

GUNet2022 でのサブネット小規模化の導入と接続機器の特定について

浜元信州, 井田寿朗, 齋藤貴英, 小田切貴志, 小川康一

群馬大学総合情報メディアセンター

n.hamamoto@gunma-u.ac.jp

Installation of Small-Scale Subnet and identification of connecting devices in GUNet2022

Nobukuni Hamamoto, Hisao Ida, Takahide Saito, Takashi Otagiri, Koichi Ogawa

Library and Information Technology Center, Gunma University

概要

群馬大学で全学ネットワークの更新を行い 2022 年 4 月より GUNet2022 として運用を開始した。GUNet2022 では、高度標的型攻撃で使われることがある横展開への対策として、研究室・部署単位の小規模サブネットを導入するとともにサブネット間のアクセスを禁止する構成とした。サブネットはプライベートアドレスで構成し、大規模 NAT 装置の導入によりグローバルアドレスと時間帯からプライベートアドレスを特定できるよう設計し、elasticsearch に集約したログから端末情報を表示するシステムを開発した。本発表では、GUNet2022 の設計と端末特定に関わる運用について述べる。

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、共同教育学部、情報学部、医学部、及び、理工学部の 4 学部、大学院は、4 研究科、1 学府、2 学環で構成されている。また、生体調節研究所、医学部附属病院を有している。6 地区分散構成であり、共同教育学部、情報学部、及び、事務局本部がある荒牧地区、医学部、医学部附属病院がある昭和地区、理工学部がある桐生地区、理工学部の一部研究室がある太田地区、共同教育学部の附属学校である幼稚園、小学校、特別支援学校がある若宮地区、中学校がある上沖地区からなる。

群馬大学学術情報ネットワーク (GUNet) は、6 地区のキャンパスネットワークと各地区と災害対策データセンタを結ぶ地区間回線及び SINET への学外接続からなる。GUNet は荒牧地区での認証 VLAN や光直収ネットワーク (FTTD) の導入等の先駆的な取組を行ってきた [1]。2016 年には全学一括更新を行い、主要 3 地区 (荒牧, 昭和, 桐生) で認証ネットワークを導入した GUNet2016 となった [2]。その後、老朽化に伴い 2022 年には GUNet2022 へと更新され全地区で認証ネットワークを導入し現在に至っている。

GUNet2022 では、物理構成に関しては、地区間回線

の冗長化、論理構成に関しては、IPv6 アドレスの導入と、研究室や部署を単位とするプライベートアドレスによる小規模サブネット構成への移行を行った [3, 4]。GUNet2016 は、サブネットは部局などの大きな単位で構成されていたが、GUNet2022 ではバックボーンや公開サーバ等はグローバルアドレスとし、研究室、部署サブネットをプライベートアドレスとした。さらに高度標的型攻撃で利用される「横展開」防止 [5, 6] のため、サブネット間のアクセス制限を導入した。これに伴い、研究室・部署サブネットと外部間では NAPT を行うこととした。このための大規模 NAT (CGN) 装置を導入し、NAPT アルゴリズムの調整やログ取得を行うことで、接続機器の特定に支障のないよう運用を行っている。本発表では、GUNet2022 の要件と構成、運用について述べる。

2 関連研究

大学のキャンパスネットワークの構成について各大学で様々な取り組みが行われている。当初、キャンパスネットワークへの接続には認証が要求されることはなかったが、認証スイッチの普及に伴い、2006 年頃から、大学のキャンパスネットワークには MAC アドレス認証及び Web 認証に基づくネットワーク認証が普及してきた [7, 8, 9, 10, 11, 12, 13]。MAC アドレス認証のみを行うもの [7] や、MAC アドレス認証に加

えて、MAC アドレスに基づく VLAN を割り当てる動的 VLAN によるネットワーク [1, 2, 8, 9, 10, 11, 12], さらに IEEE802.1X 認証を利用するものへと発展してきた。一方で、IP アドレス不足や、セキュリティ対策のため大学のプライベートネットワーク化も進んでおり、京都大学の KUINS-III[13] や静岡大学の全面プライベート化 [14], 広島大学の HINET[8, 9, 10] など採用された。ここでは、研究室毎にプライベート IP アドレスのサブネットを導入している。

