>†</sup>, 内野 文貴<sup>†</sup>,

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 2022 年度の運用状況と、2023 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

情報メディアセンターが主体となって企画・運用している基幹ネットワークは、青山学院全体の教育・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、および、ロバスト性を向上させるために回線の増強や冗長化、各種情報システムの分散に取り組んできた。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、ファイアウォール、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・課題を管理している。

本稿では、2022 年度（2022 年 4 月 1 日から 2023 年 3 月 31 日）の基幹ネットワークの運用状況、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つつ述べ、最後に、2023 年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 2022 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

2022 年度の障害発生件数は 119 件であり、特にハード故障が多く発生した。発生件数は昨年[1]と同水準であるが、ソフト・環境の障害発生件数が減少し、ハード障害が著しく増加した。その大半は無線アクセスポイント（以下、無線 AP）の故障であった。故障した無線 AP の設置箇所の多くは近辺にも無線 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 に繋がらない」という事態の発生はさけられている。2021 年度の取り組みにより予備機の台数を増やしているため、交換作業には遅延は生じていないが、2021

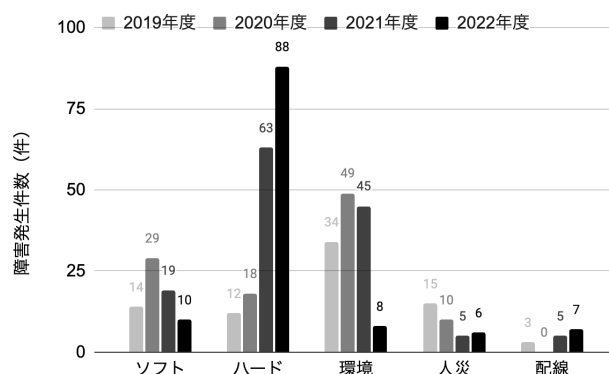


図 1 障害発生件数

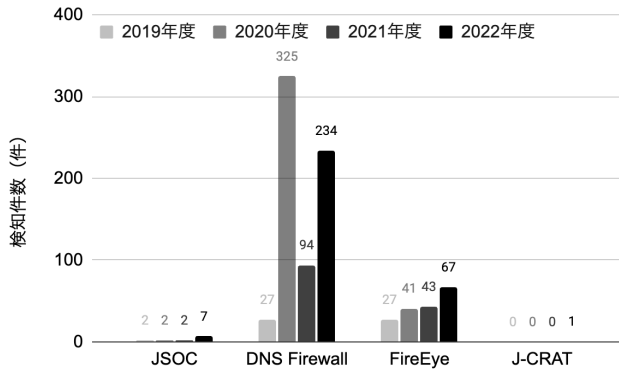


図2-(a) 検知手段別の検知件数（年度毎）

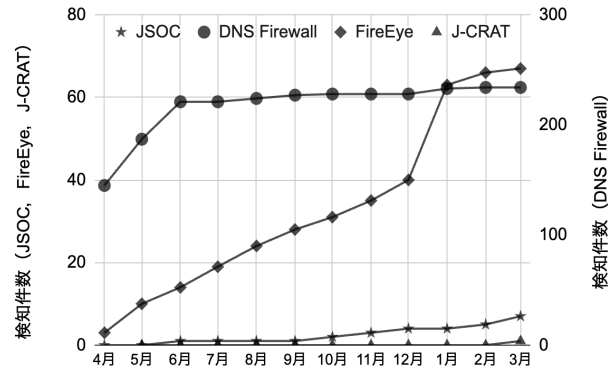


図2-(b) 2022年度検知件数の月次推移

図2 セキュリティインシデント発生件数

年度に引き続きの障害であるため、メーカーと継続的に交渉している。

他方、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発生件数が増加傾向にある。特に、無線 LAN ルータの接続ミスがしばしば発生しているため、具体的な図を用いた注意喚起を发出している。

## 2.2 セキュリティインシデント発生件数

情報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の検知件数について述べる。

侵入検知システムは、IDS のセンサーが収集した学内外との不審な通信を JSOC（Japan Security Operation Center）が分析し、脆弱性を利用した攻撃が成功していたり、利用者の端末から学外の不審サーバへの通信が成功していたりすると、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として、FireEye ネットワークセキュリティを導入しており、ウィルス・マルウェアに特有のネットワーク通信を検知・管理者に通知している。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进行を特定し、メールで連絡している。

DNS セキュリティシステムとして、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分かっている。

図2に、セキュリティインシデント発生件数を示す。(a)は、上述した JSOC、FireEye、DNS Firewall、および J-CRAT の年度ごとの検知件数であり、(b)は2022年度の月別の推移である。2019年4月以降のデータを示しているが、JSOC 以外のシステムは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避けるため、仮運用を続けてきたため、本格運用を始めた2020年に入ってから検知が急増している。2022年度は、DNS Firewall 以外の検知が過去最多となっている。特に、JSOC および J-CRAT は、機械的な判定だけでなく人手による分析も経てセキュリティインシデントと判断しており、危険度が高い。次節で述べる自動遮断が実現することで、これらのインシデントの発生を抑えることを目指している。

