

群馬大学のネットワーク運用と更新について

浜元 信州^{1,a)} 井田 寿朗¹ 齋藤 貴英¹ 酒井 秀晃¹ 小田切 貴志¹ 横山 重俊¹

概要: 群馬大学では、全学規模でのネットワーク更新を行い、群馬大学学術情報ネットワーク (GUNet2016) として、2016 年 4 月より運用を開始している。本ネットワークは、幹線機器の高速化、冗長化を施した安定で高速なネットワークであると共に、ネットワークアクセス認証と動的 VLAN による全学規模のネットワークである。本ネットワークの導入により、接続機器の管理者が明確となり、セキュリティインシデント時の機器特定も容易となった。動的 VLAN による柔構造のネットワークとすることにより、場所単位から人単位でのサブネット構成をとることが可能となり、近年、大学で多く見られる学科横断的組織構成にも柔軟に対応できるようになった。本稿では、新たに導入した群馬大学学術情報ネットワーク (GUNet2016) の導入と現在の運用状況について述べる。

The Operation and Replace of the Campus Network of Gunma University

NOBUKUNI HAMAMOTO^{1,a)} HISAO IDA¹ TAKAHIDE SAITO¹ HIDEAKI SAKAI¹ TAKASHI OTAGIRI¹
SHIGETOSHI YOKOYAMA¹

Abstract: We replaced Gunma University Network (GUNet2016) which is a campus-wide network of Gunma university. The new network GUNet2016 provides fast and stable network connections to the users with keeping security. The backbone switches are connected with 10Gbps which is faster than before and are equipped redundant apparatus working simultaneously with help of stacking technology. Our network administrator can easily specify the connected devices by using the authentication feature of the GUNet2016. Also, we introduce dynamic VLAN where the subnet of devices are determined by the mac address or user ID used in the network access authentication. The dynamic VLAN enables us to create soft network structure where the subnet are determined by the attribute of every user such as department or school not the the place (room or floor). The soft structure network easily provides subnet to some inter-department group of users created in many Japanese universities. The paper describe the replace and recent status of the GUNet2016.

1. はじめに

群馬大学は、4 学部 5 研究科からなる国立大学法人であり、学生約 6,500 人、教職員約 2,500 人の構成員が在籍している。学部は、教育学部、社会情報学部、医学部、及び、理工学部の 4 学部、研究科は、教育学研究科、社会情報学研究科、医学系研究科、保健学研究科、及び、理工学部の 5 研究科から構成されている。また、附置研究所として生体調節研究所、医学部には、医学部附属病院を有している。

全ての学部は、理系分野に関連する教員を有していることを考えると、理系が主体の人員構成の大学である。大学は 4 キャンパスにわたる分散構成であり、教育学部、社会情報学部、及び、事務局本部が設置されている荒牧キャンパス、医学部、医学部附属病院が設置されている昭和キャンパス、理工学部の設置されている桐生キャンパス、及び、理工学部の一部研究室が設置されている太田キャンパスからなる。荒牧キャンパス、昭和キャンパスは、群馬県前橋市内にあり、直線距離でおよそ 3km 離れて位置している。桐生キャンパスは群馬県桐生市内にあり、昭和、荒牧キャンパスからの直線距離はそれぞれ 25km、27km である。太田キャンパスは群馬県太田市内にあり、桐生キャンパスか

¹ 群馬大学 総合情報メディアセンター
Library and Information Technology Center, Gunma University, 4-2 Aramaki-Machi, Maebashi, Gunma, 371-8510, Japan

a) n.hamamoto@gunma-u.ac.jp

らの直線距離が14km, 荒牧キャンパスからの直線距離が33kmである。

群馬大学のネットワークは、2001年以来、キャンパス全体に関わる更新を実施できずにいた。コアスイッチに関しては、4年毎の教育用端末等の更新に合わせて更新を行ってきたが、コアスイッチから部屋の情報コンセントまでにわたる全学規模の更新は実現しなかった。有線ネットワークの更新が実現しない中で、無線やセキュリティに関する要求は増え、2008年5月より、段階的に無線LANシステムの導入が始まり、2009年に増設を行った。近年スマートフォンを始めとする無線デバイスが増加したため、2013年にアクセスポイントの大幅増設を実施し、ほぼ全ての教室と主要部分にわたる無線LANネットワークを構築した。また、2009年1月には、セキュリティ強化のため、全学ファイアウォール導入を導入しセキュリティの確保を行った。

