キャンパス情報ネットワークシステム(NUNET)の更改について

柳生　大輔（情報基盤デザイン部門）

1. はじめに

近年、大学の教育・研究・事務等の全ての活動において、ICT 技術やデジタルデータを利活用した、効率化および質的向上（大学 DX）が重要になっています。これらを支える環境の一つとして、利便性とセキュリティを兼ね備えたネットワーク環境が求められていることから、ICT 基盤センター（以下、「本センター」とします。）では、情報セキュリティ対策の強化、キャンパス情報ネットワークの性能やサービス、信頼性の向上を目的として、キャンパス情報ネットワークシステム（以下、「新システム」とします。）の更改を行い、令和 2 年 10 月より運用を開始しました。

更改に関しては、文献[1],[2]にその詳細を記しておりますが、本稿では、その概要について紹介いたします。

2. 導入の背景

2.1. キャンパス情報ネットワークシステムの歴史と運用

本学では、キャンパス情報ネットワークシステムを「NUNET」と名付けています。NUNET は、構成員約 13,500 人が利用する、本学の教育、研究、事務等（病院の医療業務を除く）さまざまな業務を支える基盤です。管理 UTP ポート数は約 9,000 ポート（本更改時点、病院内を除く）に及びます。NUNET の管理規則においては、管理区分として、（基幹 LAN に接続する）部局内のネットワークを意味する「部局 LAN」、すべての部局 LAN や学外への上位ネットワークを接続するための中継機器、通信ケーブルや監視装置等を意味する「基幹 LAN」に分かれています。ネットワークの安定稼働に必要なさまざまな業務を、機器や配線等からなるネットワークの稼働を「維持」する業務、利用者や IP アドレス等を「管理」する業務に分けたとき、管理規則上は、部局 LAN については各部局、基幹 LAN については本センターがそれぞれ「維持」「管理」を行うことになっています。

「管理」として重要な業務に、各機器への IP アドレスの割り当てと接続認証の仕組みの運用があります。管理規則上は、部局 LAN 管理者（部局長）が、接続の可否を判断し、許可した場合には利用者（機器）に IP アドレスを割り当てる、という運用になっています。また、教室等のような開放箇所においては利用権限を有しているかを認証等により確認する必要があります。マルウェア感染などインシデントが発生した際、このアドレス割当情報や認証情報により感染した機器や利用者を特定することになるため、これらの情報が適切に管理されていなければ、迅速な対応を行うことができません。

前述の（特に部局 LAN の）「維持」「管理」を実務的に担う者として、部局 LAN 管理者から部局 LAN 管理運用担当者（多くは教育職員）が指名されていますが、その業務は多くはボランティアとして位置づけられているのが現状であり、また、業務多忙やスキルの差から、障害やトラブルが発生しても、十分な対応が行えていないのが実情でした。

そこでまず、平成 22 年 4 月運用開始のキャンパス情報ネットワークシステム（以下、「前システム」とします。）において、「維持」（機器の維持（障害対応）や通信トラブルの調査・対応）については、

全学的に本センターが対応することとしました。

コンピュータネットワークが業務の基盤から生活の基盤に変化した現在、業務や学習の DX に伴い、より利便性とセキュリティを兼ね備えたネットワーク環境が求められています。この要求に応えるためには、「管理」の部分を高度化・効率化する必要があります、そこで、新システムでは、単に機器の更改ではなく、ネットワーク構造の変更や管理機能を強化したネットワークシステムへ更改しました。

表 1：NUNET の整備の歴史

稼働年度	基幹 NW プロトコル	財源	部局 LAN「維持」	部局 LAN「管理」
平成 6	FDDI	補正予算	部局	部局
平成 8	ATM	補正予算	部局	部局
平成 13	GbE	補正予算	部局	部局
平成 22	10GbE	自己財源	センター	部局
令和 2	10GbE	自己財源（リース）	センター	センター