## 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、インシデント・感染を100%防ぐことはできないため、感染してしまった際に情報漏洩や外部への攻撃通信を発生させないことが重要である。

学外からの攻撃や学外への攻撃通信を検知する JSOC については、基幹ファイアウォールによる自動遮断ができていますが、学内で利用されている端末からの不審な通信を検知する FireEye および DNS Firewall については、検知後の対応がすべて人によるオペレーションを必要としており、迅速な対応ができていたとは言い難い。

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、遮断された端末がインターネット閲覧をしようとした際に、遮断されていることが分かる仕組みを構築することで、自動遮断することで被害の拡大を防ぐ学内ネットワーク環境を目指す。

### 3. 基幹ネットワーク利用状況

本章では、2019 年 4 月から 2023 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、過去最多の通信量となり、一番多い 6 月は約 1700TByte 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の増加が大きく、相模原キャンパスはほぼ例年通りであるが、2022 年度後期から前年度と比べると通信量が増えている。

2022 年度は、緊急事態宣言等の登校する学生数が著しく減る事象は生じていないため、2022 年度の通信状況が、今の学生たちのネットワーク利用状況を表していると考えられる。2019 年度と比較すると、相模原キャンパスの方が、どの月も約 2 倍に増加しており、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。昨年の報告[1]では、

#### センター活動報告 - システム運用報告

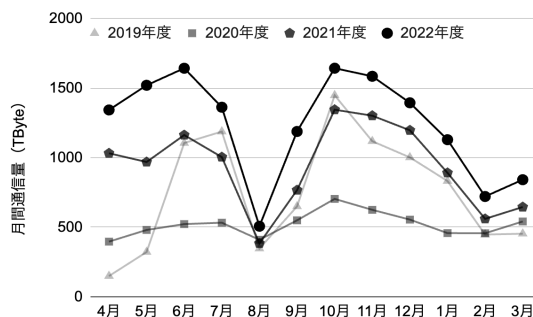


図 3 DC-SINET 間の月間通信量推移

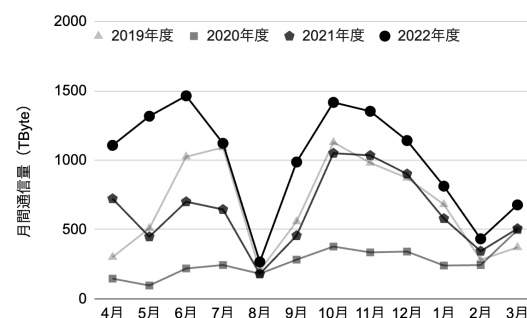


図 4 青山キャンパス-DC 間の月間通信量推移

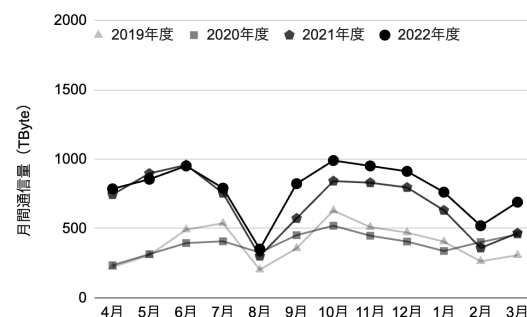


図 5 相模原キャンパス-DC 間の月間通信量推移

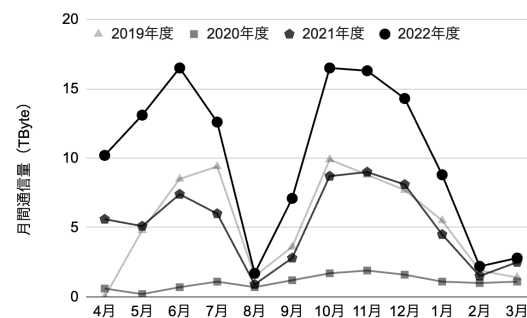


図 6 DC-eduroam 間の月間通信量推移

青山キャンパスも今後倍増すると予想していたが、5月の利用は著しく増えたものの、1年間を通して2019年度と比較すると、約2割の増加に止まっている。

図6はeduroamの月間通信量推移である。2019年度・2021年度と比較してほぼ倍増しており、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 ピークトラフィックの推移

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、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。

## 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コロナ禍においては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9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察された。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10は外部メールサーバが受信したメール件数を

