名古屋大学における近年の無線ネットワーク環境の整備とセキュリティ対策の強化について

○川瀬友貴、石原正也、岩瀬雄祐、川田良文

情報通信技術支援室　情報基盤技術グループ

概要

名古屋大学では、学生に向けた快適な学習環境の提供や、業務における利便性の向上を目的として、構成員向けの無線 LAN サービス（NUWNET）を提供している。NUWNET は、約 2,000 台のアクセスポイントのほか、それらを機能させるためのネットワークスイッチやアクセスコントローラといった機器に支えられ、名古屋大学キャンパスネットワーク（NICE、Nagoya university Integrated Communication Environment）の一部を構成している。近年の ICT 利活用推進を受けてこれら無線 LAN 設備の重要性がますます高まる中、本学においても利用可能箇所の拡大や通信速度の改善を目指して毎年増強を進め、2020 年においては、キャンパス内すべての会議室・講義室へのアクセスポイント設置を達成するとともに、NUWNET 用の UTM（統合脅威管理）装置を導入した。本発表では、このような近年における無線 LAN 設備の設置状況及びそのセキュリティ対策について述べるとともに、更新作業に際し生じたトラブル等についても紹介する。

1　はじめに

無線 LAN 規格である IEEE 802.11 が策定されたのは、1997 年のことである [1][2]。それを契機に、各社から法人又は個人向けのアクセスポイント（以下「AP」という）の販売が開始されたが、当初は IEEE 802.11 に準拠していても製品間での相互接続が保証されていない状況であった。しかしながら、相互接続の保証を行う Wi-Fi Alliance が 1999 年に現れる [3]と、ユーザが AP を導入する際の障壁が緩和された。

名古屋大学でも、これに伴い独自に AP を導入する研究室が現れ始めたが、セキュリティ上の問題が懸念されることや、導入した研究室しか利用できないことを踏まえ、2002 年に学内向け無線 LAN サービス（NUWNET）の実証実験を開始した [4]。当初は NUWNET を利用するためにはクライアント側に特定のソフトウェアが必要であり、加えて、利用者 ID の登録も必要であったが、2002 年末にはブラウザを通じて認証を行えるようにし、2004 年に利用者 ID として全学 ID（現：名古屋大学 ID）を利用できるようにした [5]。2008 年の本運用移行を経た 2011 年には IEEE802.1X 規格による認証を可能としたため、利用者は現在と同様、NUWNET を表す ESSID（Extended Service Set Identifier、無線ネットワークの識別名）を選択し、名古屋大学 ID とそのパスワードを入力すればインターネットに接続することが可能となった [6]。

NUWNET の AP 台数は当初 5 棟 10 台程度のスモールスタートであったが，台数増加によるカバレッジ向上を目指して年々増設を重ね、2011 年には 3 キャンパスで 1,000 台を超えるまでとなった。2017 年からは、5GHz 帯での良好な通信を実現する Wi-Fi 5 対応 AP の導入を開始し、2019 年から 2020 年にかけては、講義や研究において学生が積極的に ICT を活用できる環境の提供を目標に、キャンパス内の全講義室への AP 設置に加え、関連するネットワーク機器の置き換えや UTM 装置の導入等、大規模な改善を実施した。

本発表では、NUWNET を構成する機器や近年における NUNWET の整備状況及び利用状況のほか、UTM 導入や機器更新に伴うトラブルについて紹介する。

2　NUWNET を構成する機器

NUWNET を構成する代表的な機器は、パソコンやスマートフォン等の無線クライアントとデータの送受信を行う AP である。これは，多くの場合図 1 のように天井や壁面に設置されており，名古屋大学では一部（後述）を除き、自律型と呼ばれる他の AP とは連携しないモードで動作している。さて、この AP のバックグラウンドには図 2 に示すような多種多様なネットワーク機器が存在しており、これらが NUWNET を構成すると共に、無線クライアントによる学外との通信を成り立たせている。