プライベート IP アドレスでインターネットへの接続を行うには、NAT/NAPT によるアドレス変換が必須だが、NAPT の導入は端末の追跡性を落とすこととなる。つまり、グローバル IP アドレスからプライベート IP アドレスの追跡にセッションログが必要となる上に、グローバル IP アドレスと時間帯の情報のみでは、プライベート IP アドレスを特定できないケースがあり得ることになる。大規模大学ではもともとの IP アドレスが不足するため、研究室等の管理単位を設けて代表者を特定できれば、端末の特定まで行わなくても良いとする運用もある。一方で、小規模大学では NAPT ではなく NAT により追跡性を確保できる。群馬大学を含む中規模以下の国立大学法人では、クラス B のネットワークが割り当てられており、IP アドレス不足の観点からは NAPT 構成とする動機はない。しかし、ネットワークの細分化を行うと、管理上、無駄な IP 割当が増えて IP 不足となるため、NAPT が必要となり追跡不可能な状況になる。本学はこれが理由でネットワークを細分化できずにいた。GUNet2022 ではこの点を克服するため、NAT アルゴリズムを見直すことで、端末の追跡ができるネットワークとした。

3 研究室・部署サブネットの管理

小規模サブネットを導入するにあたり、どの程度の規模のサブネットを準備するかが問題となる。大学での小規模な単位としては、研究室、事務組織での課や係、病院での診療科等が考えられるが、これらの単位は部局内での情報であり、総合情報メディアセンターで把握することは難しい。このため、部局管理者として、部局単位でネットワーク管理者を置き、部局管理者が小規模な単位（グループ）を決める管理体制とした。さらに、研究室・部署サブネットには、正管理者、副管理者、メンバを置いた体制とした。つまり、図 1 のように、研究室・部署単位のグループを作成し、このグループに対して研究室・部署サブネットを割り当てる行う事とした。グループには管理者やユーザを複

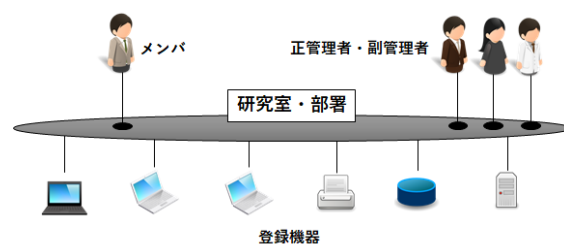


図 1 GUNet2022 での機器管理

数割り当てることができる。これにより、元々機器を管理していたユーザが退職したとしても、残りのメンバで管理を継続することができるようになった。

表 1 に、正管理者、副管理者、メンバの権限を示す。グループ内の機器登録権限を持つのは正管理者、副管理者とした。また、グループに所属する正管理者、副管理者、メンバは VPN 経由で研究室ネットワークに接続できるようにした。正管理者は、グループ内の人員を把握して機器登録を行なうユーザを指名する方を想定しており、教職員に限定した。正管理者は副管理者を指名する権限がある。副管理者はグループ内の機器を把握し、機器登録等の実務を行う方を想定しており、正管理者の指名した方とした。なお、副管理者は教職員だけでなく学生でも構わない。また、正管理者、副管理者は、メンバを指定する権限を持っており、メンバは教職員でも学生でも構わないものとした。なお、ユーザは複数グループの正管理者、副管理者、メンバを兼ねることもできるようにした。全体管理者、部局管理者の持つ権限を表 2 に示す。総合情報メディアセンターは全体管理者として、全ての研究室・部署サブネットへの正管理者登録をはじめとする全ての操作が可能である。また、部局管理者は、自身の所属する管理部局のサブネットに対して管理権限を有している。サブネットの部局への割り当ては、全体管理者のみが可能である。GUNet2016 では部局毎にグローバル IP アドレスでのサブネットを複数準備した。GUNet2022 でも同様に、部局毎に十分な数（教員数程度）の研究室・部署サブネットを準備し、全てのネットワーク機器に設定した上で、導入時に全体管理者が各部局にサブネットを割り当てた。部局管理者は、割り当てられたサブネットに対する管理権限を有し、研究室・部署サブネットの正管理者、副管理者、メンバを登録することができる。また、管理権限を持つサブネット所属している機器の登録、削除権限を有するほか、登録機器のサブネットを部局に所属する研究室・部署サブネットから選んで変更する権限も有する。