新システムの要素項目については、次章以降で述べますが、3.2 に示すマイクロセグメンテーション、3.5 に示す統一認証環境及びネットワーク一元管理装置の導入及び 3.6 に示すフロー情報を用いたインシデント検知システムの導入により、NUNET の「管理」の部分のほとんどを本センターが全学的に担当できるようにしました。

2.2. これまでのネットワークシステムにおける問題点

本学においては、ネットワーク管理単位の分割、自由な研究活動環境を提供する観点、学外からインシデント情報の提供を受けた場合の即応性から、歴史的に（機密性の高い情報を取り扱う箇所を除き）学内の研究・教育領域のネットワーク環境においては、グローバル IP アドレスを使用してきました。

もちろん、学外からの脅威を防御するため、学外と学内の境界等の重要ポイントにはファイアウォール（以下、「FW」とします。）を設置していますが、構成上、このポイント(FW)を通過するトラフィックのみにより通信制御されることになります。

これまで本学においては、学部をまたいだ複合領域研究等の形もあることなどから、学内部分においては、ネットワークの障壁をほぼ設けていませんでした。また、歴史的な経緯から、学外から利用できる研究用のサーバ等も各部局のネットワークに接続されています。このため、一度学内に脅威が入ってしまうと、その影響は容易に拡大してしまいます。したがって、扱える情報を限定し、被害極限を実施するためには、細かく障壁（パーティション）を設置する必要があります。

また、ネットワークの構造上の問題による「別研究室から自研究室のプリンタに出力された」「ネットワークに接続するための情報を手動設定せねばならず煩雑」などの状況を回避するため、利用者により簡易的な FW 機能・研究室用の無線 LAN アクセスポイント（以下、「AP」とします。）を兼ねたブロードバンドルータ（以下、「BBR」とします。）が設置されていることが少なくありませんでした。この場合、部屋をまたがってネットワーク（情報）を共有することが困難であったり（さらには、本センター管理外の LAN ケーブルが増え建屋改修の支障に）、古くなった BBR 等が障害の原因となっ

たり攻撃の対象となったりすることが避けられませんでした。また、インシデントを検知した際、インシデントが発生した端末が収容されている BBR は特定できても、その内部のどの端末であるのかの特定は（本センター側からは）困難でした。

新システムでは、集合型の NAT 装置を導入し、講座・研究室・部課等へプライベートネットワーク環境を提供することにしました。詳細は 3.2 で後述します。

2.3. 新システムの構造

図 1 は、更改後の本学のキャンパス情報ネットワークの構造の概要を示しています。更改後は、仮想 FW 機能を用いて新たにゾーニングを実装するとともに、サンドボックス機能や URL フィルタリング機能を稼働させ、ネットワークを介した情報セキュリティの向上を図っています。詳細は、3.1 で述べます。

