

IAMASにおけるネットワーク環境について 2016

About IAMAS Network Service 2016

山田 晃嗣
YAMADA Koji

Abstract 情報科学芸術大学院大学（IAMASまたは本学と記す。）では、2015年度よりネットワークを含むシステム更改を行った。すでに本学では2004年からプライベートクラウドを採用してきたが、今後もネットワークインフラの安定化のため、さらにクラウドを活用していくこととしている。これまでの動向から本学におけるネットワークの課題と方針を説明し、今回ネットワーク更改のポイントなどを中心に報告する。

Keyword 学内ネットワーク、データセンタ、プライベートクラウド、MACアドレス認証、ウェブ認証、VDI

第1章 はじめに

大学等の教育機関においてキャンパスネットワークの一つである無線LANに接続する端末数が増加傾向にあり^[1]、大学の情報インフラの一部として無線LANが整備されつつある^[2]。本学における学内ネットワークも無線LAN利用が主流となり、PCやスマートフォン・タブレット端末やブラウザ等を持たない機器類も接続するインフラとなった。また、講義では、1年前期でPC等を利用する演習系の授業が開講されているが、それ以外の講義でも大学院大学ということもありレポート作成・提出で利用したり、講義のノートとして利用したりするなど、無線LANのインフラとしての重要性が増している。そのため無線LANのアクセスポイント（AP）はほぼ全学的に利用できるように整備してきた。

本学は教員数19名、学生数は約40名の大学院大学であるため他大学の構成員とは桁違いに少なく、ネットワークトラヒックは多くはない。しかし入学前まで専門としてきた分野が理工系から文科系、アート系、社会学系など幅広いため、それぞれの学生がネットワークをどのように利用するのかは多岐にわたる。例えば、先ほどの講義で利用したり情報を収集するためのネットワークであったり、スマートフォンアプリ制作に利用するネットワークであったり、アート作品の一部としてライブ中継した動画を見せるためのネットワークであったりなど幅広い。過去にはネットワークスイッチを流れるパケッ

トの内容に応じて音を生成するエンターテインメント作品を制作する学生もいたこともあるため、教育・研究・制作活動でもネットワークを利用できる自由度を保ちつつも、安全で安定したネットワークサービスが求められている。

上述した本学における動向を元に第2章で、2015年度より前の概況と2015年度以降のネットワーク更改の方針を述べる。第3章では、ネットワーク構成図を用いて概略を説明した後、具体的にどのような構成となったのかを説明をする。

第2章 ネットワークのあり方

第1節 これまでの状況

これまで2004年以降本学はサーバ類を中心にデータセンタ（DC）に設置し、原則プライベートクラウド（一部はパブリッククラウドサービスも利用）で構成してきた。前回の2009年の機器更新の際にはそれまでラックを設置していたサーバ室の校舎に耐震強度の問題があったため、ルータ等のネットワーク機器もデータセンタに可能な限り設置して災害時のリスクを低減させるための方針を採ってきた。その5年後の2014年の校舎移転の際には校舎内に設置していた機器類のみの移設作業とすることができたため、作業量も減らすことができてスムーズな移行とすることができた。そうした状況を踏まえて次の節で本学の更改における方針を述べる。

第2節 全体の方針

全体の方針として次の3つ、「運用・構築コストの削減」、「教育研究環境の充実」「セキュリティの維持」を中心に更改のポイントを説明する。

第1項 教育研究環境の充実

教員・学生の教育研究活動をより充実させることを目的に学術認証フェデレーション（学認）に参加して外部のサービスプロバイダ（SP）へのアクセスをできるようにした。国立情報学技術研究所（NII）のサービスも学認経由でアクセスできるように変更した。さらには、学術系のネットワークのローミングサービスである eduroam JPに参加し、学外における構成員がネットワークの利用ができるようにしたり、頻繁に出入りする学外研究者が学内のネットワークサービス利用ができる環境とすることとした。

第2項 運用・構築コストの削減

構成員が少ないため、ネットワークやサービスを安定化させるため、DCを活用した。シンククライアントを導入して管理者側で端末を一括操作するなど管理コストを減らすこと、既存のパッケージソフトを活用して本学独自のアカウント等の管理方法の脱却・効率化を図った。