有線部分の更新が実現していなかった群馬大学ネットワークだが、2010年3月には、荒牧地区でネットワークの更新が実現した[8]。本更新では、光直取ネットワークと呼ぶ、各建屋に配置されたスイッチを排除し、総合情報メディアセンターに集中して配置したスイッチと各部屋の情報コンセントを光ケーブルで直接結ぶネットワークへの切り替えを行った。また、認証ネットワークの導入も同時に実施し、本更新により、荒牧地区については、安定したネットワーク提供が可能となった。しかしながら、他キャンパスでは、ネットワークの老朽化は避けられず、機器故障や誤接続によるフロア単位、建屋単位のネットワーク停止が発生する状況となっていた。また、荒牧地区の光直取ネットワークも保守期限が迫っている状況で、全学的なネットワークの老朽化が進んでいた。さらには、全学ファイアウォールも、老朽化しており、保守期限が迫る状況となっていた。

このような機器の老朽化が迫る状況のなかで、2016年に稼働開始となったSINET5への更新では、全国的なバックボーンネットワークの高速化と、10Gbps機器の価格低下により、学外接続は1Gbpsから10Gbpsへの増速が現実的となり、群馬大学でも学外接続、キャンパス間接続の10Gbps化を目指した。しかし、ファイアウォールやネットワーク機器は全て1Gbpsを想定して構築していたため、高速化に耐えられない状況となっていた。

以上のような、導入機器の老朽化が進んだことや、学外ネットワークの高速化に対応できなくなったことを背景に、2016年4月に群馬大学ネットワークは、全学的な更新を行い群馬大学学術情報ネットワーク(GUNet2016)を新たに構築した。本論文では、これまでのネットワーク運用と更新、更新後の運用について報告する。

2. 群馬大学学術情報ネットワーク

新ネットワークでは、高速、安定、そして、安全なネットワークを提供すべく更新を実施した。群馬大学学術情報ネットワークの概要を図1に示す。

2.1 物理構成

群馬大学では、2010年に荒牧地区で光直取ネットワークを導入していた。本ネットワークの導入により、荒牧地区のネットワークは、中間スイッチがない構成となり、安定なネットワークとなった。今回の更新で、昭和、桐生地区へも光直取ネットワークの導入を検討したが、光直取ネットワークは光配線や各部屋に設置するメディアコンバータの価格が高価であるため本更新では導入を断念した。このため、昭和地区、桐生地区では、建屋間を光配線、建屋内をメタル配線とした従来通りの構成を踏襲することとなった。

従来のネットワークでは、機器の故障に伴うネットワーク停止が多く、コアスイッチなどの停止の影響が大きいスイッチに関しても、冗長化などの機器故障に対する対策はなかった。新たなネットワークでは、安定なネットワークを提供するため、機器の冗長化を可能な限り実施した設計とすることとなった。

2.1.1 荒牧地区

荒牧地区の構成は、光直取構成で、総合情報メディアセンターに設置したコアスイッチ(アラクスラネットワークス社製AX-4630S-4M)2台の配下に、光多ポートスイッチ(アラクスラネットワークス社製AX-2530S-24S4X)をそれぞれ10Gbpsで接続している。コアスイッチ2台は、スタック構成をとっており、コアスイッチ1台の故障に対してもサービスを維持できる構成であるうえ、通常時には、リンクアグリゲーションを構成し、通信の負荷分散を自動的にしている。

荒牧地区では、各部屋に配置する情報コンセントの数は合計で約600になる。ユーザにはUTP接続を提供する必要があるため、各部屋には光メディアコンバータ(トランジションネットワークス社製GE-PSW-LX-01)を設置した上で、各部屋の光メディアコンバータと総合情報メディアセンターに設置した光多ポートのスイッチとを直接1000BASE-LX接続している。従来の構成では、コアスイッチ1台の配下に、光多ポートのシャーシ型スイッチ2台を接続し、荒牧地区の光接続を提供した。シャーシ型スイッチは、光接続モジュール毎に独立性は高い構成であるものの、シャーシ自体の故障など、サービスの一斉停止につながる可能性が否定できない。群馬大学では、スイッチのコントロールプレーンのCPU暴走を回復するため、スイッチ全体の再起動が必要となり、サービス停止が発生している。この場合も、特に故障ではなくCPU暴走中も正

