Vol.2020-IOT-48 No.28
2020/3/3

九州工業大学における全学セキュア・ネットワークの更新（2019年度における更新について）

中村 豊[1,a)]　佐藤 彰洋[1,b)]　福田 豊[1,c)]　和田 数字郎[2,d)]　岩崎 宣仁[2,e)]

概要：九州工業大学では2019年9月に3キャンパスのネットワークを更新した．2014年に導入した全学セキュア・ネットワーク基盤システムでは40Gbpsのネットワークシステムを導入したので，幹線ネットワークは延長することとし，セキュリティ対策，無線LAN環境の強化，ログ分析基盤等のシステムの導入を行った．セキュリティ対策では境界ファイアーウォールを異なるメーカによる2段階構成とすることで，2メーカ分の脅威情報を用いた運用が可能となった．本稿ではこれらのシステムを導入するにあたっての経緯や事前調査，準備事項などについて述べる．

キーワード：セキュリティ対策，CSIRT，BYOD

Yutaka Nakamura[1,a)]　Akihiro Satoh[1,b)]　Yutaka Fukuda[1,c)]　Sujiro Wada[2,d)]
Yoshihito Isawaki[2,e)]

Abstract: We had updated our Campus Network System in September 2019. The previous system had a high transmission performance of 40Gbps in its wired network. Therefore, we decided to remain the wired networks, with enhancing security arrangements, improved wireless networks, and introducing log analytics infrastructures. For security arrangements, we had deployed two different firewall systems at the network boundary. This paper describes the background of these systems, preliminary surveys, and preparations.

Keywords: Security arrangements, CSIRT, BYOD

1. はじめに

九州工業大学では2019年9月に3キャンパスのネットワークを更新した．2014年に導入した全学セキュア・ネットワーク [1][2] では40Gbpsの有線LAN基盤およびIEEE802.11acを用いた無線LAN基盤を導入した．40Gbpsの有線LAN基盤は帯域が十分に余裕があることから，今後5年間も十分運用に耐えると判断し，機種更新せずに延長することとした．しかしながら，喫緊の課題であるセキュリティ対策やBYODに伴う無線LAN環境の強化が求められていたため，これらの環境整備を重点的に行った．

本稿ではこれらのシステムを導入するにあたっての経緯や事前調査，準備事項などについて述べる．

2. 基盤システムの更新の背景

2014年の調達では境界ファイアーウォール，キャンパスファイアーウォール，キャンパスLANの増速化，3キャンパスの一体調達を実施した．また，一体調達を実施するための運用組織として情報基盤運用室が組織化された．2019年の調達では，2014年のシステムを継承しつつも，新たな学内からの要望に対応するためのシステムとして構築を目

[1] 九州工業大学 情報科学センター
1-1 Sensui, Tobata, Kitakyushu, Fukuoka, 804–8550, Japan
[2] 九州工業大学 飯塚キャンパス技術部
680-4 Kawazu, Iizuka, Fukuoka, 820–8502, Japan
[a)] yutaka-n@isc.kyutech.ac.jp
[b)] satoh@isc.kyutech.ac.jp
[c)] fukuda@isc.kyutech.ac.jp
[d)] swada@isc.kyutech.ac.jp
[e)] iwasaki@tech-i.kyutech.ac.jp

指した．

総合評価方式での入札となるため，仕様書の提出締切が約 1 年となる．したがって，導入から約 3 年経過した 2017 年頃から各構成要素の調達の調査を進めた．福田らの調査 [3] から無線 LAN の利用者，接続端末数の増加が著しい事，さらに無線 LAN 規格の高速化が進んでいる事が明らかとなった．また，有線 LAN 環境は 40Gbps のバックボーンで十分処理できている事，そして，境界ファイアーウォールにおいてセキュリティ対策機能が境界 FW に不足している事が運用上明らかとなった．さらに，セキュリティ対策としてインシデント対応のためのログ保存およびログ分析の重要性が増している事も課題となった．2019 年度からは大学の方針として BYOD を推進することとなったため，無線 LAN 環境の整備に重点を置く必要性が高くなった．