また、センタースイッチもDCへ設置し、校舎内にはエッジスイッチ（アプレシア・システムズ社のApresiaシリーズ）と無線LANのアクセスポイントのみを設置する環境としたため、センタービル・ワークショップ24、それぞれ年に1度の電気の定期点検の停電以外はほぼ利用できるネットワーク構成することとした。

第3項 セキュリティの維持

これまでのセキュリティレベルを下げることなく、エッジスイッチで動作するMACアドレス認証を利用してスイッチレベルで未登録端末の接続をさせないようにしてセキュリティ確保をした。また、UTM（Unified Threat Management）を利用したマルウェア等の対策やURLのフィルタリング、標的型攻撃対策など、ゲートウェイでセキュリティ対策を実施できるシンプルな環境へ移行した。また、事務局の端末は第2項で述べたシンククライアント（画面転送型の仮想デスクトップ）を導入してユーザ端末でのセキュリティ対策を実施することとした。

これらの方針を満たす各機能は、場合によっては一つ

の機能で2つの方針を満たすこともある。例えばシンククライアントは運用・構築のコスト削減となっているが、セキュリティ面にも寄与する機能である。次章ではそれぞれの機能の詳細を述べる。

第3章 ネットワークの構成

第1節 全体構成

図1にネットワークの物理ネットワークの構成図を示す。基本的には前章で述べたようにエッジスイッチと無線LANのAP以外はDCに設置して学内に設置していない。DCに設置したセンタースイッチから各フロアのエッジスイッチは光ケーブルで直接接続している。

無線LANの管理コストを考慮して、これまでと同様にコントローラでAPを管理できるタイプとした。しかし、APの通信がコントローラを経由するタイプだと、コントローラのパフォーマンスがLANに影響を与えることとなる。特にコントローラの不具合が発生すると無線LANサービス全体が停止となってしまう。今後も無線LANの利用増が見込まれるため、今回の更改ではコントローラはAPの管理にのみ関与するシステムであり、かつ安定して通信が行えるシステムを検討した。それらを考慮してラッカスワイヤレス社（現ブロード社）の無線LANを導入した。

第2節 データセンタの利用

本学はソフトピア地区に校舎があり、近隣のDCを利用しやすい環境となっている。本学でDCを利用する主な必要性は以下の通りである。

- ・人的なリソースの対策
- ・建物の対策
- ・セキュリティ対策

上に挙げた項目についてそれぞれ述べる。最初に「人的なリソースの対策」は、1章で述べたように本学の構成員は少ない。そうした状況で安定したインフラを維持するためには、ネットワーク機器やサーバ等のサービスに対して専門的な知識を持つ人が常に対応できる状態にしなければならない。そのためDCのホスティングサービスを利用することで24時間、365日対応できることとした。「建物の対策」に関して、DCは本学の情報を保持する場所であるため耐震などの基準を満たしていること、瞬停対策が確実に行えるなど電源供給が安定していて、機器類の安定稼働のための空調の対策などが重要であると

考えている。特に今回からシンクライアントを採用したこともあり、本学のデータの機密性の向上も必須である。

セキュリティ面については人の立ち入りやその管理など物理的なセキュリティ面のほか、サーバなどのソフトウェアの面における脆弱性対策なども重要視している。今回の更改では以上の点を重点的に考慮したが、もちろんこれら以外にも一般的にDCに求める要件は本学としても同じであるためここでは割愛する。

第3節 認証などのセキュリティ

この節では導入時における問題点など認証などのセキュリティ面について述べる。

第1項 端末・アカウント

これまでのネットワーク運用でも端末のMACアドレス登録は義務付ける運用をしてきた。今回も登録された端末のみ接続可能とするが、登録端末の状況把握がLDAP等と連動して管理できることからエイチ・シー・ネットワークス社製のAccount@Adapter+（以降、A@Aと記す）を採用した。これにより、未登録の端末の場合