図 1．AP の例

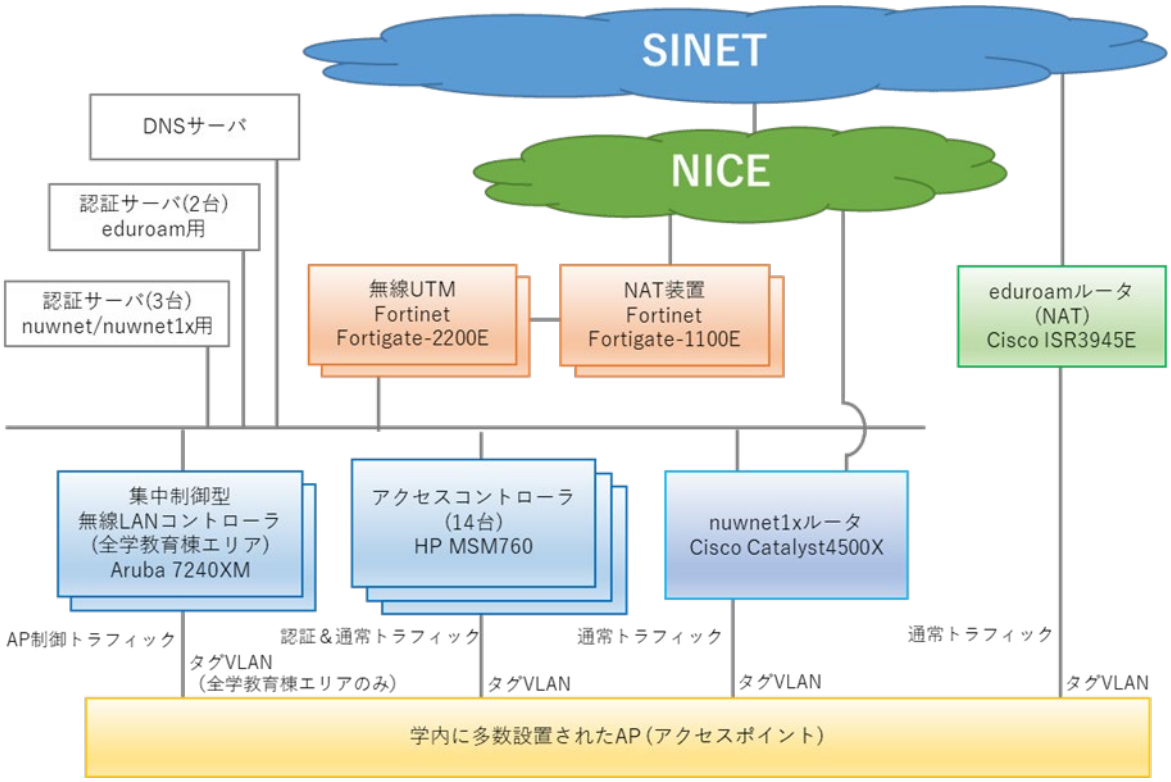

図 2．NUWNET を構成する機器群

利用者が NUWNET を使おうとした場合，まずは認証を行う必要があるが，これは WEB 認証と IEEE802.1X 認証の場合で通信経路が異なる。WEB 認証の場合はアクセスコントローラが認証画面を表示するとともに、認証サーバ（RADIUS サーバ）に対し RADIUS クライアントとなって認証情報を問い合わせるが、IEEE802.1X 認証の場合は，AP 自身が RADIUS クライアントとなって認証サーバに認証情報を問い合わせる。認証が完

了した後の通常トラフィックは、WEB 認証の場合はアクセスコントローラ経由で、IEEE802.1X 認証の場合は nuwnet1x ルータ経由で無線 UTM へと向かう。無線 UTM は、NUWNET 独自のセキュリティポリシーの下、NICE と NUWNET との間でリスクのある通信が流れることを防いでおり、NUWNET はこれを介して NAT 装置に接続されている。NAT 装置は NICE と NUWNET の接続点に置かれている機器で、NICE のグローバル IP アドレスと NUWNET のプライベート IP アドレスの変換を担っている。

また、全学教育棟及び全学教育棟 A 棟に設置された AP については、集中制御型というモードで動作させているため、これらの AP を一元管理し、最適な電波環境に調整するために、専用の無線 LAN コントローラが LAN 内に置かれている。集中制御型の AP を経由した IEEE802.1X 認証については、RADIUS クライアントの役割もこの無線 LAN コントローラが担う。

このほか、NUWNET 内部での名前解決を行うために、DNS サーバが設置されている。

3　近年における NUWNET の整備状況

3.1　AP の整備状況

運用開始以来、キャンパス内のどの建物においても NUWNET が使える環境の提供を目指し、AP の増設を続けてきた（図 3）。その結果、2010 年度に 933 台だった AP は 2020 年度末には 1,957 台と、約 2 倍になるまでとなった（病院系 AP との統合があり、NUWNET の AP としては減少した年度もある）。特に、2019 年度においては、学生の ICT 活用推進を目的に、ほぼすべての講義室に AP を設置し、加えて、教職員が利用する会議室にも大規模な設置を実施したため、大幅に AP の台数が増加している。