この様な背景を考慮して，限られた予算から以下の様な方針を策定した．

(1) 無線 LAN AP に関して，BYOD を実施する可能性の高い講義室には，高密度エリアでの高速伝送可能な無線 LAN 規格である IEEE 802.11ax[4](以下 802.11ax) を仕様に含める
(2) 無線 LAN AP を接続するスイッチは，[5] より 1Gbps を超える可能性を考慮して，IEEE 802.3bz[6] を仕様に含める
(3) アンケートを実施して，BYOD の可能性がある講義室のリストアップおよび講義室の収容人数と AP に関連したサイジングを決定する
(4) 境界 FW について，既存の 1 メーカでは十分な対策が実施できない状態であったため，2 メーカのカスケード接続を SDN スイッチを用いて実施する
(5) FW や無線 LAN 機器からのログを十分に蓄積するシステムおよび，それらの分析を迅速に実施するシステムの構築が必要である

2.1 大学の概要

九州工業大学は図 1 に示す様に，福岡県内に 3 箇所のキャンパスを有し，戸畑キャンパスに工学部，飯塚キャンパスに情報工学部，若松キャンパスに大学院生命体工学研究科を置いている．平成 30 年 5 月において学部学生が約 4100 人，大学院学生が 1500 人，非常勤事務職を含めた教職員が約 1000 名の中規模国立大学である．

SINET への接続は戸畑キャンパスから接続され，飯塚キャンパスおよび若松キャンパスには QTNet 社が提供しているダークファイバーを用いて戸畑キャンパスから接続している．また，各キャンパスには NTT フレッツ VPN ワイドを用いたバックアップ回線も準備しており，QTNet による工事に伴うファイバールート変更による通信断においても通信を維持することができる構成としている．

図 1 九州工業大学　拠点図

2.2 全学セキュア・ネットワーク基盤システム

全学セキュア・ネットワーク基盤システムは総合評価方式による入札のため，仕様策定委員会の設置から運用開始まで約 1.5 年近くの時間を必要とする．特に，仕様書の締切から導入開始まで 1 年程度の期間があるため，最新の機器を導入する際には，注意が必要である．2019 年の調達では，2018 年 1 月に仕様策定委員会を設置し，2018 年 9 月に仕様書の締切，入札締切が 2018 年 12 月，開札が 2019 年 3 月，納入期限が 2019 年 9 月といったスケジュールであった．この予定に合わせるために導入機器の選定を行う必要があるため，事前に評価期間を十分取っておかないと，機器選定が間に合わない事となる．今回の調達では，[11] で示した様に数年に渡ってセキュリティ機器の評価を実施していたため，大きな問題は発生しなかった．

2.3 事前調査と要求要件

以下の節では事前アンケートの内容とその結果およびキャンパス毎の事前調査および要求要件について述べる．

2.4 アンケート

2018 年 6 月頃にアンケートを実施した．アンケート項目としては「無線 LAN 基地局の設置場所についての要望」および「基幹ネットワークとしてサービスの要望」の 2 点を項目とした．回答として多かった内容は，講義室およびリフレッシュスペース等へのアクセスポイントの設置の要望および BYOD に対応したアクセスポイントの高速化，大容量化であった．また，情報工学部からは講義棟の改修工事が進んでいたことから，BYOD 対応も含めて無線 LAN 環境の整備を依頼された．以上を考慮して，BYOD に関係する講義室では 802.11ax 対応の AP を重点的に配置することとした．

