

名古屋大学無線ネットワークにおける新 Web 認証システム導入と ゲスト専用ネットワークの展開について

○石原正也^{A)}、岩瀬雄祐^{A)}、川瀬友貴^{A)}、川田良文^{A)}

^{A)} 情報通信技術支援室 情報基盤技術グループ

概要

名古屋大学では名古屋大学構成員およびゲストユーザ向けの全学的な無線 LAN サービスとして名古屋大学無線ネットワーク（NUWNET）を提供している。2002年に学内向け無線 LAN サービスの実証実験として開始した NUWNET は、2008年の正式運用サービス開始、およびその後のサービス更新を経て、ウェブブラウザを通じての認証（Web 認証）と IEEE802.1X 規格による認証（802.1X 認証）を提供するようになった。NUWNET は、Web 認証では名古屋大学 ID とゲスト ID（名古屋大学構成員が発行可能なゲスト用 ID）を、802.1X 認証では名古屋大学 ID をログイン ID として使用しているが、導入から 10 年以上経過した Web 認証システムの老朽化対応に加え、ゲストユーザによる学内情報資源へのアクセス制限および 802.1X 認証対応の要望があった。本発表では、キャンパスネットワークの維持管理の一環として行った新 Web 認証システム導入やゲスト専用ネットワークの展開を含めた NUWNET のサービス更新について報告する。

1 はじめに

名古屋大学では、大学の教育・研究および大学運営を支える全学的なキャンパス情報ネットワークとして名古屋大学キャンパス情報ネットワーク（NICE）があり、その一部として無線 LAN サービスである名古屋大学無線ネットワーク（NUWNET）を提供している。各キャンパスの主要な建物に NUWNET の無線 LAN アクセスポイント（AP）が設置されており、大学内の会議室や講義室をはじめ、食堂等学内の多くの場所でインターネットアクセスが可能となっている。

NUWNET は 2002 年に学内向け無線 LAN サービスの実証実験として開始され、当初利用時にはクライアント側に特定のソフトウェアおよびシステム独自のログイン ID が必要であったが、後にウェブブラウザを通じての認証（Web 認証）に加え、ログイン 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。2008 年に正式運用サービスとして開始した後、2011 年にはサービス更新を行い、名古屋大学 ID（名大 ID）とは別のゲスト ID（名古屋大学構成員が発行可能な期間限定のゲストユーザ用 ID）をログイン ID に追加した。さらに、新たな認証方式として IEEE802.1X 規格による認証（802.1X 認証）を提供するようになった。

また、NUWNET は AP の他、認証サーバ（Radius サーバ）、NAT 装置、ルータおよびこれらの機器を収容するネットワークスイッチで構成されている。2011 年度以降、AP および認証サーバの増強・更新を行ってきたが、2019 年度には AP の増強・更新の他に、無線 LAN アクセスコントローラ導入による一部 AP の集中制御化、統合脅威管理（UTM）導入による情報セキュリティ強化を図った（図 1）。さらに 2020 年度にはコロナ禍の影響により講義のオンライン化が必須となったため、オンライン講義の受講環境の向上を目的とした整備として、数世代前の古い規格の AP の更新を行った[1]。しかしながら、Web 認証では名大 ID とゲスト ID を、802.1X 認証では名大 ID をログイン ID として使用しているが、導入から 10 年以上経過した Web 認証