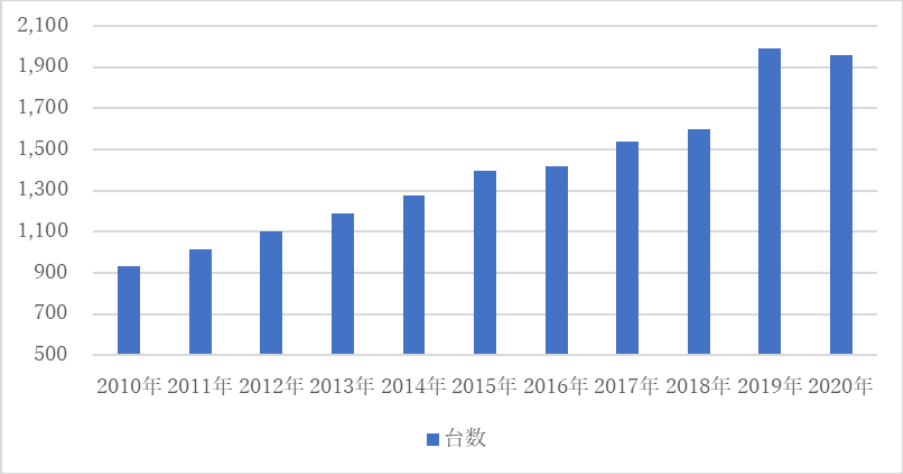

図 3. AP 設置台数の推移（全体数）

表 1. AP 設置台数の推移（規格別の詳細、各年度末の台数）

年度	2016	2017	2018	2019	2020
Wi-Fi3	454	366	363	140	17
Wi-Fi4	951	858	850	616	278
Wi-Fi5	14	313	382	1047	1.195
Wi-Fi6	-	-	-	188	467
合計	1,419	1,537	1,595	1,991	1,957

通信規格別で見ると、2016 年末の時点では IEEE 802.11g 対応の AP（便宜上「Wi-Fi 3」という）が 454 台，IEEE 802.11n（Wi-Fi 4）の AP が 951 台あったが、2020 年度末にはそれぞれ 17 台、278 台にまで減少している。この世代，特に、Wi-Fi 3 の AP は規格上 54Mbps での通信が可能であるが、実際は数 Mbps 程度でしか通信ができないことが多く、各種コンテンツの大容量化に伴い、苦情が出るようになっていた。

これらを置き換える形で導入を開始したのが IEEE 802.11ac 対応（Wi-Fi 5）の AP であり，2016 年度にはわずか 14 台しかなかったものの，、2020 年度末には 1,195 台にまで増えている。この世代は、数 100Mbps の通信速度を容易に実現することが可能である。2019 年度からはさらに高速で，複数のクライアントへ同時に情報を送ることが可能な IEEE 802.11ax 対応（Wi-Fi 6）の AP の導入も開始した。

3.2　ネットワークスイッチの整備状況

AP を新しいものに交換しても、通信経路上の LAN ケーブルやネットワークスイッチ（以下単に「スイッチ」という）の対応可能なデータ転送速度が遅いものであった場合、AP は十分に性能を発揮することができない。具体的には、本学で導入していた Wi-Fi 4 以降の AP はアップリンクとして 1Gbps の通信が可能であったが、それらの繋がれたエッジスイッチの中には、ダウンリンクとして 100Mbps のポートしか持たないものがあり、機能が制限されている状態であった。そこで、2017 年 10 月には、そのような古いスイッチ（Cisco 社製 Catalyst2960 シリーズ）計 38 台について、1Gbps に対応したスイッチ（Cisco 社製 Catalyst2960L シリーズ及び Catalyst2960X シリーズ）に置き換えを実施した。併せて、速度的には問題のないスイッチ 4 台についても、AP に対し電力供給が可能な PoE スイッチと呼ばれる機器に更新を行った。PoE スイッチでない場合は、図 4 のとおりスイッチと AP の間に PoE インジェクタという電源供給専用の機器を挟む必要があり、電源コンセントの確保やケーブルの取り回し等の手間が発生するが、PoE スイッチを用いた場合は、図 5 のとおり PoE スイッチが直接 LAN ケーブルを通じて AP に電力を供給するため、電力供給を制御することで AP を遠隔で再起動できるほか、PoE インジェクタのスペースを省くこともでき、管理面で有利である。ただし、PoE スイッチで供給できる電力量には上限があることには注意が必要である。