2.5 無線 LAN 環境の強化

九州工業大学では 2018 年度から飯塚キャンパスにおいて BYOD が試行され，2019 年度からは全学で BYOD が

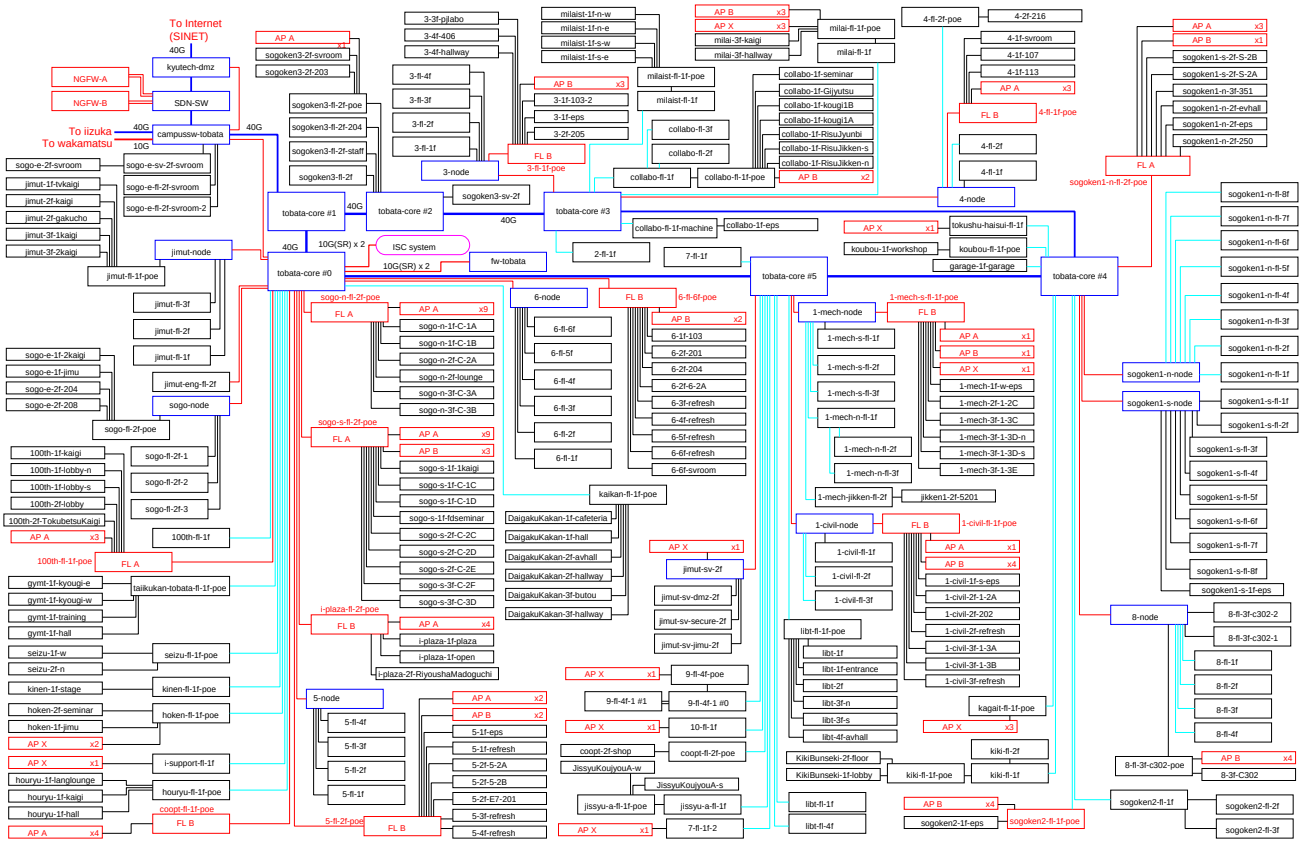

図 2　戸畑キャンパス接続構成図

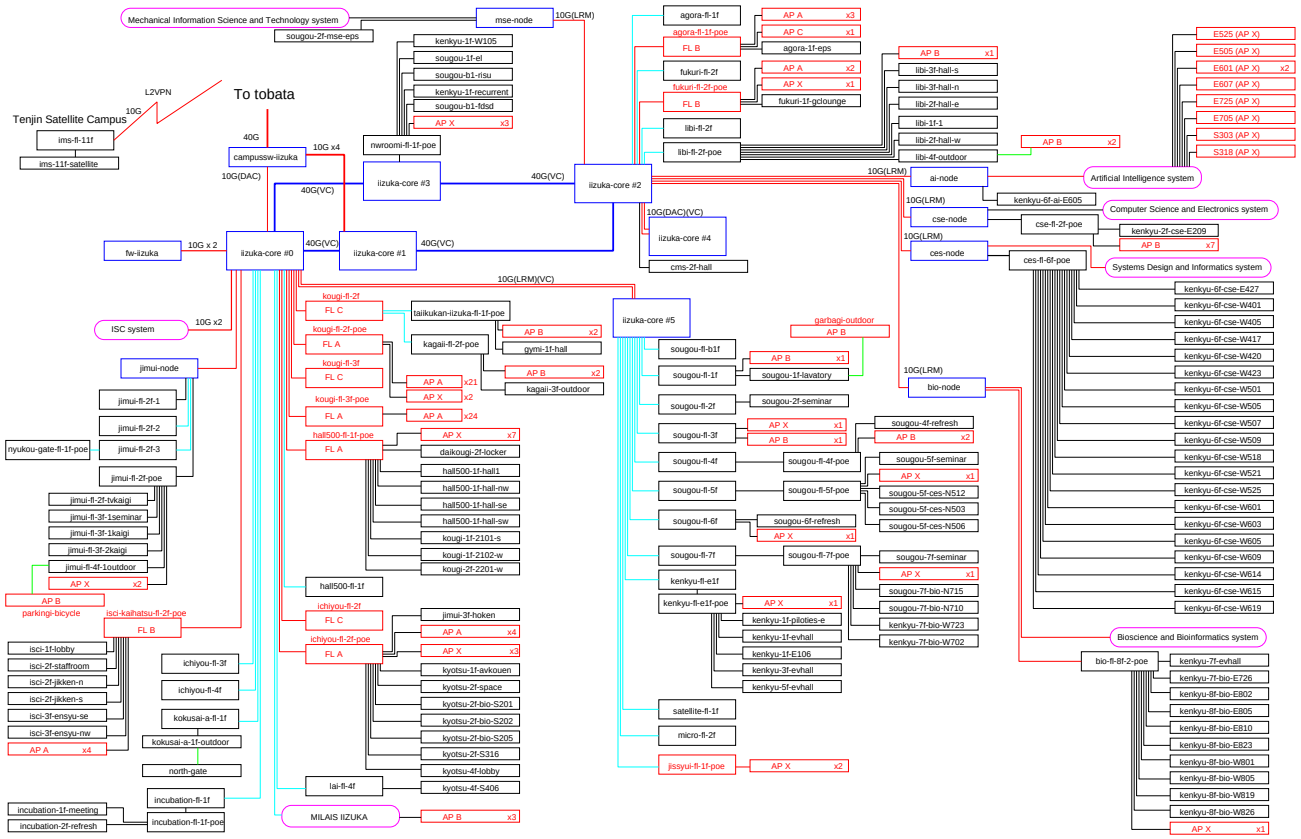

図 3　飯塚キャンパス接続構成図

開始される事が決定した．それに伴い，無線 LAN 環境の整備が課題となった．講義においてどの様な利用形態で無線 LAN 環境を用いるのか？想定される条件が明確には定義されていなかったため，可能な範囲で高スループットを実現できる様な環境の実現を目指した．

福田ら [7][8] の調査から，1 台のアクセスポイントに対して，25〜50 名程度の収容人数を想定した AP 配置を基本方針として決定した．収容人数が 100 名以上の大きな講義室では 1 台のアクセスポイントに対して 50 名のサイジングとし，収容人数が 60 名程度の講義室では 1 台あたり 30 名程度として，アクセスポイントの配置を決定した．

飯塚キャンパスでは講義棟の改修工事が行われていたことと，BYOD 環境での利用が想定されていたため，AP の設置場所およびポート収容に関して，既存の設置環境から AP の台数の増強および高スループット実現のために 802.11ax 対応の AP を設置することとした．また，それらを収容するスイッチに関しても，1，2 階の AP を 2 階のスイッチへ収容し，3，4 階の AP を 3 階のスイッチへ収容することとした．これにより各階へスイッチを設置する必要がなくなったため，スイッチの集約化を図ることができた．また，無線 LAN の高速化を図るため，AP を収容するスイッチは，これまではフロアスイッチの配下に接続されていたが，コアスイッチへ直接収容することとした．