システムの老朽化対応に加え、ゲストユーザによる学内情報資源へのアクセス制限および802.1X認証対応の要望があった。

本発表では、新Web認証システム導入やゲスト専用ネットワークの展開を含めたNUWNETのサービス更新について報告する。

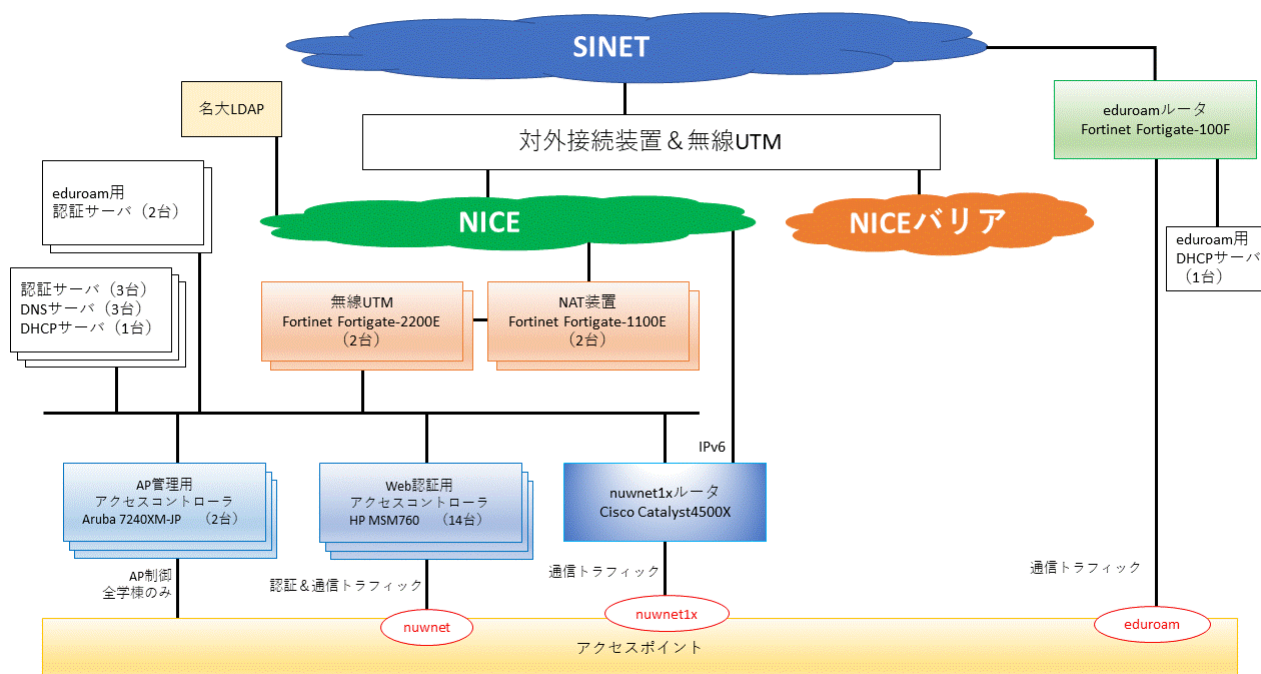


図 1. サービス更新前の NUWNET 概要図

2 新 Web 認証システムの構築

2.1 新旧システムの比較

旧 Web 認証システム（アクセスコントローラ、HP MSM760）は2010年3月に導入されたもので、文系地区や理系地区などエリアごとに分散配置され、各コントローラは1Gbpsで上流のネットワークと接続されていた[2]。導入から10年以上が経過し、老朽化したハードウェアの故障によるサービス停止が発生するとともに、対応するTLS（Transport Layer Security）のバージョンが古いことで、新しいウェブブラウザによってはWeb認証画面をセキュリティに問題があるサイトと判断されてログインできなくなるといった問題があった。



図 2. Web 認証画面（名大 ID, ゲスト ID）

新 Web 認証システムは、FreeBSD をベースにしてファイアウォールとルータ機能を提供する pfSense [3] を用いて仮想マシンとして構築し、情報基盤センターにある仮想基盤サーバ上に各エリアのコントローラを集約して、上流と下流のネットワークを合わせて 10Gbps×2 で接続した。コントローラを仮想化することによってリソースの調整や障害時の対応が容易となり、TLS のバージョンが上がったことで新しいウェブブラウザで Web 認証が利用可能となった。ただし、新システムではログイン ID の種類によって通信設定を変えることができないため、名大 ID とゲスト ID で専用コントローラを準備し、ログイン ID の誤入力を防ぐためにゲスト ID の Web 認証画面のデザインを変更した（図 2）。

2.2 新システムの構築とテスト

新 Web 認証システムは、旧システムと同じエリアを分担する名大 ID 用コントローラ（nwcp-XX、開発・テスト用を含む）15 台、ゲスト ID 用コントローラ（nwcp-g）1 台、仮想基盤サーバ（nwcp-srv1X、VMware ESXi, Dell PowerEdge R440）2 台によって構成される（図 3）。各コントローラは上流（NICE、もしくは NICE バリア（学外相当）への接続）と下流（PC、スマートフォン、タブレットなどが接続）ネットワークへ接続する 2 つのネットワークインタフェースをもち（nwcp-g は管理用にもう 1 つインタフェースをもつ）、下流ネットワークからの通信要求に対して、Captive Portal 機能による Web 認証、上流ネットワークへのアクセスを提供する。