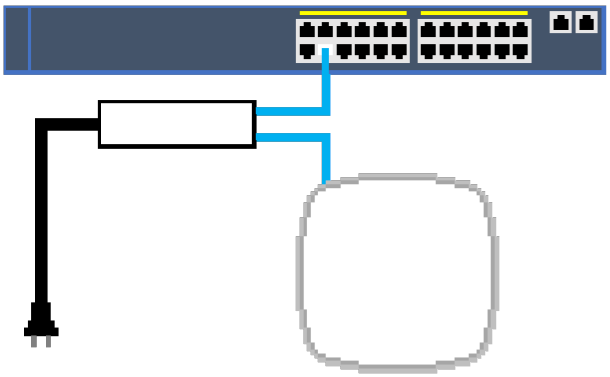

図 4. 通常のスイッチの場合

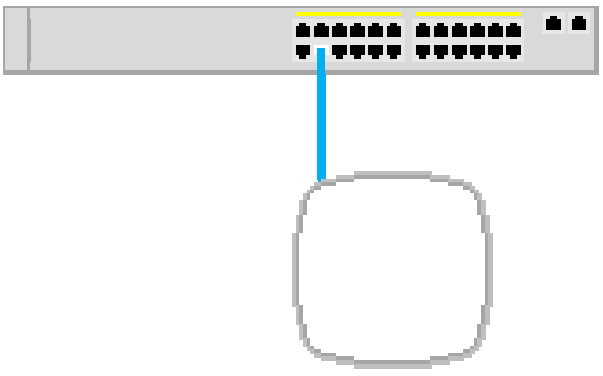

図 5. PoE スイッチの場合

2019 年 2 月においても、講義室への AP 増設に合わせて大々的なスイッチの更新・増設を行い、それに伴い、まだ残っていた古いスイッチ 68 台を新しいもの（うち 6 台は PoE スイッチ）に交換するとともに、18 台の PoE スイッチを、AP の収容先として新たに増設した。

4　UTM 導入について

日々高度化するサイバー攻撃に対するセキュリティ強化を目的として、2020 年 4 月には、UTM（Unified Threat Management）装置（Fortnet 社製 FortiGate 2200E）の運用を開始した [7]。UTM 装置は、悪性と判断された通信や IP アドレスの遮断などの様々な脅威に対応することが可能なセキュリティ機器であり、ネットワークの最外殻に置かれることが多い。本学の場合、図 6 に示したとおり、NICE 全体を守るための UTM 装置のほかに、NUWNET 専用の UTM 装置を設置している。ただしこれは、UTM 装置が物理的に 2 台あるわけではなく、仮想化機能を用いて 1 台の上で複数の（仮想）UTM 装置を動かしている状態である。UTM 装置の導入によって、従来の全学ファイアウォール（Fortnet 社製 FortiGate 1000C）と同様なパケットフィルタリングに加え、Web フィルタ（危険なサイトを開かない機能）、アプリケーションコントロール（組織の定めた基準でアプリケーションの利用を制御する機能）、侵入防止（IPS）及び SSL インスペクション（暗号通信のチェック）等が可能となった。