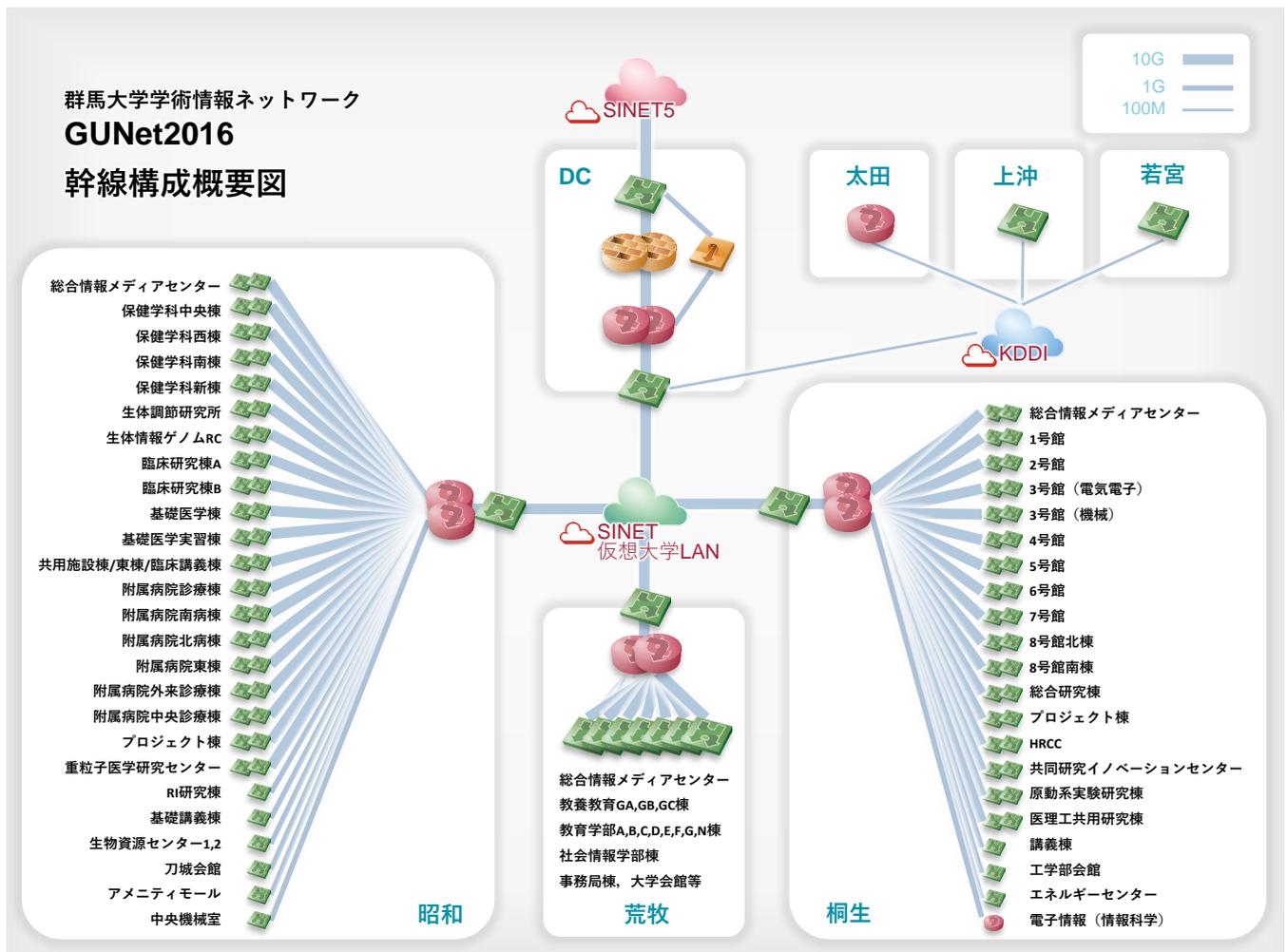


図 1 群馬大学学術情報ネットワーク (GUNet2016) 幹線接続概要図
Fig. 1 Overview of the backbone network of Gunma University Network (GUNet2016).

常なフレーム/パケット転送を実施していたが、CPU 暴走を止めるための機器全体の再起動が必要になり、短時間ではあるが荒牧地区全体に及ぶ広範囲のネットワーク停止が発生してしまった。このような経験から、機器の独立性を高めた構成により、機器故障の影響を最小限に抑えることが、更新時の方針となった。更新後の構成では、光直取スイッチは、25 台に分散/独立したスイッチで構成されることとし、機器 1 台の故障が、他の機器に影響を与えない構成とした。光直取スイッチの故障により、その配下の情報コンセントに対してサービスは提供できなくなるが、影響は最小範囲にとどめることができる。

光直取ネットワークの問題点の一つは、メディアコンバータの耐用年数である。荒牧キャンパスに 600 個配置されているメディアコンバータは、導入から 6 年が経つ現在でも故障はしていないこともあり、今回の更新ではメディアコンバータはそのまま利用しつづけることとした。メディアコンバータには稼動部品などはないため、比較的故障しにくい製品であるが、今後、故障が頻発する可能性は否定できない状況である。