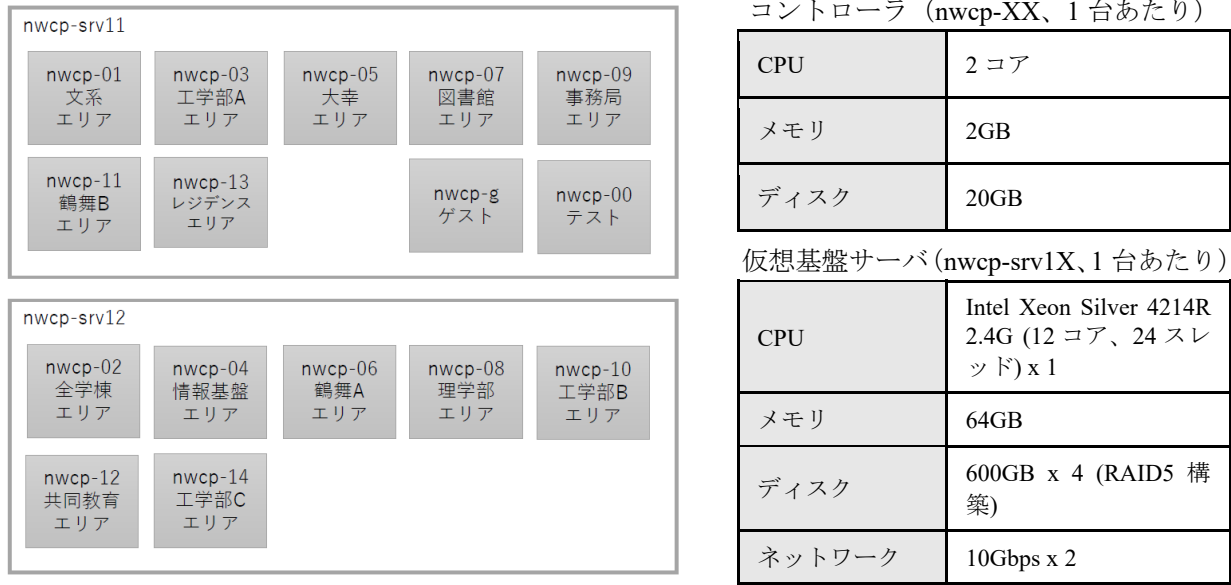


図 3. 新 Web 認証システムのシステム構成

多ユーザの同時接続に耐えられるかどうか確認するため、新コントローラの負荷テストを行った。Web 認証システムではウェブブラウザによる認証作業が必要となるため、ウェブブラウザの作業を自動化できる Selenium [4]を用い、別の仮想基盤サーバ上にサーバ・クライアント型の負荷テストのシステム（仮想マシンにて Selenium サーバ 1 台、Selenium クライアント 55 台、ファイルダウンロード用のウェブサーバ 1 台）を構築した。同時ログインとファイルダウンロードを検証し、新コントローラ 1 台あたり、50 ユーザの同時ログイン、2.5Gbps 程度の通信を処理できることを確認した。

2.3 本番運用

2021年4月に附属学校において、コロナ禍によってタブレット端末が導入されたが、新しいブラウザでゲストIDによるWeb認証が必要となったため、新Web認証システムを先行導入した。附属学校の先行導入によって、新システムの正常動作を確認できた一方、名大IDとゲストIDを誤入力する事例があったため、ゲストIDのWeb認証画面のデザインを変更することになった。その後、2021年9月に新Web認証システムを全学展開した。情報コンセントをNICEから有線NUWNETへ切り替えた文学部を含む文系エリア等の通信障害を恐れていたが、全学の通信においてリソースが逼迫することなく安定運用ができた。

3 ゲストユーザ専用サービスおよびネットワークの構築

3.1 ゲスト専用サービスの検討

従来のNUWNETにおいてゲストIDはWeb認証のみ利用可能としていたが、以前からゲストIDにおいても802.1X認証による利用の要望があった。今までゲストIDをWeb認証限定にしていたのには理由があり、「制限ありゲストID」「制限なしゲストID」の2種類のゲストIDが存在し、通常は制限ありゲストIDであり、「ウェブ」「メール」「SSH」等の一部のサービスのみ利用可能であった。なお、制限なしゲストIDは特別な申請により利用サービス制限を外したものであった。NUWNETシステムのデータベースの中にユーザテーブルがあり、ユーザIDとともに「名大ID」「制限ありゲストID」「制限なしゲストID」といったユーザ種別情報を保存している。旧Web認証システムでは、Radiusから得られたユーザ種別情報を基に、それぞれに適用するアクセスコントロールリスト（ACL）を選択することができたが、802.1X認証システムではユーザ種別情報を基に適用するACLを選択することが難しいため、ゲストIDでの802.1X認証による利用を提供していなかった。また、同様に新Web認証システムにおいてもユーザ種別情報を基に適用するACLを選択することが難しい。