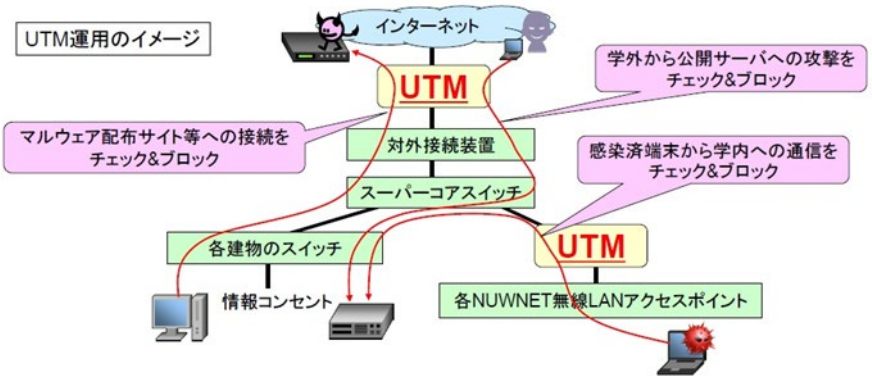

図 6.　UTM 運用イメージ

当初、UTM 装置を設置したのは 2019 年 11 月であったが、CPU が過負荷となり、（対外通信プロトコルの）BGP セッションが切れて対外通信が遮断される不具合が発生した。2020 年 4 月の本運用開始時点でも原因の特定には至らず、調査のための設定変更が夜間において繰り返された。本学情報連携推進本部が持つ公式サイトに残された大量の全学ファイアウォール・メンテナンス情報はその名残である（図 7）。本学のデータ通信量に対し UTM 装置の性能が不足していることも疑われたため、UTM 装置のスペックアップも実施したが問題の解決には至らず、BGP をスタティック設定にしても解決はしなかった。加えて、納入業者内の再現環境では発生しないという原因特定に厳しい状況でもあった。それでもログ管理システムやパケットキャプシステムを導入し、現象を監視し続ける中で、nTurbo 機能（FortiASIC にてフローベースのセキュリティポリシーを処理することで、CPU 負荷を下げる機能）[8]を無効化することで不具合が収束することが判明（不具合の原因は調査中、導入した FortiGate の CPU 性能が良く nTurbo を止めても処理性能の問題は生じず）、本問題の存在により有効化できていなかった全ポリシーを 2020 年 9 月に有効化して、UTM 装置導入が完了した。

図 7. 大量の全学ファイアウォールのメンテナンス情報

5 NUWNET の利用状況について

NUWNET の利用状況（ユニークユーザ数）を図 8 に示す。山と谷が繰り返されているのは、例年、講義期間の 4 月～7 月、10 月～翌年 1 月にユーザ数が増えるためである。2017 年度以前と 2018 年度以降を比べると明確にユーザ数が増加しており、NUWNET のインフラとしての重要性が増していることが分かる。しかしながら、2020 年度はコロナ禍によって遠隔講義が増えたため、ユーザ数が大幅に減少した。ただし、2020 年 4 月～5 月、および 2021 年 1 月以降の緊急事態宣言による減少が見られるものの、大学での講義が再開された 10 月以降にはユーザ数の増加しており、NUWNET が活用されていることが確認できる。2019 年度の AP 増強の効果については継続して見ていく必要があるが、ICT を活用した学生の学習や、教職員による効率的な業務遂行に貢献しているものと期待したい。

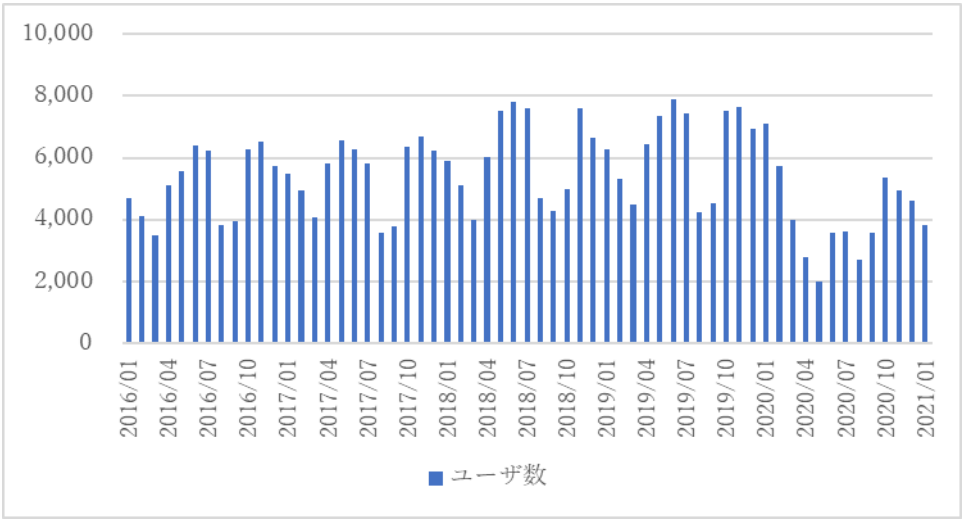

図 8. 1 日あたりのユニークユーザ数（2016 年 1 月～2021 年 1 月）

6　機器更新に伴うトラブルについて

機器更新の現場においては、往々にして予期しないトラブルが生じる。これは、ネットワーク機器が様々な機器と連携して動作しているという論理的事情に加え、それらのネットワーク機器が様々な場所に設置されているという物理的事情が挙げられる。また、大学においては、学生から教職員まで多数のユーザが存在し、あらゆるネットワーク端末を用いていることも、時に原因となる。UTM 装置交換に伴うトラブルについては、すでに述べたとおりであるが、ここではその他のトラブルの一部について、紹介したい。