図 2，3 に戸畑キャンパスおよび飯塚キャンパスの接続構成図を示す．コアスイッチ，フロアスイッチ，PoE スイッチおよび AP の接続構成図を示している．FL A および FL B で記述されているスイッチが 802.11ax および 802.3bz 対応のスイッチである．これらの配下に AP A(802.11ax 対応 AP) および AP B(802.11ac 対応廉価版 AP) を接続している．また，既設 AP の流用も行っている．

無線 LAN コントローラも全学セキュア・ネットワーク [1] で導入した aruba 社の 7210 コントローラを引き続き利用することとしたが，802.11ax 対応の AP をサポートするためにバージョンの更新が必要となった．また，バージョンの更新に伴い，これまで運用していた HA 構成を実現するために Mobility Master の導入が必要となった．

また，[3] より利用者が非常に多い戸畑キャンパス大学生協 1F については，新規で光ファイバー敷設工事を行った．

2.6 セキュリティ対策の強化

全学セキュア・ネットワーク基盤では境界ファイアーウォールに fortigate 社の FG-1000C を導入し，様々な次世代機能を有効にして運用してきた [9]．しかしながら，振る舞い検知機能を有していないことや，性能上限に近づいていたこともあり，更新の対象となった．また，ファイアーウォールの機能だけでは十分なセキュリティ対策を実施することが困難であることから，ファイアーウォールの出力するログを保存するためのログ分析基盤や，pcap を蓄積するためのネットワーク・フォレンジックシステム，さらに DNS セキュリティ対策ソリューションと学外公開 IP アドレスに対する脆弱性診断を実施するためのシステムも併せて更新を行った．以下ではそれぞれのシステムについて詳述する．