は連携するエッジスイッチ側で学内LANに接続させないように設定されている。また、登録された端末であっても一定期間接続されなかった場合、端末情報を削除するなど端末情報のメンテナンスを自動化し効率化を図った。今回は、該当する端末が最後に接続されてから540日間有効としている。接続されていない期限が近づくと削除されることをメールで通知（メール通知の時期については管理者側であらかじめ設定が可能）し、特にその後も接続をしないと自動削除される。これにより端末情報が更新されるようにした。登録手続きはユーザ側でA@A側の申請フォームで申請し、管理者側で許可されたものが利用できるようになる。

また端末と同様にユーザアカウントのパスワードの有効期限も設定してセキュリティの確保をしている。期限が近くなるとパスワードの再設定のメールをユーザへ送信して更新を促すようにしている。ここで更新手続きを行わなかった場合はアカウントがロックされ、ユーザ側からロックを解除する連絡が本学側へない限り利用することができない。これらのパスワード変更に関わるメール通知機能は以前のシステムでも本学にて構築済みで

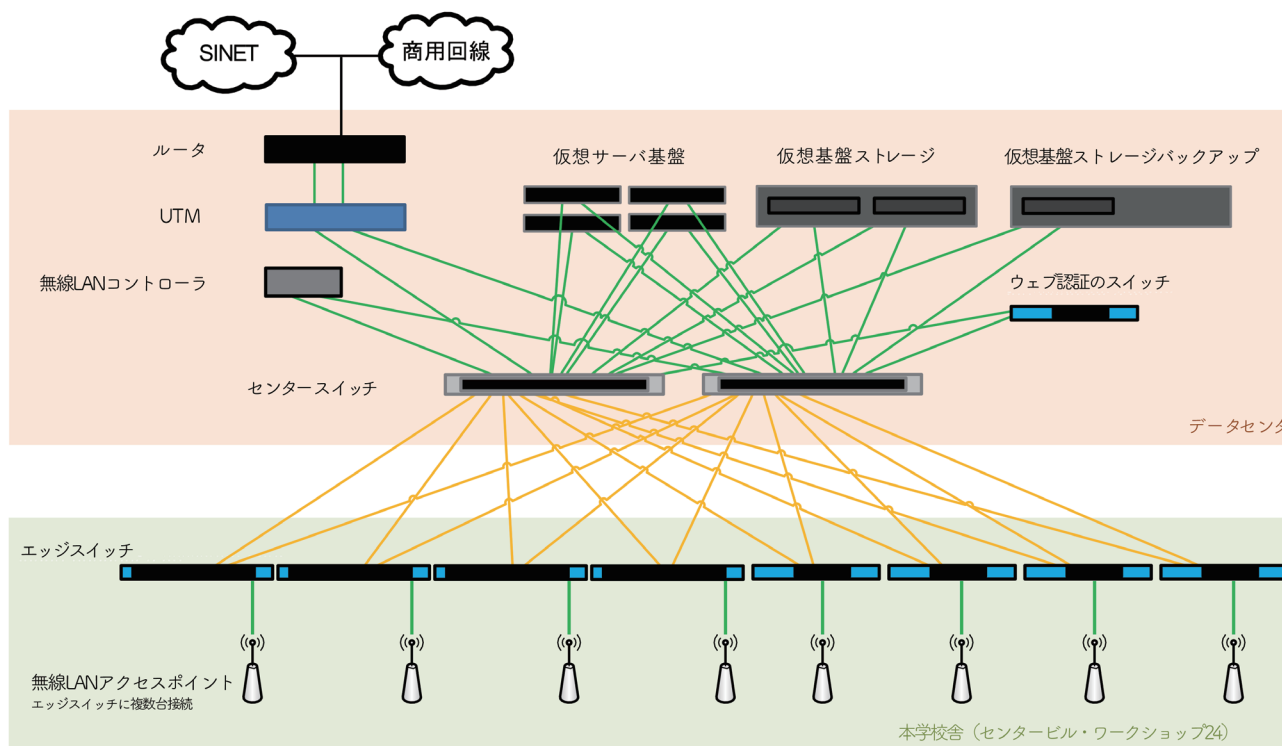


図1 ネットワーク概要図

あったが、アカウントなど部分的な機能であったためA@Aというパッケージソフトを導入することで容易に導入することができた。

しかし、2017年1月にパスワードの有効期限が近いユーザへパスワード再設定の通知メールが同一内容の本文で何度も送信される不具合が発生した。不具合や新機能に対応するためのソフトウェアの更新が頻繁に行われているため、今後の運用では機器側の更新情報に注意してA@Aのバージョンアップをする、不具合を回避するための運用規則を設ける、などの対応が必要である。