2.1.2 昭和, 桐生地区

昭和, 桐生地区の構成は、キャンパスのコアスイッチを中心としたスター型の構成である。コアスイッチからは、各建屋に配置された建屋スイッチに対して、それぞれ 10G-BASE-LR 接続されている。各地区のコアスイッチは冗長化されている他、各建屋に配置した建屋スイッチもほぼ全て冗長化されている。各建屋スイッチからは、各階に配置されたフロアスイッチにそれぞれ UTP 配線により 1000BASE-T 接続され、フロアスイッチが各部屋へ UTP ケーブルを介して情報コンセントを提供している。フロアスイッチがない建屋では、建屋スイッチから直接、各部屋へ UTP 配線され情報コンセントを提供している。建屋スイッチは、利用ポート数に応じて、アラクスネットワーク社製 AX-2530S-48T2X または、AX-2350S-24T4X を採用し、フロアスイッチは、AX-2530S-24TD を採用している。

昭和, 桐生地区の構成は、スター型の構成であることから、コアスイッチの地理的分散は行われていないものの、コアスイッチ、建屋スイッチのスタック構成による冗長化

が行われている。この構成では、コアシッチ 1 台の故障に対しては、サービス停止が発生しない。また、建屋スイッチ 1 台の故障に対してのサービス停止発生の有無は建屋のネットワーク構成に依存する。建屋スイッチそのものが情報コンセントを提供している場合には、配下の情報コンセントが停止するが、建屋スイッチ配下にフロアスイッチが冗長化接続されている場合には、建屋スイッチ 1 台の故障に対して、情報コンセントに対するネットワーク停止は発生しない。従来は、建屋スイッチ、コアシッチともに冗長化されていない構成のため、これらのスイッチ故障に対する影響が大きかったが、更新により影響はなくなり安定なネットワーク提供に貢献している。

2.1.3 災害対策 DC

群馬大学では、災害対策などを目的として災害対策データセンター（災害対策 DC）を準備し主要サーバを配置している。また、災害対策 DC には、コアシッチ（アラクスサラネットワークス社製 AX-3830S-44XW）の他、ファイアウォール、VPN 接続装置を配置し、各地区からインターネットへの通信は、本 DC のファイアウォールを経由する構成をとっている。コアシッチ、ファイアウォール共に 2 重化されており、1 台の障害に対して通信が継続する構成となり、安定性は、従来のコアシッチ 1 台構成と比較して向上している。

2.1.4 太田, 上沖, 若宮地区

太田地区, 上沖地区, 及び, 若宮地区は, 他地区と比較して小規模な地区である。太田地区には理工学部の一部の研究室があり, L3 スイッチ 1 台とフロアスイッチが設置されている。上沖地区は, 教育学部附属中学校が, 若宮地区には, 教育学部附属小学校, 幼稚園, 特別支援学校があり, 各地区の L2 スイッチと各フロアにフロアスイッチが設置されている。

2.2 論理構成

2.2.1 IP 設計

本学では, /16 のグローバルアドレスを保有しており, 学内の全ての機器にグローバル IP アドレスを付与する運用を行なっている。これは, 可能な限り NAT などによる IP アドレスの隠蔽を行わないことで, セキュリティインシデント時などの追跡が容易となるためである。更新後もこの方針は変わらず, グローバル IP アドレスを維持することとした。IP アドレスは /24 のサブネットに分割し, 部局毎にいくつかのサブネットを割り当てている。これまで, 荒牧地区を除いては, 機器の設置場所を基準に, 建屋とフロアにより, サブネットを割り当てていた。本学でのネットワークの管理体制は, 部局, 学科単位を基本としている。これまで, 建屋, フロアが部局, 学科に対応していたため, 部局毎にサブネットを割り当てる形となっていたが, 近年, 総合研究棟などのプロジェクト型の研究ス

ペースなどが増え, 複数学科の研究室が混在するフロアが増えてきた。また, 主に医学部の臨床系研究室など, 研究室と附属病院を往来するユーザも多い。さらに, 学科を超えた改組などもあり, 1 フロア, 1 サブネットの単純なネットワーク構成では学科などに対応したサブネット分割に対応できない事例が増えていた。このような状況を抜本的に改善するため, 本更新では, 後述する認証と連動した動的 VLAN を導入し, 場所に付随したネットワークから, 個人の所属に基づいたネットワークへと変更することとした。この変更により /24 のサブネットは, フロアや建屋ではなく, 部局に所属する人, デバイスに割り当てる形となり, 主に教職員は, 学科, 研究室などの所属に基づきサブネットが決まることとなった。端末には DHCP を利用し, サーバ等には固定 IP を部局管理者が付与する管理とした。