図 4 ネットワーク・フォレンジックシステム

2.6.1 ネットワーク・フォレンジックシステム

本学では，これまでネットワーク・フォレンジックシステムとして，学外へ通信するパケットのフルキャプチャを行う機器として，HP SL4540 を運用してきた．実行容量はおおよそ 200TB で約 3 ヶ月の pcap を蓄積することができたが，パケットロスの問題やストレージ容量のさらなる確保のため，更新することとした．更新後は DDN 社の SFA 7990 が導入された．図 4 にネットワーク・フォレンジックシステムおよび仮想基盤システムを示す．実行容量として約 700TB 確保することができたので，400TB をパケットキャプチャ用として用い，残りの容量を仮想基盤システムのゲスト OS のバックアップ用パーティションとして確保した．これまで仮想基盤システム上のゲスト OS については，esxi 上でのスナップショットしか確保していなかったため，esxi で事故が発生した際に問題となっていた．今回の更新により，キャプチャ容量の倍増と仮想基盤システムのバックアップを実現することができた．

2.6.2 ログ分析基盤

全学ログサーバとして HP DL380 gen10 を導入しているおり，物理容量 72TB のストレージを RAID6 構成で実効容量 60TB のログサーバとして運用している．このサーバ

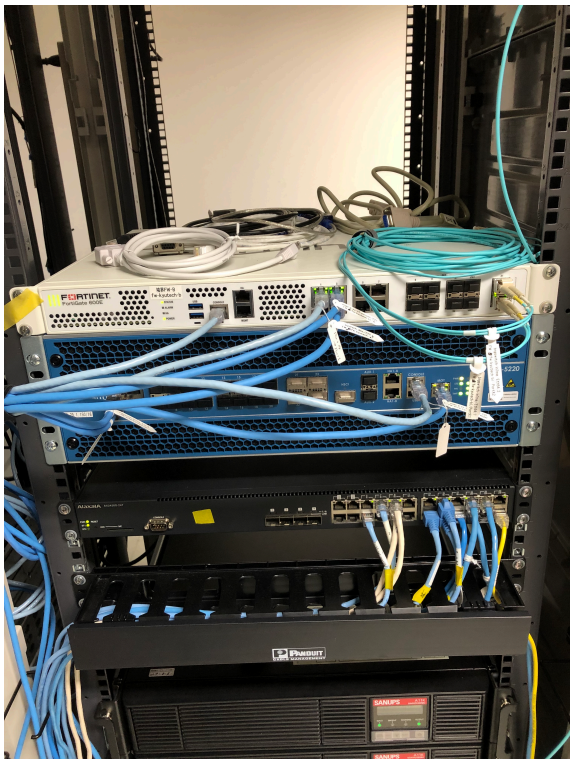

図 5 二重化された境界ファイアーウォール
図

に境界 FW，キャンパス FW，無線 LAN システム，DNS キャッシングサーバ，AD サーバ，スイッチ等のログを集約している．また必要なサーバのログは splunk forwarder を用いて外部の splunk server へデータを転送している．また，splunk サーバでは，得られたログに対して，異常通信が発生していないかのチェックスクリプトを構築し，定期的にレポートを送信している．具体的には，学内の同一 IP アドレスから 1 時間に 1000 通以上のメールが送信された場合，SPAM 送信と判断して通知される．

2.6.3 DNS セキュリティ

DNS のフルリゾルバとして，全学 DNS キャッシングサーバを BIND を用いて運用していた．これらは戸畑キャンパスに 3 台，飯塚キャンパスに 3 台設置して稼働させていた．しかしながら運用工数がかかることや，DNS におけるセキュリティ機能の要望から，infoblox 社の Trinzic 825 を導入した．これを各キャンパスに 1 台ずつ設置し，DNS キャッシングサーバ機能，および無線 LAN における DHCP サーバ機能を有効にして稼働させている．NXDOMAIN の大量のクエリを受診した場合に管理者に通知がなされるなど，セキュリティ対策の一翼を担っている．