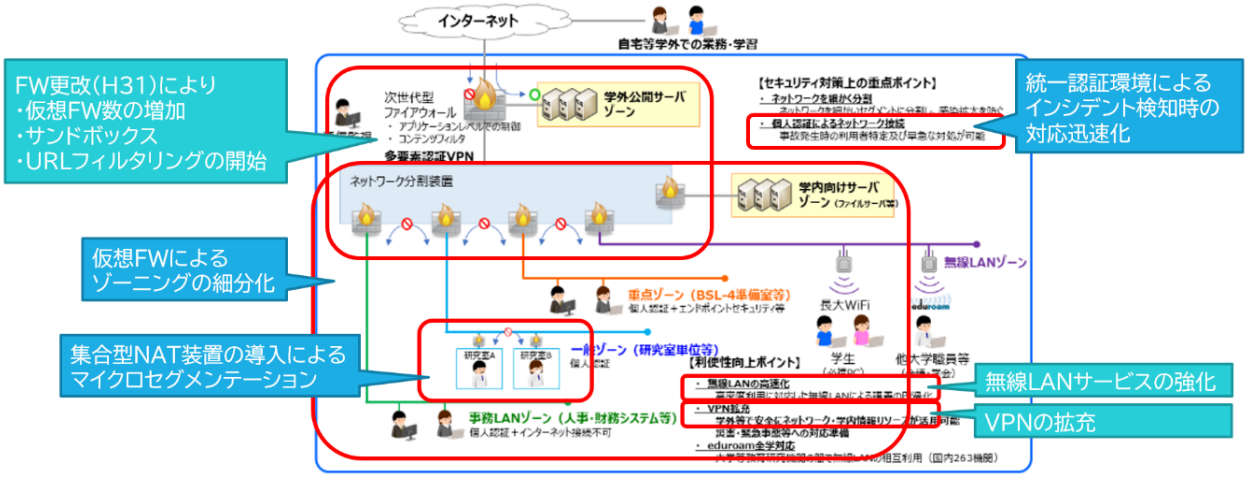


図 1：更改後のキャンパス情報ネットワークシステムの構造

3. 新システムにおける新機能・強化ポイント

3.1. ゾーニング・パーティショニング

表 2：ゾーニング計画

ゾーン名称	ゾーンの概要
学外公開サーバゾーン	学外からのコネクションを受け入れるホストを設置。他ゾーンのコネクションは不許可
学内グローバルアドレスゾーン	グローバルアドレスを使用するホストを設置。部局の共同プリンタ等のデバイスに使用。大まかな部局ごとに一方向のファイアウォールを設置
学内公開サーバゾーン	学内にのみ ICT サービスを提供することを意図するホストを設置。情報漏洩の阻止のため、このゾーンから学外への通信はアップデート等の通信を除き原則許可しない
個別 NAT ゾーン	研究室、講座、部課係等の単位を基本として提供するプライベートアドレス空間。異なる個別 NAT の内側間では通信を許可しない
ハイセキュアゾーン	特に高度な情報管理が必要な端末を設置。エンドポイントセキュリティソフトウェアの導入を必須とするなど、高度なセキュリティを提供
教育系ネットワークゾーン	教室、会議室等不特定多数が入室しうる場所で使用。収容人員が同時に無線 LAN を快適に使用できることが必要である。各教室の情報コンセントもこのゾーンに収容
ゲストゾーン	「教育系ネットワークゾーン」と同様であるが、本学構成員以外のゲストが使用するため、学内のリソース等へはアクセスできない。eduroam 等を含む

新システムにおいては、これまで、学外・学内・講義用無線 LAN、事務情報程度の区分しかなかったネットワークのゾーニングを細分化し、FW 等で分離することにより、万が一機器への侵入やマルウェア感染等のインシデントが発生した場合でも、影響する範囲を局所化し、不適切な情報の取得ができない構造としました。構成・通信可否の絵的わかりやすさを重視し、穴開け等の例外（個別）設定を行わないことによる事故防止も意図しています。

移行については、IP アドレスの付け替えが必要となることから、システムとして納入されたサーバ等については、リプレイスのタイミングで移行するなど、順次行っていきます。

3.2. プライベートネットワーク環境の提供（マイクロセグメンテーション）

本学では、部局 LAN 内の IP アドレス管理を、各部局に委任しています。また部局内では、メリットもあるとは言え、同じセグメント（broadcast が届く領域）が使用されています。このため、

・隣の研究室の学生から、自研究室のプリンタに出力された
・「ネットワークコンピュータ」で見える端末が多すぎる
・端末を買い換えた際、ネットワークに接続するための情報を手動設定せねばならず煩雑
・割り当てられた IP アドレスが少なく、希望の台数をネットワークに接続できない

などの状況が発生しており、この状況を回避するため、各研究室等において、無線 BBR が設置されていることが少なくありませんが、前述のとおり独自に BBR を設置される形態は、ネットワーク管理の点からは必ずしも好ましくありません。