2.2.2 認証と動的 VLAN

群馬大学では, 以前よりファイアウォールを導入しセキュリティインシデントの検知を行ってきたが, 接続機器の特定が十分でないことがあり問題となっていた。荒牧地区では, 従来より動的 VLAN による認証ネットワークが導入されており, 接続機器の特定が確実なものになっていた。今回の更新では, 動的 VLAN による認証ネットワークを, 昭和地区, 桐生地区に対しても適用し全学でのインシデント追跡性を上げることとなった。動的 VLAN では, 認証情報に基づいて端末の所属する VLAN が決まるネットワークであり, 広島大学 [1], 岡山大学 [2] などでの採用例がある。大学では, 多様な機器が接続されることから, プリンタを含め多くの機器に対応可能な MAC アドレス認証と Web ブラウザを利用したユーザ認証 (Web 認証) が併用されており, 本学もこの 2 方式を採用した。

認証ネットワークを大学などで導入する際には, MAC アドレスなどの認証情報の管理が問題となる。今回の更新では, Web 認証の利用も可能ではあるが, ユーザ ID の入力などが煩わしいなどの理由によりユーザからの不満が予想されるため, 本学では MAC アドレス認証を主に利用することとした。MAC アドレス登録は様々な事例がある [3], [4], [5], [6]。登録作業は, 個人単位, 部局管理者単位, 管理者一括など, 大学の実情により様々だが, 本学では, 荒牧地区と同様に, 基本的に個人が個々に MAC アドレスの登録を行う方法を採用した [8]。これまでの荒牧地区での運用では, 登録用の Web システムを独自開発していたが, 本更新では, 認証サーバとして日立電線ネットワークス社製 Account@Adopter+を採用し, 登録用の Web 画面も提供することとした。

動的 VLAN では, 機器の移動などがあっても, スイッチの再設定は必要なく, 場所によらない柔軟なサブネット構成をとることができる。これにより, 管理者は, サブネット配置の設計を行う際には機器や個人の属性のみを考慮すれば良い。大学には, 総合情報メディアセンターや学科の

表 1 GUNet2016 構成スイッチ一覧

Table 1 The list of network switches constituting the GUNet2016.

スイッチ	機種名	荒牧	昭和	桐生	DC	認証	スタック
コアスイッチ A	AX-4630S-4M	2	2	2			あり
コアスイッチ B	AX-3830S-44XW				2		あり
基幹建屋スイッチ	AX-2350S-24T4X		28	14			あり
認証建屋スイッチ	AX-2530S-48T2X		10	15		あり	
光直収認証スイッチ	AX-2530S-24S4X	25				あり	
認証フロアスイッチ	AX-2530S-24TD		121	50		あり	

共用 PC, 研究室の PC, プリンタ, ブロードバンドルータ, サーバ, 実験機器, 学生の持ち込み PC, 事務職員の PC, サーバなど様々な機器が配置されている。本学では, 研究室の機器は, 基本的に研究室の教員に管理責任があり, 学生の持ち込み PC は学生が, 事務職員の PC などは事務部門として組織的に管理されている。本学の動的 VLAN の導入では, サブネット構成も基本的に管理者分類に則ったものとし, 教員の管理するサブネット, 学生の管理するサブネット, 事務職員が管理するサブネットを動的 VLAN により導入する方向とした。

これらのサブネットへの実際の配置は, MAC アドレス認証, Web 認証に基づく動的 VLAN により, 自動的に配置される。教員, 事務のサブネットへの配置は, MAC アドレス認証を利用している。前述の登録用 Web システムへの登録は教職員に限定し, 登録した MAC アドレスは教職員の所属に応じたサブネットへと自動的に配置される。更新前に荒牧地区で導入していたシステムでは, 各ユーザが部局毎に決められた範囲の中で VLAN ID の指定を行っていたが, 必ずしも正確な VLAN ID を選択するユーザばかりではないことがわかった。このため, 更新後はユーザ毎の所属を基に VLAN ID を決定し, 各ユーザには, VLAN ID を意識させない構成をとることにした。学科管理の共用 PC など, 管理上の都合により, 特別なサブネットを利用したい場合には, 学科のサブネット管理者が登録できるようにした。

学生は, 基本的に Web 認証のみを利用することとなるため, 教職員とは自動的にサブネットが分かれる。また, 公開サーバは, 極力, 学内公開サーバのサブネットに集約することとした。以上のように, 学内のサブネットは, 図 2 に示す 4 つの種類に分けることとなった。

2.2.3 アクセス制限

群馬大学ネットワークは, 学外の接続点にファイアウォールを配置し学外から学内への通信を基本的に拒否する設計としている。学外にサーバなどを公開する際には, 申請が必要であり, 許可されたサーバのみが学外に公開されている。この構成は, 大変単純で, ユーザに取ってもわかりやすい構成であるという利点はあるものの, 学内同士の通信は監視できない構成であり, APT 攻撃など, 巧妙化し