第2項 ウェブ認証・MACアドレス認証

上述のようにA@A側で事前に端末登録することを必須としている。接続された端末が登録済みの場合、エッジスイッチがA@Aへ問い合わせでMACアドレス認証をパスすることでネットワーク接続が許可される。未登録の端末の場合、DHCPでIPアドレスが割り当てられた後、A@Aの申請フォーム等の一部の制限されたネットワークのみ接続可能としてセキュリティを担保することとした。

また、MACアドレス認証では当初動的VLANと組み合わせて認証できた場合にVLANを変えることを想定していた。しかし、一部のIoT（Internet of Things）機器が対応できないことが判明したためMACアドレス認証のみを利用している。

MACアドレス認証にパスした端末類はその後ウェブ認証のスイッチを通過しなければ接続できない。ウェブ認証のスイッチは、A@AへRADIUS認証の問い合わせにより実現した。原則MACアドレス認証とウェブ認証の両方をパスした端末のみ学内ネットワーク、外部ネットワークへアクセスできるように設定しているが、プリンタやNAS、IoT等などのブラウザによるウェブ認証ができない端末類についてはA@Aで登録の際にチェック項目を設定し、ウェブ認証をバイパスするようにした。

第3項 デスクトップの仮想化

昨今の状況を踏まえて個人情報等の事務的な情報をよりセキュアに管理すること、端末の運用管理の効率化から本学では事務局を中心に画面転送型のシンクライアント、VDI（デスクトップの仮想化）を導入した。教職員のみこれらを利用することとするが、教員については個人情報などを含む一部の情報を扱う場合のみ利用し、

それ以外の研究教育等においてはこれまで通りの通常の端末（ファットクライアント）を利用することとした。

端末側に情報を保持しないようにすることでセキュリティが確保できることや、これまでにVMware社のソフトを利用してサーバの仮想化をしていたこと、VMware社のHorizon Viewが採用しているPCoIPが安定していることなどからこの方式とした。Windows10を用いた共有方式のリンククローンでの利用を前提として運用を行い、管理者は基本的に一つのマスタイメージをメンテナンスすることで負担軽減を図った。ただ、一部の特殊なアプリを必要とするユーザについてはApp Volumesにて一部のユーザに紐付いたアプリの導入をすることとした。しかしWindowsのアプリであってもリンククローン環境でのメーカーによる動作保証がないケースもあり、そうしたアプリについては専有方式のフルクローンアカウントを作成して、アプリを利用する時のみログインするなど運用面を変更した。

教員側はファットクライアントのソフトウェアでVDIを利用し、事務局職員はゼロクライアント端末でVDIを利用している。VDIになることでソフトウェアは原則共通アプリのみの利用とする、ファイル等はデスクトップに保存せず個人領域への保存をするなどユーザ側にもいくらかの制限がかかり、利用に関する混乱等や慣れるための時間が必要であった。また、ソフトウェアでのVDIアクセスは安定しているが、ゼロクライアントからのアクセスはゼロクライアントの端末側との相性からかログイン時の挙動が安定しないこともあり、ログイン直後の画面が出ない、解像度が安定しないなどこちらについては現在も調整をしているところである。

第4項 ゲートウェイのセキュリティについて

今回はUTMのゲートウェイセキュリティとしてパロアルトネットワークス社のPAシリーズを導入した。これによりネットワークを通過するウイルス・ワーム対策に限らず、URLフィルタリングによる制限の他、どのようなアプリによるパケットが多く流通しているかなどの見える化もできるようになった。また、この機器はウイルス対策ソフトのパターンでは検出できない、いわゆるゼロデイ対策・標的型攻撃対策などにも対応している。なお、この機能を有効にするにはパロアルトネットワークス社のクラウドサービスであるWildFireと連携したサンドボックスによる検出が必須となるため利用環境に注