そこで新システムでは2種類のゲストIDの統一とともにサービス制限を廃止し、全てのACLを統一することにした。それに加え、ゲストID用コントローラの構築とともにゲスト専用サービス用のNAT装置を新たに導入した。

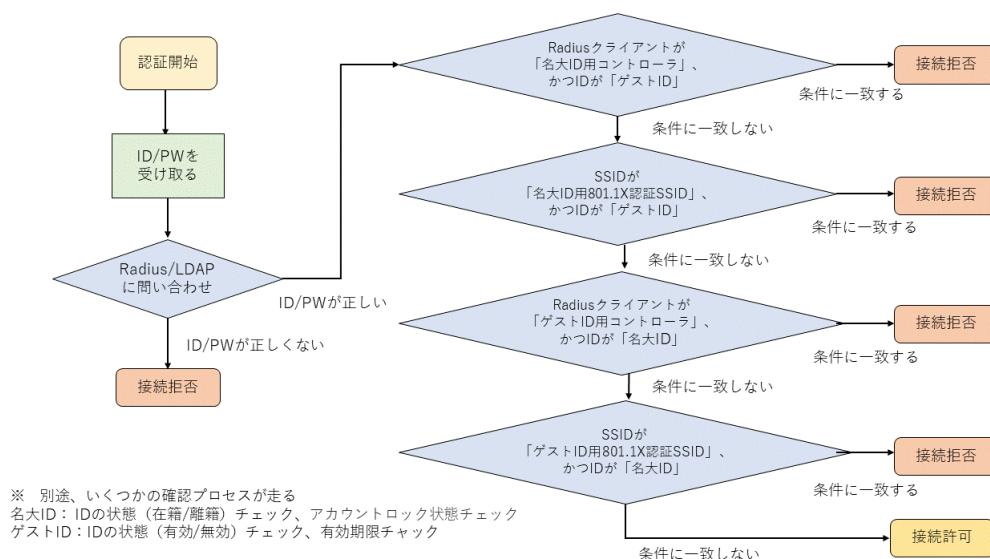


図 4. NUWNET における認証シーケンス概要

図 5. サービス更新後の NUWNET 概念図

4 新 Web 認証システムとゲスト専用サービスの全学への展開

4.1 SSID の整理

名古屋大学で導入している大多数の AP は 2.4GHz/5GHz のそれぞれ 16 個の SSID を設定することができるが、新 Web 認証システムとゲスト専用サービスおよびネットワークの導入の際に、SSID 数が増え過ぎて煩雑にならないようにするため、以下の基本方針を立て、SSID の整理と付け替えを行った[5][6]。

- 新 Web 認証 SSID は名大 ID 用とゲスト ID 用とともに 2.4GHz 帯/5GHz 帯で共通の SSID とする
- ゲスト ID 用 802.1X 認証 SSID は 2.4GHz 帯/5GHz 帯で共通の SSID とする
- 新 Web 認証システム側が煩雑になるため、鶴舞プライベートネットワークへ接続する Web 認証サービスの提供を終了
- 一部の部局で提供していた“nuwnet”に部屋番号等の識別子を付けた SSID（“nuwnet-101”等）の廃止

サービス更新前後の SSID 一覧を以下に記す（表 1、表 2）。

表 1. サービス更新前の SSID 一覧

SSID	周波数帯	認証方式	利用可能 ID	
			名大 ID	ゲスト ID
nuwnet	2.4GHz	Web 認証	○	○
nuwnet (5GHz)	5GHz	Web 認証	○	○
nuwnet1x	2.4GHz	802.1X 認証	○	-
nuwnet1x (5GHz)	5GHz	802.1X 認証	○	-
eduroam	2.4GHz/5GHz	802.1X 認証	○	-
nuwnet-med	2.4GHz	Web 認証	○	○
nuwnet-med (5GHz)	5GHz	Web 認証	○	○
nuwnet1x-med	2.4GHz	802.1X 認証	○	-
nuwnet1x-med (5GHz)	5GHz	802.1X 認証	○	-

※ "eduroam"のアカウントは「名大 ID@nagoya-u.ac.jp」

※ "nuwnet-med", "nuwnet-med (5GHz)", "nuwnet1x-med", "nuwnet1x-med (5GHz)"は鶴舞キャンパス限定