表 1 登場人物と権限

権限	正管理者	副管理者	メンバ
副管理者の指定	可		
メンバの指定	可	可	
機器登録・編集・削除	可	可	
サブネットへの VPN アクセス	可	可	可

3.1 機器登録システム

管理権限を上で述べたグループ単位での管理を実現するため、機器の MAC アドレスを Web インタフェースから登録する機器登録システムを開発した [3]。MAC 認証を利用したい場合には、管理者が「機器登録システム」にログインして MAC アドレスの登録を行う。この際に「グループ」も選択する。グループは各部局で決定した研究室や部署に相当し、MAC アドレス認証後に収容される研究室・部署サブネットの VLAN が対応している。なお、複数の部局の組織を兼任するユーザがいるため、ユーザは複数のグループに所属できるようにしている。ユーザは MAC アドレス登録の際にどのグループに機器を紐づけるか選択できる。また、異なるグループ間で通信をしたい場合には、学内から VPN 接続することで、機器の所属するグループとは異なるグループへアクセスできるようにしている。機器登録システムで、ユーザは自身の所属するグループから VPN 接続でアクセスできるグループを 1 つ選ぶことができる。

4 GUNet2022 の構成

図 2 に GUNet2022 の物理構成の概要に示す。各地区のコアスイッチは、データセンタ（DC）のコアスイッチと接続されている。この接続は冗長化されており、荒牧、昭和は 10Gbps を 2 つ束ねた LAG 構成、若宮、上沖地区は、1Gbps を 2 つ束ねた LAG 構成である。桐生、太田地区は、DC と 3 地点で 10Gbps のリング構成とした

データセンタには、大学全体のルーティングを行うコアスイッチを置いている。プライベートネットワーク導入に伴う NAT 機能を提供する CGN 装置と、学外接続用 FW もデータセンタに配置している。また、図では省略したが、データセンタと SINET、各地区の接続に利用する対外接続用 L3 スイッチをデータセンタに配置しており、SINET6 とはデータセンタ接続冗長化サービスにより BGP で冗長化接続している。各地区のネットワークは、荒牧地区は FTDD 構

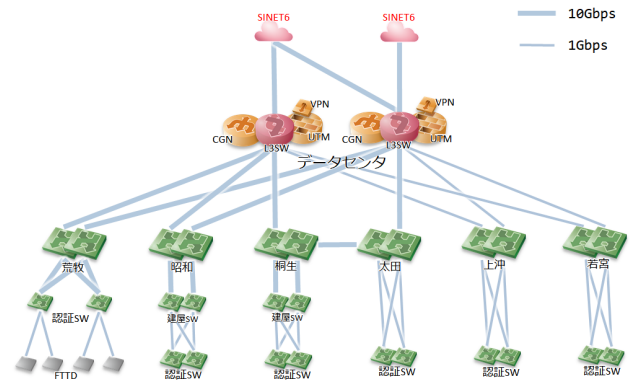


図 2 GUNet2022 物理構成概要図

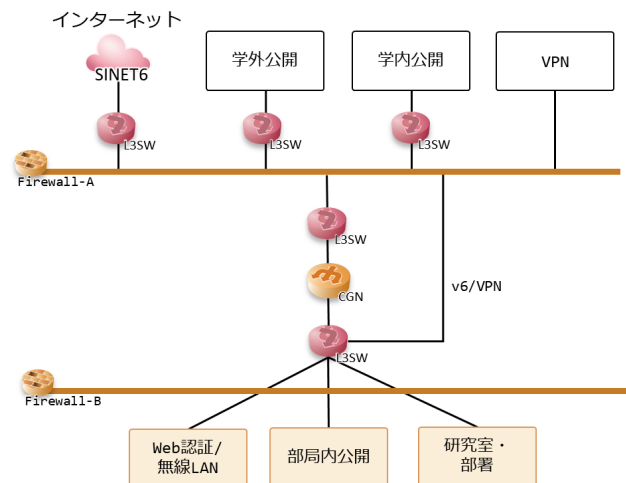


図 3 GUNet2022 論理構成概要図

成としており、サーバ室の認証スイッチは、各居室に置かれたメディアコンバータに 1000BASE-LX で接続されている。ユーザ側には 10BASE-T/100BASE-TX/1000BASE-T の UTP 接続を提供している。その他の地区は、各フロアの認証スイッチが各部屋に対して UTP 接続を提供し、上流は各建屋スイッチまたはコアスイッチに冗長化接続されている。

GUNet2022 の論理構成の概要を図 3 に、サブネット間のアクセス制限の概要を図 4 に示す。サブネットの種類は学外公開、学内公開、部局内公開、研究室・部署、Web 認証/無線 LAN に分かれている。サブネッ