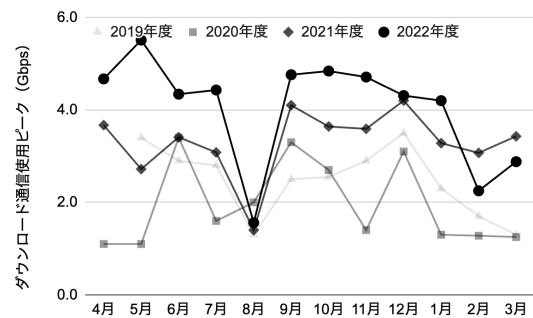


図7 DC-SINET 間のダウンロード通信  
ピークトラフィック推移

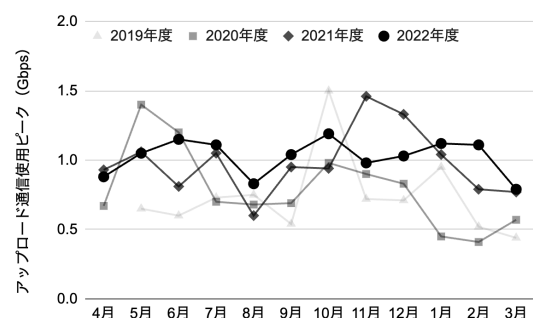


図8 DC-SINET 間のアップロード通信  
ピークトラフィック推移

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3,000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11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、前期に10万通前後、後期に6万通前後で推移しており、この傾向は変わっていない。

## 5. 課題管理

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8名（他の業務と兼務）と常駐業務委託5名が連携して行っている。利用者からの申請や機器障害への対応とは別に、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や運用改善案などについてチケット管理システムを用いて管理し、定例ミーティングを行っている。2021年6月からは以前の隔週開催から毎週開催へと変更し、「数日は待てるが2週間は待てない」課題がチケット管理システムに乗ら

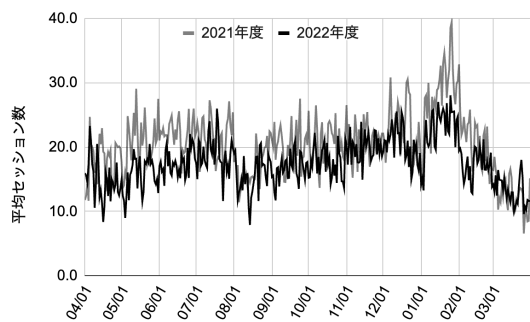


図 9 SSL-VPN 接続 接続数推移

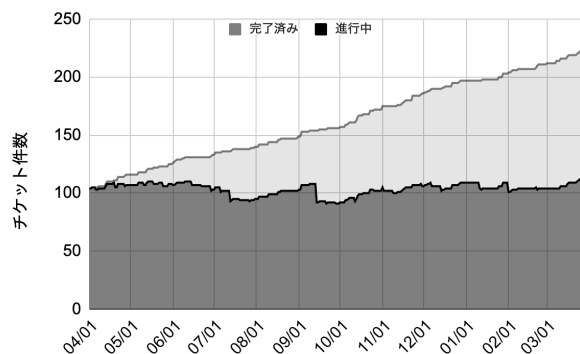


図 12 課題管理チケット数・完了数推移

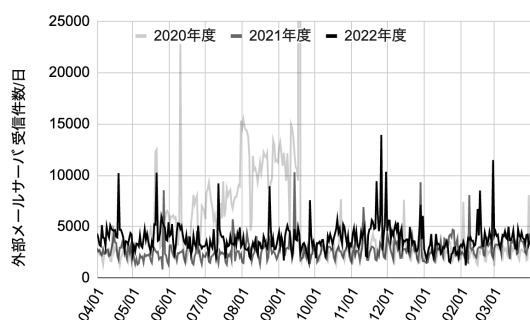


図 10 外部メールサーバ受信件数

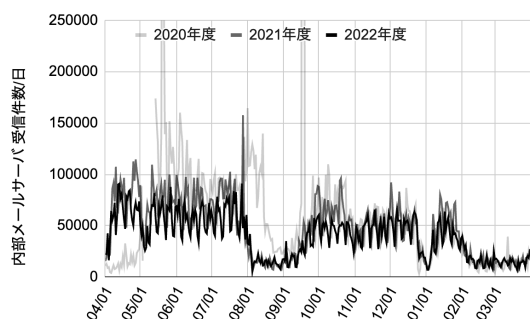


図 11 内部メールサーバ受信件数

ず、チャットや電話での取り組みになり記録が残り辛い課題を解決している。2022年度に取り組んだ主な課題は以下の通りである。

- 1) 増強箇所検討のためのエッジスイッチの通信量モニタリング
- 2) SOCK サービス廃止
- 3) Radius サーバ増強

#### 4) ドッペルゲンガードメイン対策

図 12 は、2022 年度の基幹ネットワークに関する課題チケットの件数を示している。4 月 1 日時点で 101 件のチケットが進行中であった。9 月中旬には夏季法定点検による停電を活用したシステムメンテナンスにより解決した課題が多数あった。2022 年度中に作成された課題は、126 件で、そのうち 67 件（約 53%）が 2022 年度末時点で完了している。月平均 20 件のペースで、課題が完了しつつも同じペースで新たに作成されており、進行中の課題は 100 件前後を推移している。

## 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・利用者が利用するため、求められるネットワーク像は多岐にわたる。オンライン授業を始めとする利用方法の急激な変化に対し、基幹ネットワークがその変革に対する障害にならないよう、通信速度という性能面だけでなく、利便性と安全性のバランスを今後も継続して検討していく。

## 参考文献

- [1] 丸山広, 中川幸子「2021 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.49, No.1, 2021, pp.36-41.