表 2. サービス更新後の SSID 一覧

SSID	周波数帯	認証方式	利用可能 ID	
			名大 ID	ゲスト ID
nuwnet	2.4GHz/5GHz	Web 認証	○	-
nuwnet1x	2.4GHz	802.1X 認証	○	-
nuwnet1x (5GHz)	5GHz	802.1X 認証	○	-
nuwnet-guest	2.4GHz/5GHz	Web 認証	-	○
nuwnet1x-guest	2.4GHz/5GHz	802.1X 認証	-	○
eduroam	2.4GHz/5GHz	802.1X 認証	○	-
nuwnet1x-med	2.4GHz	802.1X 認証	○	-
nuwnet1x-med (5GHz)	5GHz	802.1X 認証	○	-

4.2 APおよび有線 NUWNET コンセントへの展開

NUWNET で使用している AP は 4 メーカーで合計 2000 台近くあり、そのうち 1700 台以上を自律型 AP、200 台以上を制御型 AP として動かしている。AP への展開について、制御型 AP の場合、無線 LAN アクセスコントローラもしくは仮想コントローラの WebUI 経由で管理下の AP 設定を一括で変更することができるが、自律型 AP では 1 台 1 台に対し設定を投入する必要がある。そのため、各メーカーや機種にあわせて設定変更スクリプトを作成した。また、AP 以外にも「有線 NUWNET」と呼ばれている情報コンセントの設定を変更する必要があった。有線 NUWNET は情報コンセントに端末を接続した際に Web 認証を行わせるもので、Web 認証システムの VLAN を情報コンセントに設定している。こちらについても設定変更スクリプトを作成し、切り替えに掛かる時間短縮を図った。

新 NUWNET システムへの切り替えは東山キャンパス（東地区）、東山キャンパス（西地区）、鶴舞・大幸キャンパスをそれぞれ 1 日、合計 3 日間で切り替えを行った（表 3）。なお、各 AP 接続スイッチに VALN を通す設定作業は事前に行った。

表 3. 切替対象 AP および有線 NUWNET の数と作業実績時間

		1 日目（東山/東地区）	2 日目（東山/西地区）	3 日目（鶴舞・大幸）
自律型 AP	A 社	547 台	404 台	207 台
	B 社	93 台	135 台	97 台
	C 社	5 台	6 台	-
	D 社	96 台	61 台	97 台
制御型 AP	A 社	-	188 台	-
	B 社	-	-	37 台
有線 NUWNET		1401 ポート	1626 ポート	410 ポート
作業時間（実績）		2 時間 20 分	2 時間	1 時間 45 分

5 おわりに

名古屋大学無線ネットワークの概要とともに、キャンパスネットワークの維持管理の一環として行った新 Web 認証システム導入やゲスト専用ネットワークの展開を含めた NUWNET のサービス更新について報告した。新 Web 認証システムは以前から導入を検討しており、またゲスト ID の 802.1X 認証対応についても数年前から要望を受けていたものの、大学からの要望もあり毎年のように AP の増強・更新やセキュリティ強化（UTM 導入）といった無線 LAN 提供エリア拡大のための整備を先に進めてきたため、サービス面での改善等が後回しになっていた。今回のサービス更新により利用者の利便性向上とともに、管理者の運用面での業務量改善に繋がることを期待したい。また、本サービス更新は、2021 年 8 月下旬の情報連携推進本部内の会議にて切り替えスケジュールが了承され、9 月上旬に全学アナウンス、9 月末にサービス更新を行ったが、短い周知期間にもかかわらず、大きな混乱もなく無事終了した。

2020 年 4 月に東海国立大学機構が発足し、2021 年度から学生・教職員に機構アカウントが配布されている。名大 ID に基づく統合認証サービスの段階的縮小、および東海国立大学機構統合認証サービス提供の方針により、近い将来名大 ID をログイン ID として使用できなくなる見込みである。そのため、機構アカウントに対応し、さらによりセキュリティを強化した認証システムの構築が直近の課題となっている。

参考文献

- [1] 川瀬友貴, 石原正也, 岩瀬雄祐, 川田良文, “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”, 令和2年度第16回名古屋大学技術研修会, O10, 2021年3月
- [2] 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, OJOU-3, 2011年3月
- [3] pfSense, <https://www.pfsense.org/>
- [4] Selenium, <https://www.selenium.dev/ja/>
- [5] 名古屋大学無線ネットワーク (NUWNET), <https://icts.nagoya-u.ac.jp/ja/services/nuwnet/>
- [6] 802.1x 認証の NUWNET(nuwnet1x)の利用方法, <https://icts.nagoya-u.ac.jp/ja/services/nuwnet/nuwnet1x.html>