そこで新システムでは、マイクロセグメンテーションの機能を実装し、プライベートネットワーク環境の提供を開始しました。

具体的には、Cisco Systems 社 ASR1000 型アグリゲーションサービスルータにより、講座・研究室・部課等の単位で閉じたプライベート IP アドレスを用いるネットワーク環境を提供し、アドレス変換を行います。また、本環境内において DHCP サービスを提供し、DHCP のリース記録やアドレス変換記録については、本センターが一定期間保管します。また、ネットワークシステム全体としてネットワーク機器を流れるトラフィックのフロー情報を収集しており、3.6 に示すインシデント検知システムとの連携により､学内全体の通信の把握やインシデント発生時の即応が可能となっています。これらにより、

・他研究室等から、自研究室等のネットワークおよび接続された機器を秘匿・防御が可能
・部屋をまたがって同じプライベートネットワーク環境を利用可能
・マルウェアが検知された場合でも端末の特定ができ、被害を最小限にとどめることが可能
・DHCP サービスを提供し、IP アドレスは自動取得（固定 IP アドレス使用も可能）
・使用できる端末・デバイス数（IP アドレス数）が大幅に増加

を実現しています。

本環境内は、他の研究室・講座等からアクセスできないネットワークのため、自研究室・講座等以外からアクセスする必要がある機器（サーバ等）は、3.1 で示したゾーニングの考えに基づき、学外もしくは学内のみからアクセス可能なゾーンに移行することになります。プライベートネットワーク環境への移行については、調査やヒアリングが必要なことから、現時点においては申し込み形式を取っており、順次切り替えを行っています。

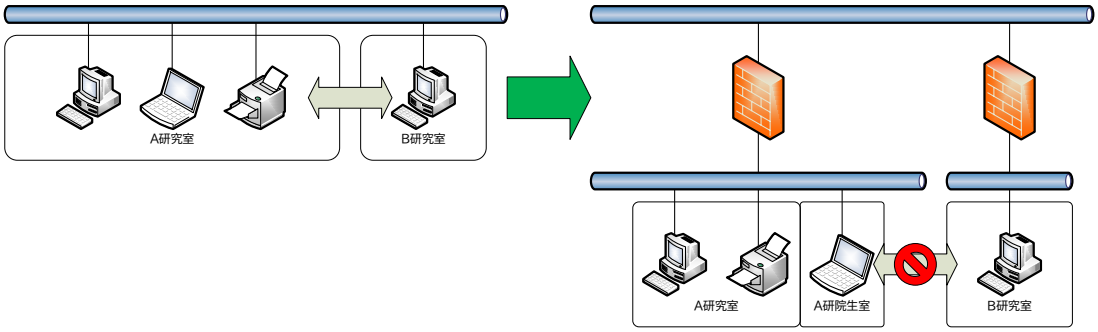


図 2：プライベートネットワーク環境（マイクロセグメンテーション）の模式図

3.3. 無線 LAN 拡充

前システムの無線 LAN システムについては、仕様書策定時点における想定としては、主に教員が使う会議室、大規模な教室、自習等に用いられる附属図書館や学生が集まる食堂、休憩スペースを中心として一時的なネットワーク利用を想定したものでした。平成 26 年度の学生 PC 必携化（授業の中で PC を活用する）により、要求要件が大きく変化しました。必携 PC を活用する授業の場合、受講している（教室にいる）全員が同時にネットワークを利用することを想定しておかなければなりません。そこで、利用者が利用する通信環境は無線 LAN によるものを中心とし、AP の追加増設を行いました。設置方針にかかる大学当局の判断としては「まずはどの教室でも利用できるようにすること」であり、授業に用いられる教室のうちこれまで AP が設置されていない教室のすべてに 1 台ずつ設置（収容人数が非常に大きい教室のみ 2 台設置）しましたが、対応通信規格や管理機能上の限界もあり、利用者から、生協食堂や大規模教室においてつながりにくい・遅いというクレームを受けていました。

新システムにおいては、教室で授業に参加する全員が快適に利用できる、という整備目標を達成するため、設計方針や配置方針を検討し、調達を進めていたところ、COVID-19 による社会状況の変化が生じ、授業手法や受講方法等も変容しました。ピークを脱した後も、そもそも、密を避けなければならず、同時に教室や実験室に入る人数は制限され、また、自宅等のネットワーク環境が十分ではなくオンライン授業を大学で受講する学生への対応も必要となりました。分散授業等に対応するため、これまで授業では使用されていなかった資料室や実験室にも調整の上設置しました。教育目的ではこれ以上設置する箇所はない、という部局さえあります。