表 2 管理者と権限

権限	全体管理者	部局管理者
サブネットの部局への割り当て	可	
正/副管理者、メンバの指定	可	管理部局のみ可
機器登録・編集・削除	可	管理部局のみ可
機器の割り当てサブネット変更	可	管理部局のみ可

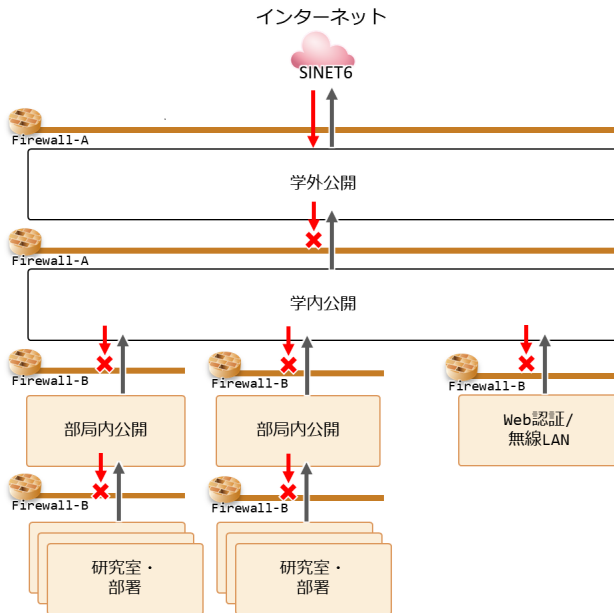


図 4 GUNet2022 アクセス制限概要図

ト間の通信はファイアウォールを経由し、図 4 に示すアクセス制限を設けている。また、研究室・部署、Web 認証/無線 LAN はプライベートアドレスで構成されており、これらのサブネット外と通信する際には CGN 装置を経由し、NAPT による IPv4 アドレスの変換を行っている。なお、IPv6 アドレスは、すべてのサブネットでグローバルアドレスでの運用としている。研究室・部署サブネットではサブネット間の通信を拒否している。また、研究室・部署サブネットは部局に属しており、対応する部局内公開サブネットへの通信は許可している。

GUNet2022 では情報コンセントに接続するには、MAC アドレス認証、または、Web 認証が必要となる。Web 認証の場合はウェブブラウザを開き、群馬大学の全学認証アカウントでログインして接続する。認証機能は認証スイッチ（ALAXALA 社製 AX2530）及び認証サーバ（FreeRADIUS, MariaDB）により実現している。MAC アドレス認証された機器は、機器登録システムで指定された MAC アドレスに紐づく VLAN に応じて適切なサブネットに収容される。

学内公開、学外公開サブネットは、学外公開する Web サーバ、複数の研究室から接続するサーバやプリンタ、学生が講義のために接続するサーバなどが収容されている。ここに機器を配置する場合は、ユーザからの申請を受けて、総合情報メディアセンターで MAC アドレスに対応する VLAN を手動で変更する。

無線 LAN への接続には、Web 認証または PEAP による IEEE802.1X 認証が必要となる。認証は、無線 LAN 接続端末からの通信が、無線 LAN コントローラにトンネルされて、コントローラで行われる。接続が許可された端末は、GUNet2022 の無線 LAN のサブネットへ接続するよう構成されている。

VPN 接続のサブネットについては、図 4 の制限とは別にログインしたユーザの所属する研究室・部署サブネットへのアクセスができるようにしている。ただし、複数の研究室・部署サブネットに属する場合はユーザの選んだ 1 つのサブネットに限定している。この機能は、VPN を提供している UTM 装置で、ユーザが機器登録システムで指定したサブネットの VLAN ID を定期的に LDAP から取得し、ログインしたユーザに対応する VLAN を許可する ACL を適用することで実現している。

5 サブネットの小規模化

全学で、研究室・部署サブネットを構成する場合には、十分なサブネット数を準備する必要がある。群馬大学の規模は、教員数は約 1,000 人であるため、全員が個人研究室としても 1,000 程度のサブネットを準備すればよい。サブネット数は最大 2,000 を提供できるよう設定し、必要な場合は VLANID の規格上の上限（4,096）程度まで拡張可能な構成とした。群馬大学はクラス B のグローバル IP アドレスのネットワークを所有しているが、1,000 程度のサブネットを提供するには、一律に /24 のサブネットを提供することはできず、研究室の規模に応じて想定する接続機器数を見積もり、研究室毎に適切な大きさのサブネットとする必要がある。しかしながら、このような大きさの調整を