ている攻撃手法に対応するためには, 不十分とされている。学内同士でのアクセス制限はユーザによって分りにくいものとなる可能性があることもあり, サブネットを超える Windows 共有, 印刷の禁止を除いては導入を見送っていた。今回の更新では, これまでなかった学内の通信に対する制限を加えることによりセキュリティ対策の強化を行った。

更新後, 図 2 に示すように管理者に基づいて分類した 4 つの種類にサブネットは, 程度の差はあるものの, お互いにセキュリティレベルの異なる端末が設置されている。学内同士の通信制限は, 異なる種類のサブネット間に適用し, 異なる種類のサブネットを超える通信は, 適宜ファイアウォールを利用したアクセス制限や, UTM 機能の適用を行うこととした。特に事務ネットワークなどでは, 動的 VLAN との連携で, 事務室の場所によらず, 厳しいセキュリティを確保することが容易となった。

本構成を実現するため, VRF (Virtual Routing and Forwarding) を利用したネットワークの仮想化によって, 各地区のコアスイッチを論理分割し, 地区内では異なる種類のサブネット間での通信ができないように構成した。また, 同じ種類のサブネット内での通信は各地区のコアスイッチで折り返すこととなり, 通信遅延や帯域不足が起こらないよう配慮している。

上記のような構成をとることにより, これまでの学内-学外間の通信だけでなく, 学内-学内間の通信にも最低限の制限を加えることが可能となった。さらに, 学内の MAC 認証用サブネットは部局毎に分割されるが, 基本的に地区を超える通信は発生しないことから, 地区間での通信を拒否するようアクセス制限を行った。

2.2.4 ループ検知

これまでは, 機器の機能の問題があり, ループ検知は導入していなかったため, 学内でループが原因のネットワーク停止が発生していた。更新後は, 認証スイッチの全てでループ検知機能を利用することとし, ループを検知した場合, 5 分間検知したポートを閉塞する設定を導入した。

2.2.5 地区間接続

地区間は, 荒牧, 昭和, 桐生, 災害対策 DC 地区と SINET の間は, SINET5 の共同調達により調達した 10Gbps の回

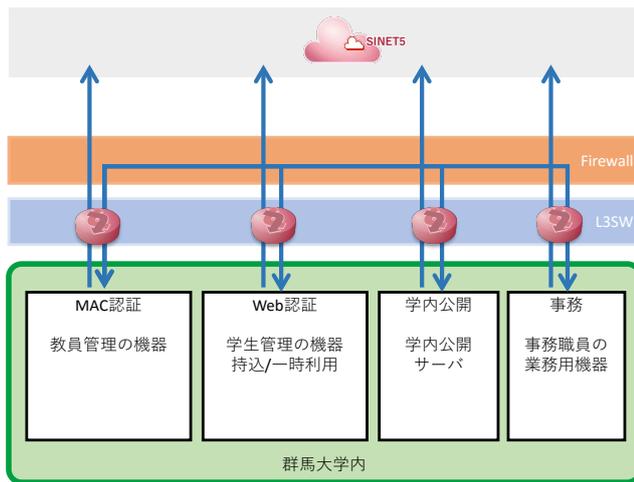


図 2 サブネット分類に基づくネットワーク論理構成

Fig. 2 The network logical structure of GUNet2016 based on the subnet types.

線を利用している。また、小規模地区の太田，上沖，若宮地区と災害対策 DC との間は，KDDI による接続で 100Mbps の帯域が保証されている。

荒牧，昭和，桐生，災害対策 DC 地区と SINET の間の接続には，SINET5 の提供する仮想大学 LAN を利用して複数の VLAN を自由に通過する環境を現在整えている。仮想大学 LAN の利用により，地区間のネットワークをサブネットの種類毎に論理分割することが容易となった。また，将来的には，他のクラウド DC との通信に対しても VLAN による分割を検討しており，その際の VLAN 追加なども従来に比べて容易となることを期待している。現時点では，試験的に国立情報学研究所千葉分館との仮想大学 LAN による接続を申請している。この構成が実現すると，群馬大学のサブネットを国立情報学研究所千葉分館で利用できることとなり，地理的には学外だが，論理的に学内（ファイアウォールの内側）となる構成をつくることことができる。

3. 導入及び運用状況

3.1 導入スケジュール

全学規模のネットワークアクセス認証の導入には，ユーザの協力が欠かせない。失敗すると，ユーザから接続ができないとの苦情が多数寄せられる結果となるため，限られた期間の中で，慎重に導入を行った。また，今回の更新では，総合研究棟などのサブネットを廃止し，各部局のサブネットに収容したため，IP アドレスの変更も伴うものであった。導入スケジュールの概略を表 2 に示す。

荒牧地区には，すでに動的 VLAN が導入されていたため，MAC アドレスの登録の必要もなく，導入はスムーズであった。IP アドレスの変更も伴うものであったが，各自で VLAN ID を変更可能な Web インタフェースを提供していたため，IP アドレスの変更も，各自で実施でき，トラ

