

キャンパス情報ネットワークの更新について

渡邊 美穂・田中 昌二・万田 真樹・上田 康信

岐阜大学 情報連携統括本部

岐阜大学では、キャンパス情報ネットワークの基幹を担う情報ネットワーク機器のサポート終了に伴い、2018 年度に大規模なネットワークの更新を行った。また、セキュリティ強化のため、ネットワークに接続するユーザー端末の MAC アドレスによる認証やプライベート IP アドレス化への移行を行った。さらに、利用者の利便性向上を図るため、無線 LAN 環境の拡充や各研究室の回線高速化も行った。本稿では、キャンパス情報ネットワーク更新の概要について報告する。

Key Words : MAC アドレス認証, プライベート IP アドレス, 動的 VLAN

1. はじめに

岐阜大学における教育・研究・事務に関する情報処理の円滑化ならびに情報の促進を図る上での重要インフラとなるキャンパス情報ネットワークは、ひとたびこれが停止することにより、本学における上記の諸活動に大きな影響が及ぶ。また、情報ネットワーク機器の一般的な耐用寿命は 10 年程度と言われている。岐阜大学のキャンパス情報ネットワークは、全学の基幹を担う基幹スイッチ群、部局の基幹を担う部局基幹スイッチ、各部屋の情報コンセントを収容するフロアスイッチから構成されているが、これらを構成する大半のフロアスイッチは 2018 年度に導入から 10 年を迎えることになる上、基幹及び部局基幹を担っているスイッチについてもメーカーによるサポートが終了となる。耐用寿命を超えた機器の故障率は高くなる一方であることや、メーカーサポートを受けられない機器の継続運用は、障害発生時に大学における諸活動において致命的な事態をもたらす可能性があるため、大規模なネットワーク更新を数年前から計画し、2018 年度に実施した。

また、セキュリティ面においてもさらなる強化を図るため、MAC アドレス認証の導入及びユーザー端末のプライベート IP アドレスへの移行を併せて行うことにした。さらに、各研究室の通信の高速化等、利用者の利便性に

も考慮したネットワーク環境を構築することにした。

本稿では、更新した新キャンパス情報ネットワークの概要について、報告する。

2. 旧キャンパス情報ネットワークについて

更新前のキャンパス情報ネットワーク(以下、旧キャンパス情報ネットワークという)は、セキュリティ対策として、学外からの不正アクセスを防御するファイアウォールと、あらゆる通信を監視し異常な通信があればその通信を検知・ブロックする機能をもつ不正侵入防止システム(IPS)の 2 種類のセキュリティ機器を用いていた。この構成において一定の安全性を確保していたが、本来正常な通信に問題が発生した際、その問題がどちらの機器に起因しているのか、原因の切り分けが困難であるという課題があった。

また、旧キャンパス情報ネットワークでは、各部局単位にグローバル IP アドレスをセグメント単位で割り当て、部局にて IP アドレスの管理を行っていた。ユーザー端末に割り当てる IP アドレスはすべて固定であったため、部局におけるグローバル IP アドレスの管理負担も大きく、利用者においては、端末設定が難しいという声も聞かれていた。さらに、昨今のセキュリティ情勢を鑑みると、ユーザー端末がインターネット(学外)の脅威に直接さらされ

るグローバル IP アドレスを利用することについては、キャンパス情報ネットワークを運用する中で、セキュリティ面や端末管理面で懸念事項であった。

3. 新キャンパス情報ネットワークについて

今回更新を行ったキャンパス情報ネットワーク(新キャンパス情報ネットワーク)においては、各機器を一新するとともに、以下のような変更を実施した。

- (1) セキュリティ機器の統合
- (2) プライベート IP アドレス化
- (3) MAC アドレスによる認証
- (4) 動的 VLAN
- (5) 全研究室 1Gbps 化
- (6) 無線 LAN 環境の拡充

(1) セキュリティ機器の統合

旧キャンパス情報ネットワークでは別々の機器だったセキュリティ機器を 1 台に統合した。また、セキュリティレベルを新規に導入し、図 1 に示すゾーニングを行った。

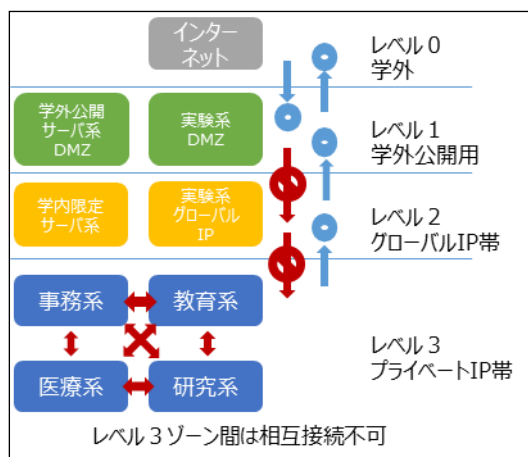


図 1 セキュリティレベルによるゾーニング

本ゾーニング構成は、通信の目的に応じてレベル 1 からレベル 3 の三つのレベルにより構成され、レベル 3 が最も高い安全性を要する目的で設定される。低いレベルから高いレベルへの通信をアクセス制限することで、利用目的を達成しつつ通信の安全性を確保する。また、

ある情報機器が学外から攻撃を受けた際、学内全体に被害が蔓延する事態を防ぐことができる。

なお、学外からの攻撃対象となる危険性の高い学外公開サーバにおいては、定期的にサーバ管理者に対し、セキュリティパッチの適用状況等、適切なセキュリティ対策がなされているかのチェックを促す。