1,000 近くのサブネットに対して行うことは現実的ではないため、GUNet2022 では、大きさを/24 に固定したプライベート IP アドレスのサブネットを準備した。その結果プライベート IP アドレス数はグローバル IP アドレス数を超えるため、NAT ではなく、NAPT 構成とした。

実際に導入されたサブネットの規模を確認するため、MAC アドレス登録されている機器数をサブネット毎（グループ毎）に集計した。図 5 の下段に移行が完了した 2023 年 4 月 1 日時点での研究室・部署サブネットの登録機器数の分布を示す。横軸は登録機器数を 10 毎に区切った階級を、縦軸はその階級に属するサブネット数を示している。

図 5 の上段は、GUNet2022 移行開始前である 2022 年 5 月 1 日時点での GUNet2016 のサブネットに登録された登録機器数の分布を示す。各グループには/24 のサブネットが割り当てられているが、動的に IP アドレスを割り振るのは最大 191 個とし、残りの部分は必要に応じてグループ内で固定 IP アドレスを割り当てる方針とした。図 5 の上段を見ると、更新前のサブネットでは、動的に割り当てられる IP アドレスの上限 191 を超えたサブネットが多数あることがわかる。このようなサブネットでは、利用者が多い時間帯では一部の端末で IP アドレスが取得できず接続できなくなっていた。一方で、GUNet2022 移行後である図 5 の下段を見ると、グループに含まれる MAC アドレスはほとんどが 20 以下となっていることが分かる。MAC アドレスが 40 を超えるグループもあるが少数となる傾向である。更新により研究室・部署単位としたことで、全体のサブネット数が増加するとともにサブネットあたりの機器登録数は減り、小規模サブネットが実現していることが分かる。

5.1 NAPT 配下の機器特定

大学のネットワークでは、セキュリティインシデント対応のため、グローバル IP アドレスと指摘された時間帯から、迅速に端末を特定することが求められている。NAPT 構成にした場合、グローバル IP アドレスに対応するプライベート IP アドレスが複数となるため、端末を 1 つに特定できなくなる。その場合、複数の端末を調査することになるが、これは単なる手間だけでなく、利用者にあらぬ疑いをかけることにもなり、運用上の問題となる。この問題点が群馬大学で NAPT 構成を採用しない理由の一つとなっていた。

しかしながら、群馬大学は大規模大学とは異なり、端末数は 10,000 程度に収まっている。この場合、NAT

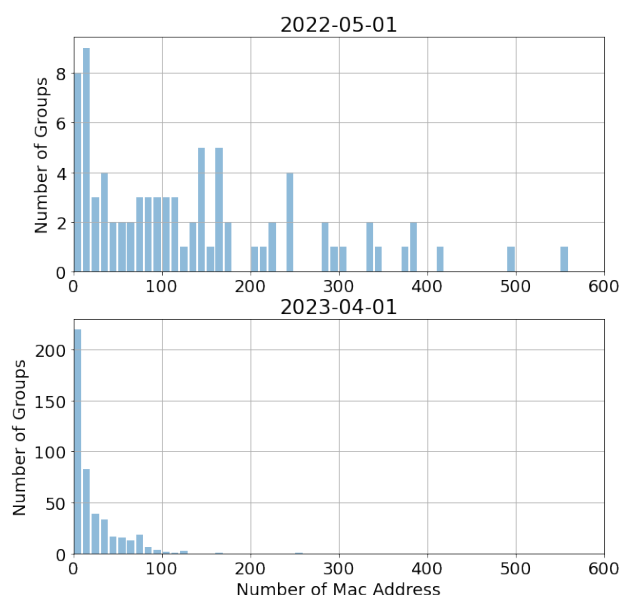


図 5 MAC アドレス数毎のサブネット数分布。下段は 2023 年 4 月 1 日時点の研究室・部署サブネットのもの、上段は 2022 年 5 月 1 日時点の GUNet2016 のサブネットのものを示す。

装置で内部 IP アドレス（プライベート IP アドレス）と外部 IP アドレス（グローバル IP アドレス）の対応アルゴリズムが適切であれば、内部サブネットの方が大きい NAPT 構成でも、外部 IP アドレスに対応する内部 IP アドレスを 1 つにすることが可能となるはずである。GUNet2022 では CGN 装置を導入し NAPT アルゴリズムを工夫することで、内部アドレスを 1 つに特定できるように設計を行った。具体的には、外部 IP アドレスの選択アルゴリズムとして、今回導入した A10 の機器では、以下が選択できる。