ブルなく終了した。

昭和，桐生地区は，今回初めて認証を導入する部局であるため，MAC アドレスの登録が必要となる。導入の 1 ヶ月以上前の 2 月中旬に説明会を開催し，機器登録システムへと MAC アドレスの事前登録を開始した。図 3 に機器登録システムへの MAC アドレス登録状況を示す。赤線は荒牧地区，緑は昭和地区，青は桐生地区の登録状況であり，横軸に日付を，縦軸には，その時点で登録されていた MAC アドレスの総数を示す。

荒牧地区は，従来より認証を導入していたので，MAC アドレスは，一部を除き，従来の旧機器登録システムのデータを段階的に移行している。このため，一括移行作業を実施したときを除いては，変化は緩やかである。3 月 3 日の機器入れ替え後も特に目立って MAC アドレスの登録が増えることはない。

桐生地区は，2 月 19 日に説明会を実施し，3 月 14 日に認証を導入した。説明会実施後に，一旦急激に MAC アドレスの登録が増え，2 月 26 日頃，入試などのせいか一旦登録が落ち着くが，3 月に入ると再び登録が増える。認証導入の 3 月 14 日時点でも全ての MAC アドレスが登録されている様子はないが，一週間後の 3 月 21 日には，新規登録は収まっている。

昭和地区は，2 月 15 日に説明会を実施し，3 月 22 日に認証を導入した。桐生地区と同様に，説明会から 1 週間くらいは急激に登録は増えるが，その後は大きく増えることはなく，3 月から再び登録が徐々に増えていった。この間，ポスター配布なども実施している。しかしながら，3 月 22 日の認証導入後，再び急激に MAC アドレス登録が増えていることから，事前登録が十分に行き渡らないケースがあったことが読み取れる。認証導入後，一週間程度で，大半の MAC アドレス登録は完了し，その後は登録ペースは緩やかとなる。

桐生地区は理工学系のキャンパス，昭和地区は医学系のキャンパスであり，昭和地区は桐生地区の 2 倍程度の規模である。規模の大きさによりアナウンスの難しさがわかる結果であった。しかしながら，当日，事前に更新があるという事実を知らなかったユーザはいなかったため，MAC アドレス未登録に起因するネットワークの問題が発生しても，ユーザは状況を理解しており，激しい苦情を受けることはなかった。

3.2 運用状況

導入以降は，幸いなことに大きな問題は発生していない。今回の更新では，MAC 認証を中心に構成したこともあり，スイッチに大きな負荷はかかるともない状況である。動的 VLAN 設定のため，全スイッチに地区の全てのサブネットを通しており，ブロードキャストの範囲が広がっているため，arp 要求などの負荷が問題になる可能性を懸念して

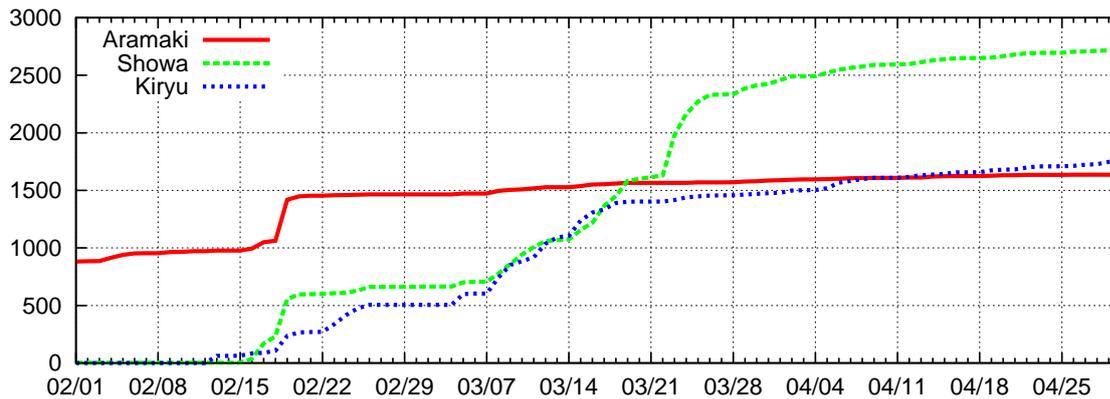


図 3 機器登録システムへの MAC アドレス登録状況

Fig. 3 The number of MAC addresses registered on the device registration system.