2.6.4 境界 FW の二重化

図 5 に二重化された境界ファイアーウォールを示す．図 2 における NGFW-A が PaloAlto 社の PA-5220 であり，NGFW-B が Fortinet 社の FG-600E である．2 台を論理的にカスケード接続しており，大学の外側が FG-600E で内側が PA-5220 である．二重化することにより，2 メーカのインテリジェンスを利用することが可能となるため，異常検知の幅が広くなる．しかしながら，メンテナンス中に通信できない問題が発生するため，これを回避するために，それぞれが SDN スイッチに接続され，メンテナンス中は論理的なパスから外す運用を行っている．このため，異なるメーカであるが，それぞれが同じポリシーで運用する必要があるため，運用負荷は高くなっている．

2.6.5 脆弱性診断

本学では学外公開 IP アドレスに対して，tenable 社の nessus の web API を用いた脆弱性診断システムを運用していた [10]．しかしながら，nessus のバージョンアップに伴い，web API が利用できなくなる問題が発生した．このため，引き続き脆弱性診断システムを運用するために，nessus から tenable.io へのシステム変更を行った．アセット数の上限の問題が課題として挙げられているが，移行自体は大きな問題もなくスムーズに実施できている．

3. まとめと今後の課題

更新に伴う利点として，セキュリティ対策機能が大幅に更新されたことにより，検知や異常通信の遮断の実施が容易になったことが挙げられる．しかしながら，キャンパス有線 LAN の機器 (Juniper 社の EX シリーズ) を保守延長で運用することにしたため，販売終了品が出てしまったことや，新規で機器を購入することが難しくなった点があげられる．また，tenable.io のアセット上限に関しても問題が残っている．今後の課題として，導入されたセキュリティ機器の機能を十分に発揮させるためのチューニングを実施していく必要がある．また，出力されたログの分析の自動化や，異常検知ロジックの開発が今後の課題として挙げられる．

参考文献

[1] 中村 豊，福田 豊，佐藤 彰洋：九州工業大学における全学セキュア・ネットワークの導入について，情報処理学会技術研究報告 (インターネットと運用技術研究会)，Vol. 2015-IOT-28, No. 20, pp. 1-6, 2015.03.06.
[2] 福田 豊，中村 豊，佐藤彰洋：九州工業大学・全学セキュアネットワーク導入における無線 LAN 更新，情報処理学会技術研究報告 (インターネットと運用技術研究会)，Vol. 2015-IOT-28, No. 21, pp. 1-6, 2015.03.06.
[3] 福田 豊，中村 豊：九州工業大学・全学セキュアネットワークにおける無線 LAN 利用について，情報処理学会技術研究報告 (インターネットと運用技術研究会)，Vol. 2016-IOT-32, No. 1, pp. 1-8 (2016).
[4] IEEE Standard for Wireless Local Area Networks：入手先 ⟨http://www.ieee802.org/11/Reports/tgax_update.htm⟩
[5] 福田 豊，中村 豊，畑瀬 卓司，冨重 秀樹，林 豊洋：IEEE 802.3bz Switch を用いた無線 LAN 通信実験，インターネットと運用技術シンポジウム 2018.
[6] IEEE : IEEE Standard for Ethernet Amendment 7: Media Access Control Parameters, Physical Layers, and Management Parameters for 2.5 Gb/s and 5 Gb/s Operation, Types 2.5GBASE-T and 5GBASE-T, IEEE

802.3bz-2016 (2016).
[7] 福田 豊, 畑瀬 卓司, 冨重 秀樹, 林 豊洋 : BYOD 環境整備に向けた無線 LAN 通信実験, 情報処理学会技術研究報告 (インターネットと運用技術研究会), Vol. 2018-IOT-40, No. 10, pp. 1-6 (2018).
[8] 福田 豊, 畑瀬 卓司, 冨重 秀樹, 林 豊洋 : BYOD による講義を想定した無線 LAN 通信実験, 情報処理学会研究報告, 情報処理学会第 80 回全国大会, 2D-01 (2018).
[9] 中村 豊, 佐藤 彰洋, 福田 豊, 和田 数字郎：九州工業大学における情報セキュリティ対策の取り組みについてインターネットと運用技術シンポジウム 2017.
[10] 佐藤 彰洋, 中村 豊, 福田 豊, 和田 数字郎：九州工業大学 学外公開 IP 申請システム, 九州工業大学 情報科学センター広報 第 30 号 2018.3.
[11] 中村 豊, 佐藤 彰洋, 福田 豊, 和田 数字郎：ネットワークセキュリティ機器の評価に関する考察, インターネットと運用技術シンポジウム 2019.