1. ランダム
2. ラウンドロビン
3. 最小 used port
4. 最小 reserved port
5. 最小 user
6. Fixed-NAT(Deterministic NAT)

大規模 NAT 装置は、通常はグローバルアドレスを節約するために利用されるため、1 つの外部 IP アドレスに極力多くの内部 IP アドレスを重ねるように NAPT される。つまり、IP アドレスあたりのポート数 (65,535) を使い切るまでは、新たに外部 IP アドレスを割り当てることがない。(1), (3), (4) ではそのような振る舞いをする。

(2) のラウンドロビンでは、新たに内部 IP アドレスからの通信があった際には、最後に割り当てた外部 IP

アドレスの次の IP アドレスを割り当て、外部 IP アドレスが範囲の最後に到達した場合には、最初の外部 IP アドレスに戻って割り当てるアルゴリズムとなる。(6) の Fixed-NAT(Deterministic NAT) は、予め、外部 IP アドレス/ポートと内部 IP アドレス/ポートの対応を固定しておく方式である [15]。この場合は、固定方法が静的となるため慎重に対応を検討しないとポート不足が発生する可能性があると判断して採用を見送った。(5) の最小 user では、NAT セッションで外部 IP アドレスに対応する内部 IP アドレス数を最小にするようにプールアドレスから外部 IP アドレスを選択する。GUNet2022 ではこの方式 (5) を利用することとした。

方式 (5) では、準備した外部 IP 数に対して内部 IP 数が多くなければ、外部 IP に対する内部 IP は 1 つになる。しかし、外部 IP が頻繁に再利用されると、外部 IP に対して内部 IP が頻繁に変わるため、指定した時間帯が広いと内部 IP 特定に支障をきたす。このため、UDP,ICMP に対しては、7,320 秒通信がなくても NAT セッションを維持するようにした。TCP に対しては、通常の NAT セッションは FIN を受け取ると終了する。Full-Cone の NAT の場合は FIN が来てもセッション維持するため、80 と 1024 以上のポートに対して、Full-Cone NAT のセッション維持時間を 3,600 秒（機器の上限）とした。この設定で群馬大学の環境で運用した結果、時間帯を 2 時間以内に絞ることができれば、一部の例外を除いて、グローバル IP に対してプライベート IP アドレスが 1 つに決まるようにすることができた [4]。

6 端末検索システム

近年の UTM のログは膨大になり検索にも時間がかかる状況である。このため、ログサーバ上で elasticsearch によるログデータベースを構築した。ネットワーク機器のログはログサーバに蓄積するよう構成したが、さらに fluentd により構造化されたうえで、elasticsearch に投入される。データベースへの投入により、ログの検索性能は格段に向上した。

ログサーバは、認証スイッチ、無線 LAN 等のログが蓄積されるログサーバ#1、UTM 装置のログが蓄積されるログサーバ#2 からなる。表 3 に、今回導入したログサーバのスペックと対象となるログを示す。ログサーバは VMWare 社の esxi 仮想マシンとして構成され、CPU は Intel 社製 Xeon(R) Gold 6230 2.10GHz、ディスク容量は#1 が 1TB、#2 が 2TB メ

	メモリ	HDD	対象機器
ログサーバ#1	8GB	1TB	L2SW(mac 認証) L2SW(mac 認証) L3SW CGN(NAPT) 無線 LAN
ログサーバ#2	16GB	2TB	UTM(traffic) UTM(VPN)

表 3 サーバ構成

モリ容量は#1 が 8GB、#2 が 16GB である。蓄積されるログは、ログサーバ#1 に L2SW、L3SW、CGN、無線 LAN のログを、ログサーバ#2 に UTM のログを蓄積している。UTM 装置のログには、通信のログの他に、VPN の認証ログも含んでいる。蓄積したログは fluentd で構造化され、サーバ内の elasticsearch に蓄積される。各サーバでログ検索には kibana を利用できるようにしている。また、これらとは別に、IP アドレスと MAC アドレスの対応を取るため、L3 スイッチの arp テーブルおよび ndp テーブルを 1 時間間隔で取得してログサーバ#1 の elasticsearch に保存している。

図 6 に端末検索システムの検索画面を示す。IP アドレスと時間帯を指定すると、その時間に関連する端末やログの情報を表示するように構成されている。具体的には以下のような流れで検索を行っている。特に記載のない限り検索は elasticsearch に対して検索を行っている。