意が必要である。月に数件程度WildFireへファイルがアップロードされるが、現段階では検出した事例はない。

第4節 各種フェデレーション等の参加

第1項 学術認証フェデレーション

本学はこれまで上流は商用回線を利用してきたが、2015年度より学術情報ネットワーク（SINET）^[3]をメインの上流回線とし、商用回線をバックアップ回線とするマルチホーム環境で利用している。2016年度には学術認証フェデレーション（学認）^[4]に参加し、外部の学術リソースを提供するサービスプロバイダ（SP）にもアクセスできる環境を整えた。学認とは、NIIと学認参加大学等、SP等で構成され、大学等が学術リソースの利用者として、それらを提供する機関や出版社がSPとして構成する連合体のことである。各参加機関は学認が定めた規程を信頼しあうことで、認証連携環境を構築することができる。本学でも参加するにあたりShibboleth認証ができるようにファルコンシステムコンサルティング社製のWisepoint Shibbolethを利用してIdPサーバ（認証サーバ）を構築し、NIIが実施しているCiNii^[5]へ学認経由でアクセスできるようにした。SPは今後の状況を見てさらに追加をしていく予定である。また、学内の一部のサービスについてもShibboleth認証を導入してシングルサインオンの環境を取り入れて利便性を図ることとした。

第2項 eduroam JPへの参加

以前より本学はゲスト用の無線LANネットワークをサービスとして運用してきた。しかしここ数年は本学に一時的に出入りする他大学の研究員なども多いため、

2016年度よりeduroam JPに参加することで学内・学外でのネットワークの利便性を図ることにした。eduroamは、世界80か国(地域)が参加している大学等のキャンパスネットワークの相互利用できる環境で、日本でのサービス（eduroam JP）はNIIが行っている。利用者認証に本学のアカウントでも対応は可能であるが、セキュリティ的側面から本学では学認のShibbolethに対応したeduroam仮名アカウント発行システム^[7]にてあらかじめアカウントを発行して利用することとした。

第4章 まとめ

センタースイッチをデータセンタへ設置し、校舎側にはエッジスイッチと無線LANのアクセスポイントのみを設置する環境として停電によるサービス停止をできるだけ短時間とすることができた。

また、エッジスイッチとA@AによりMACアドレス認証を利用してスイッチレベルで未登録端末の接続を拒否し、登録端末やユーザアカウントの定期的な棚卸を容易に実現することができた。また、UTMを利用しゲートウェイでのセキュリティ対策をシンプルにできる環境へ移行したり、画面転送型のシンクライアントの仮想デスクトップを導入してユーザ端末におけるセキュリティ対策も実施した。

学認への参加とネットワークローミングサービスであるeduroam JPに参加し、教育研究環境の充実と利便性の向上を図ることができた。

一方でVDI関係やA@Aなど一部では度々不具合が起きていて現在でも調整をしているサービスもある。本学では運用業者と定期的な打ち合わせを行っており、今後も密に連携して対応をしていく予定である。

参考文献

- [1] 鳩野 逸生：全学無線LAN利用ログ情報の解析と応用、研究報告インターネットと運用技術（IOT）、Vol. 2015-IOT-31, No. 10, pp.1-6（2015）
- [2] 文部科学省平成27年度学術情報基盤実態調査結果報告：<http://www.janul.jp/j/documents/mext/jittai27kekka.pdf>（2017年1月5日確認）
- [3] 学術情報ネットワーク（SINET）：<https://www.sinet.ad.jp/>（2017年2月7日確認）
- [4] 学術認証フェデレーション（学認）：<https://www.gakunin.jp/>（2017年2月6日確認）
- [5] NII学術情報ナビゲータ（CiNii）：<http://ci.nii.ac.jp/>（2017年2月7日確認）
- [6] eduroam JP：<https://www.eduroam.jp/>（2017年2月6日確認）
- [7] eduroam仮名アカウント発行システム：<https://eduroamshib.nii.ac.jp/>（2017年2月7日確認）