表 2 GUNet2016 導入スケジュール概略

Table 2 The schedule summary of the replacement of GUNet2016

日程	作業内容等
2016/01/31	荒牧地区サブネット移行完了
2016/02/15	利用者説明会 (荒牧地区)
2016/02/15	利用者説明会 (昭和地区)
2016/02/19	利用者説明会 (桐生地区)
2016/03/03	SINET5 切り替え
2016/03/03	機器入れ替え (荒牧地区)
2016/03/07-10	機器入れ替え (桐生地区)
2016/03/14	認証導入 (桐生地区)
2016/03/11-16	機器入れ替え (昭和地区)
2016/03/21	機器入れ替え (DC)
2016/03/22	認証導入 (昭和地区)

いたが、こちらも現時点では、問題ないようである。

認証ネットワークの導入により、不正アクセスユーザがなくなったことは一つの成果である。これまでブロードバンドルータの LAN 側が接続されることにより、DHCP サーバとして稼働し、該当するサブネット全てに対しての通信に影響が出ることがあった。しかし、認証ネットワークの導入により、LAN 側の MAC アドレスを登録しない限りこのような接続ができなくなったため、同様のインシデントが発生する可能性は低くなり、更新からこれまで、一度も発生していない。ループ検知機能によるループ接続防止も更新後は無事機能し、これまで、2 回検知があったが、ポート配下以外への影響なく、ループ解消に至っている。

今回の更新で、学内公開サブネットを新たに作ることとなった。本サブネットは他地区への公開を行わない限り、ユーザに影響ないように設計した為、導入時の混乱は防げたものの、本サブネットの存在に気付かずに運用し、本来他地区への公開が必要なものも気づかずに運用されている場合が数件あった。また、動的 VLAN のため、ユーザ毎のサブネットを決定する必要があるが、今後、改組などあった場合、対応が必要となる点も課題の一つと言える。

上記のように、小さな問題はあったが、ユーザからの苦情などはないと言ってよい状態であり、更新は順調に終了し、適切に運用されていると言える。

4. おわりに

群馬大学で、2016 年 4 月より全学的に運用を開始した群馬大学学術情報ネットワーク (GUNet2016) の構成と、その設計、特徴を述べた。本更新により、学内の基幹ネットワークを 10Gbps 対応とするとともに地区間接続、学外接続も 10Gbps にすることで、高速なネットワーク環境を提供できた。基幹部分の機器は全て冗長化し、基幹部分の機器故障に対しても止まらないネットワークの安定性も確保した。さらに、ネットワーク接続時のネットワークアクセス認証と、動的 VLAN を組み合わせた設計により、セキュリティレベルの異なる機器を緩やかに分離したサブネット種別を設けるとともに、異なる種類のサブネットに対しての通信を制御することで、安全性を向上させることができた。

5. 謝辞

本システム構築に多大なご協力を賜りました日立電線ネットワークス株式会社に感謝の意を申し上げます。

参考文献

- [1] 近堂 徹, 田島 浩一, 岸場 清悟, 大東 俊博, 岩田 則和, 西村 浩二, 相原 玲二, "利用者認証機能を備えた大規模キャンパスネットワークの性能評価", インターネットと運用技術シンポジウム 2008, IPSJ Symposium Series Vol 2008, pp.121-128 (2008).
- [2] 岡山 聖彦, 山井 成良, 大隅 淑弘, 河野 圭太, 藤原 崇起, 稗田 隆, "岡山大学における認証・ロケーションフリーネットワークの構築," 学術情報処理研究, no.15, pp.161-165, Sept. 2011.
- [3] 田島浩一, 西村浩二, 近堂徹, 岸場清悟, 相原玲二: ホスト登録を用いたネットワーク認証システムの実装と評価, 学術情報処理研究, No.11, pp.42-49 (2007).
- [4] 浜元 信州, 五十嵐 瑛介, 青山 茂義, 三河 賢治, "ホスト

- 登録システムを利用したネットワークアクセス認証システムの運用” , 情報処理学会研究報告 2010-IOT-9, pp. 1 - 6, 2010
- [5] 志村俊也, 徐浩源: 横浜国立大学「認証ネットワーク」: 運用管理方法の改良, 学術情報処理研究, No.10, pp.81-84 (2006).
- [6] 徐浩源, 大山清, 志村俊也: IP アドレス管理システムの開発と運用, 学術情報処理研究, No.8, pp.79-82 (2004).
- [7] 浜元信州, 青山茂義, 三河賢治: 全学ネットワークアクセス認証システムの導入, インターネットと運用技術シンポジウム 2009, IPSJ Symposium Series Vol 2009, No. 15, pp.1-8 (2009).
- [8] 上田 浩, 井田 寿朗, 青木 正文, 齋藤 貴英, 酒井 秀晃, 伊比 正行, 高橋 仁, 船田 博, 矢島 正勝, 久米原 栄: キャンパス内光直取ネットワークの構築と運用, 学術情報処理研究, No.14, pp.56-63 (2010).