1. グローバル IP アドレスと時間帯を指定して検索を指示
2. UTM ログを IP アドレスと時間帯で検索する
3. NAT ログをグローバル IP アドレスと時間帯を指定して検索し、プライベート IP アドレス群を特定する。
4. 見つかったプライベート IP アドレスすべてに対して以下の検索を繰り返す。見つからない場合はグローバル IP アドレスで検索する。
 - (a) UTM ログを IP アドレスで検索しログを表示：通信の有無を確認
 - (b) arp のログを IP アドレスで検索しログを表示：MAC アドレスを特定
 - (c) 機器登録システムの MariaDB を MAC アドレスで検索する：機器の管理者等を特定

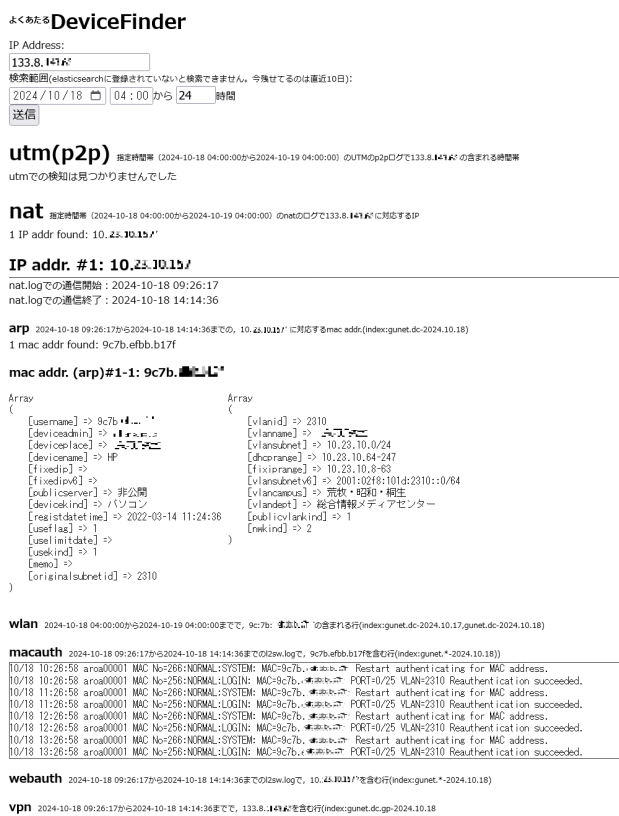


図 6 端末検索システムの検索画面

- (d) 無線 LAN のログを MAC アドレスで検索しログを表示：ユーザ ID を特定
- (e) MAC 認証のログを MAC アドレスで検索しログを表示：接続スイッチポートを特定
- (f) Web 認証のログをプライベート IP アドレスで検索しログを表示：ユーザ ID, 接続スイッチポートを特定
- (g) VPN のログをグローバル IP アドレスで検索しログを表示：ユーザ ID を特定

本検索システムにより，グローバル IP アドレスを指定した際に端末を特定できる．検索にかかる時間は数秒程度となっており，grep 等で複数ファイルを検索するのに比べると格段に早い．このシステムは，インシデント時の追跡や，UTM 装置で検知された P2P 通信の特定のために利用されている．

7 むすび

本発表では，2022 年度に更新した群馬大学学術情報ネットワーク（GUNet2022）で導入した研究室・部署単位でのサブネットの小規模化を中心に記載した．導入にあたっては，小規模サブネットの管理の部局への

移行，研究室・部署等の管理単位の構成，機器登録システムの開発などを経て実施した．サブネットはプライベートアドレスで構成され，サブネットに登録された MAC アドレスは 20 以下がほとんどとなり，サブネットの小規模化が実現した．さらにサブネット間のアクセスを禁止していることから，横展開を防ぐこととなり，ネットワークの安全性も向上した．

プライベートアドレスの導入に伴い，NAPT によるアドレス変換を行った．NAPT を導入すると，グローバル IP に対応するプライベート IP アドレスが「複数現れる」または「頻繁に変化する」ことにより，グローバル IP アドレスからプライベート IP アドレスを特定することが難しくなる点が問題であった．GUNet2022 では CGN 装置に搭載された最小 user となるアルゴリズムを利用するとともに，NAT セッションのパラメータを調整して，2 時間程度に時間を絞ることができれば，グローバル IP アドレスに対応するプライベート IP アドレスを一つすることができた．このことにより，ネットワーク関連のログを elasticsearch に集約し，グローバル IP アドレスと時間帯から，接続機器情報を迅速に検索するシステムを開発し，インシデント時の追跡も支障なく行えるネットワークを構築できた．