(2) プライベート IP アドレス化

ユーザーが利用するすべての一般端末が使用する IP アドレスをプライベート IP アドレスへ移行した。また、本学の教育職員(以下、教員という)1 名につき 1 セグメントを割り当て、教員自身が 245 個の IP アドレスを管理可能とした。これにより、部局の IP アドレス管理負担が軽減された。さらに、教員へ配布可能な IP アドレス数のばらつきや配布可能な IP アドレスの枯渇等、部局により差があったさまざまな IP アドレスの問題も解消された。

なお、導入したネットワーク機器の性能的制限によりセグメントを保有できる教員は常勤の助教以上としている。

(3) MAC アドレスによる認証

すべての情報機器に固有の MAC アドレス(物理アドレス)を用いた認証を導入し、事前に登録された機器以外の接続を許可しないこととした。

MAC アドレスの登録は、Web で提供する管理サイトで行う。なお、この管理サイトで使用するユーザーIDは、岐阜大学情報連携統括本部が管理している統合認証システムで利用するIDを用いる。また、この管理サイトへのログインは、セグメントを保有できる教員にのみ権限が付与されるような仕組みとなっている。

なお、MAC アドレスによる認証は、教員が主に利用する研究室や実験室の情報コンセントを対象としており、後に記載する無線 LAN 環境については、ユーザーIDとパスワードによる認証を用いている。

(4) 動的 VLAN

旧キャンパス情報ネットワークでは、各部屋の情報コンセントに対し固定で VLAN を設定していた。一方、利用者はグローバルIPを固定で設定していたため、VLANとIP アドレスの不一致による接続トラブルも多かった。また、部屋の利用者変更による情報コンセント側の設定変更も定常的に発生し、管理担当者の負担も大きかった。

今回、MAC アドレスによる認証を導入することにより、各情報コンセントに接続された機器から VLAN(ひいては利用者)が特定されるため、各情報コンセントは、接続された機器から特定された VLAN を動的に割り当てる仕組みとした。

この動的 VLAN の仕組みを導入することで、利用者は、MAC アドレスを登録済の機器であれば、学内のどの情報コンセントへ接続しても自身のセグメントで利用可能となり、利用者の利便性の向上につながった。

(5) 全研究室 1Gbps 化

各部屋の情報コンセントにおける通信速度を、100Mbps から 1Gbps へ変更することにより、利用者がより快適にネットワークを利用できる環境を整備した。なお、新キャンパス情報ネットワークは、基幹スイッチと部局基幹スイッチ間を 10Gbps、部局基幹スイッチとフロアスイッチ間を 1Gbps で接続している。

(6) 無線 LAN 環境の拡充

無線 LAN 環境については、これまで主に学生に提供するサービスとして提供を続けてきた背景があり、教育・研究に不要と判断されるコンテンツへのアクセスを制限する等制約のある環境であった。また、昨今の無線 LAN 環境の急激な需要増加もあり、授業において教員が利用する際に不便との声や、学会や会議での利用要望も増えてきていた。

そのため、今回の更新で、新たに教職員用無線 LAN 環境を整備することとした。しかしながら、1 つの無線 LAN アクセスポイントにつきアナウンス可能な識別名 (SSID) は 1 つという制約から、複数の識別名をアナウンスするためには、学生用に加え、新たに無線 LAN アクセスポイントが必要となる。この問題を解消するため、無線 LAN コントローラを導入し、1 つの無線 LAN アクセスポイントで複数の識別名をアナウンスすることを可能とした。現在、無線 LAN アクセスポイントを設置しているエリアにおいては、学生用無線 LAN 識別名、教職員用無線 LAN 識別名、さらに大学等教育研究機関の間でキャンパス無線 LAN の相互利用を実現する「eduroam」の 3 つを同時に提供し、利用者の利便性を高めた。

さらに、無線 LAN が利用可能な通信エリアも拡充を

図り、全学共通教育棟においては全講義室に環境を整備した。

なお、学生用及び教職員用無線 LAN 環境へ接続するには識別名に付随するセキュリティキーに加え、前述の統合認証システムにて利用する ID での認証を必須とする。

4. 今後の課題

今回のキャンパス情報ネットワーク更新では、キャンパス情報ネットワークの安全かつ安定した運用を最大の目的とし、上述のような仕組みを導入した。本更新について今後改善すべき課題について述べる。

例えば、MAC アドレス認証においては、管理者不在の端末がキャンパス情報ネットワークに接続される事を防いでいるが、管理者が退職等で大学を離れた際に残置された機器については、管理者不在の端末としてキャンパス情報ネットワークへ接続されうる状態のまま学内に残ることとなる。安全な運用を継続するためには、今後、このような管理者不在となる端末の定期的な棚卸しが必要である。また、セキュリティ機器においても、学外に対して開放している通信設定と学外公開サーバの運用状況との整合性を定期的に調査することで不要な通信がなされないよう確認する必要がある。

今後は、機器の障害を早期に検知するための監視や、障害発生時の迅速な対応を可能とする保守契約を限られた予算の中で締結することにより、高い可用性を維持した運用を目指す。

謝辞

本報告を作成するにあたり、ご指導、ご助言をいただきました岐阜大学情報連携統括本部の皆様方、及び、今回のキャンパス情報ネットワーク更新にあたり、ご協力をいただきました学内の皆様方に深く感謝いたします。