6.1　AP が制限モードでの動作になる

ここでいう制限モードというのは、アップリンクの通信速度が 1Gbps よりも低い速度で動作している状態のことである。AP を新しいものに取り換え、スイッチ側も 1Gbps に対応しているにも拘わらず、制限モードになってしまう場合があった。この場合の原因は、主に 2 つである。1 つは、間に存在する PoE インジェクタが古く、1Gbps に対応していないものであるケース、もう 1 つは LAN ケーブルがカテゴリ 5 であり、同じく 1Gbps に対応できていないケースである。前者の場合は PoE インジェクタを交換することで即対応が可能であるが、後者の場合、配線工事を実施する必要があるため、経費の問題も含め、すぐには対応することが困難な事案となる。

6.2　PoE スイッチが AP にうまく電力を供給できない

既設の PoE スイッチに、新たに AP を接続すると、最大供給電力量をはるかに下回っているにも拘わらず、電力が供給されないという事態が複数個所において起こった。原因は不明であったが、試行錯誤の結果、図 9 のとおり、接続されているポートの位置を分散させると電力供給が行われる場合があることがわかった。しかし、これを実施しても電力供給されない場合もあり、そういった場合はやむなく PoE インジェクタを併用することで対応した。

図 9．PoE スイッチの電力供給の問題を接続の工夫によって解決した事案

6.3 ESSID が見つからない

NUWNET の AP がある場所においては、「nuwnet」といった ESSID（ネットワークの識別名）がクライアント側に表示されるようになっている。しかし、2019 年度に更新した一部の AP において、クライアント側にこの ESSID が表示されないという事態が生じた。これについては、AP が新しくなったために、クライアント側の無線 LAN 用ドライバでは対応できなくなったことが原因であり、クライアントのドライバを最新のものにすることによって解決した。

6.4 AP に一切接続できない

全学教育棟及び全学教育棟 A に導入した集中制御型の AP において、当初 ESSID が見えており、認証画面も開かれるにも拘わらず、まったくと言ってよいほど認証が通らないという現象が起きた。AP のランプは正常に動作していることを示しており、またごく稀に認証が通ることもあることからこれは非常に不思議な事態であったが、調査の結果、原因は集中制御型 AP 用に新たに導入した無線 LAN コントローラにあることが判明した。この無線 LAN コントローラは、認証に失敗した場合、10 分間は再認証させないという設定になっており、この所為で認証がしにくくなっていたが、この時間を 0 分にすることで、正常に認証が可能となった。

7 おわりに

本学における AP の設置台数は、2020 年度末には 2,000 台に迫るまでとなった。単純に数だけを見れば、多くの方は膨大な数と感じることと思うが、様々な建物が立ち並ぶ大学にあっては、まだまだフロアにおいて電波状況の悪い場所が残っている状況であり、更なる AP の増設が望まれる。

しかしながら、情報技術を取り巻く環境は日々変化しており、ただ単純に AP を増やすだけではなく、ときには例えばローカル 5G といった新技術も取り込むことも視野に、学生がより一層情報にアクセスしやすく、教職員がより一層効率的に業務を成せる環境を提供していければ良いと考える。

参考文献

[1] 三輪 賢一、”プロのための[図解]ネットワーク機器入門、技術評論社、2015 年

[2] 竹下 隆史、村山 公保、荒井 透、苅田 幸雄、”マスタリング TCP/IP 入門編 第 4 版”、 2010 年

[3] Wi-Fi Alliance、History、https://www.wi-fi.org/who-we-are/history(2021/2/26)

[4] 河口 信夫、“名古屋大学無線ネットワーク実証実験”、名古屋大学情報連携基盤センターニュース、Vol. 2、No. 2、2003 年

[5] 河口 信夫、“名古屋大学における無線ＬＡＮの利用について”、名古屋大学情報連携基盤センターニュース、Vol. 5、No. 1、2006 年

[6] 石原 正也、“名古屋大学無線ネットワーク(NUWNET)の導入について”、平成 22 年度 第 6 回名古屋大学技術研修会、pp. OJOU-3、2010 年

[7] 情報連携推進本部、UTM 設置によるサイバーセキュリティ対策の強化、http://www.icts.nagoya-u.ac.jp/nu-only/ja/services/nice/utm.html (2021/2/17)

[8] Fortnet 社、”NTurbo offloads flow-based processing、“ https://docs.fortinet.com/document/fortigate/6.0.0/hardware-acceleration/896174/nturbo-offloads-flow-based-processing (2021/2/23)