謝辞

広島大学全学ネットワーク HINET に関する情報提供を頂いた近堂 徹博士に感謝申し上げます．機器登録システムの開発にご尽力いただいた株式会社アイクルの皆様，GUNet2016 及び GUNet2022 の構築にご協力いただいた株式会社エイチ・シー・ネットワークスの皆様に感謝の意を申し上げます．

参考文献

- [1] 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，“キャンパス内光直収ネットワークの構築と運用”，学術情報処理研究，Vol.14, pp. 56–63 (オンライン)，DOI: 10.24669/jacn.14.1 56(2016)．
- [2] 浜元信州，井田寿朗，齋藤貴英，酒井秀晃，小田切貴志，横山重俊，“動的 VLAN を利用した全学認証ネットワークの構築”，学術情報処理研究，Vol. 20, pp. 65–74 (オンライン)，DOI: 10.24669/jacn.20.1 65 (2016)．
- [3] 浜元信州，小川康一，井田寿朗，齋藤貴英，小田切貴志，綿貫明広，“全学認証ネットワークの運用

- を支える機器登録システムの開発”, 学術情報処理研究 Vol 26. No.1, pp. 10-19 (オンライン), DOI: 10.24669/jacn.26.1 10 (2022).
- [4] 浜元信州, 井田寿朗, 齋藤貴英, 小田切貴志, 綿貫明広, 小川康一, “全学認証ネットワークのサブネット小規模化とその運用”, 情報処理学会論文誌 Vol. 65 No. 3, pp 623–634 DOI: <http://doi.org/10.20729/00233241> (2024)
- [5] Hutchins, E. M. Cloppert, M. J. and Amin, R.M., “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains”(online), 入手先 (<https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf>) (参照 2024-08-09) .
- [6] 情報処理推進機構, “「高度標的型攻撃」対策に向けたシステム設計ガイド”, 入手先 (<https://www.ipa.go.jp/files/000046236.pdf>) (参照 2024-08-09) .
- [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 論文集, Vol. 2009, pp. 1–8, (2009).
- [8] 相原玲二, 西村 浩二, 近堂 徹, 岸場 清悟, 田島 浩一, “全教員に個別ファイアウォール機能を提供するキャンパスネットワークの構築”, 情報処理学会研究報告, Vol. 2008-IOT-002, No. 72, pp. 29–34, (2008).
- [9] 近堂徹, 田島浩一, 吉田朋彦, 岸場清悟, 岩田則和, 西村浩二, 相原玲二, “アクセス制限機能を提供するキャンパスネットワークの実装と評価”, 学術情報処理研究, Vol.21, pp. 36–43 (オンライン), DOI: 10.24669/jacn.21.1 36(2017).
- [10] 近堂徹, 田島 浩一, 岸場 清悟, 岩田 則和, 相原 玲二, “自動構成機能を有する大規模キャンパスネットワーク管理システムの実装と評価”, 情報処理学会論文誌, Vol. 57 ,No. 3, pp. 98–1007, (2016).
- [11] 小川康一, 吉浦紀晃, “埼玉大学における光ファイバ直収型ネットワークの運用経験について”, 情報処理学会研究報告, Vol.2015-IOT-30 No.10, pp. 1–8, (2015).
- [12] 阿多信吾, “キャンパスネットワークにおける異常の予兆検知に向けたデータ分析”, 情報処理学会研究報告, Vol.2018-IOT-41, No. 7, pp. 1–6, (2018).
- [13] 高倉弘喜, 江原康生, 宮崎修一, 沢田篤史, 中村素典, 岡部寿男, “安全なギガビットネットワークシステム KUINS-III の構成とセキュリティ対策”, 電子情報通信学会論文誌 Vol.J86-B No.8 ,pp. 1494-1501, (2003).
- [14] 長谷川孝博, 望月邦昭, 高橋秀年, 高田重利, 井上春樹, 八巻直一, “全学プライベート IP 網の構築と運用”, 学術情報処理研究, Vol 10, No 1, pp. 29-38, DOI: 10.24669/jacn.10.1_29 (2006)
- [15] Donley, C., Grundemann, C., Sarawat, V., Sundaresan, K., and O. Vautrin, “Deterministic Address Mapping to Reduce Logging in Carrier-Grade NAT Deployments” , RFC 7422 (online), DOI: 10.17487/RFC7422 (2014).