表 3：無線 LAN AP の設置台数

	前システム	新システム
稼働時期	平成 22 年 4 月より順次	令和 2 年 10 月
規格・台数	520 台 (IEEE802.11n, Max. 300Mbps) 当初 80 台から補助金等 により順次増設 計 520 台	高密度タイプ：20 台 （11ax, Max. 5.38Gbps） 高密度タイプ：173 台 （11ac, Max. 5.2Gbps） 一般タイプ：245 台 （11ac, Max. 867Mbps） 令和 3 年 3 月以降 100 台増設 計 538 台 加えて附属学校に 64 台（GIGA スクール）

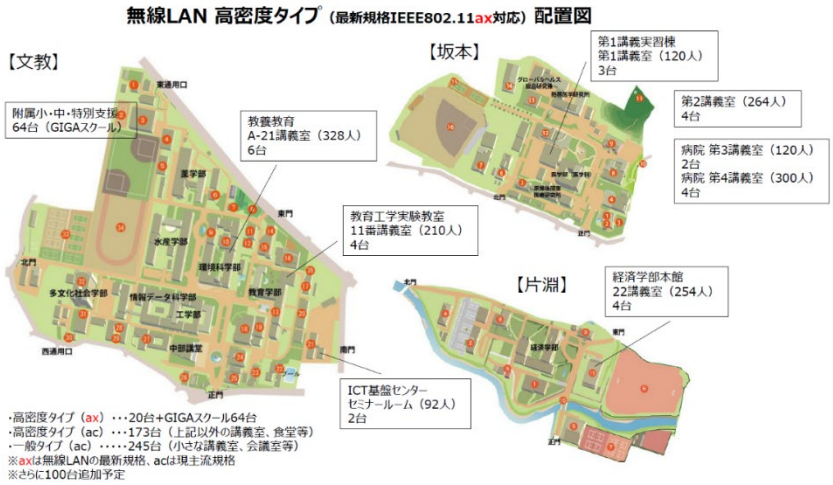


図 3：無線 LAN AP の配置数

入札制度上、また今回から機器についてはリースとしたため、簡単に台数や機器を変更できず、別途予算確保が必要となりました。そこで、これまで大学予算で附属学校に設置していた AP については GIGA スクール構想補助金により設置するものとし、加えて 100 台分の追加予算を確保しました。

本学の無線 LAN においては、授業受講等に特化した「講義用無線 LAN」と、一般的な利用が可能な「一般用無線 LAN」があります。新システムでは、より簡単に講義用無線 LAN が利用できるよう、IEEE 802.1X による認証方式の提供を開始しました。ただし、共用端末も存在しうることから、これまでの Web 認証方式も当面提供します。

無線 LAN につながりにくい、というクレームは、端末側の問題や相性問題を除き、ほぼなくなりました。これは、認証方式として 1X 認証方式を正式運用したこと、無線 LAN システム・環境として機能・性能が改善されたことによるものと思われます。COVID-19 の影響による同一場所での接続数の減少も一因として考えられますが、COVID-19 が第 5 類化し、対面授業が戻ってきた本稿執筆時点でも、（システム側の性能が原因で）つながりにくい、というようなクレームはまずありません。

これまで本学において eduroam を利用できる箇所は、システムの機能・性能の問題から限定された箇所のみで利用可能でしたが、新システムでは、技術的にはすべての無線 LAN 設置場所において利用できるようになりました。現在は、すべての設置場所で利用できるようにしていますが、物理的セキュリティ等の問題により、設置場所ごとに停止することもできるようにしています。また、今後、災害発生時における大学の地域貢献として、災害用無線 LAN の提供体制を整えていきます。

3.4. VPN 拡充

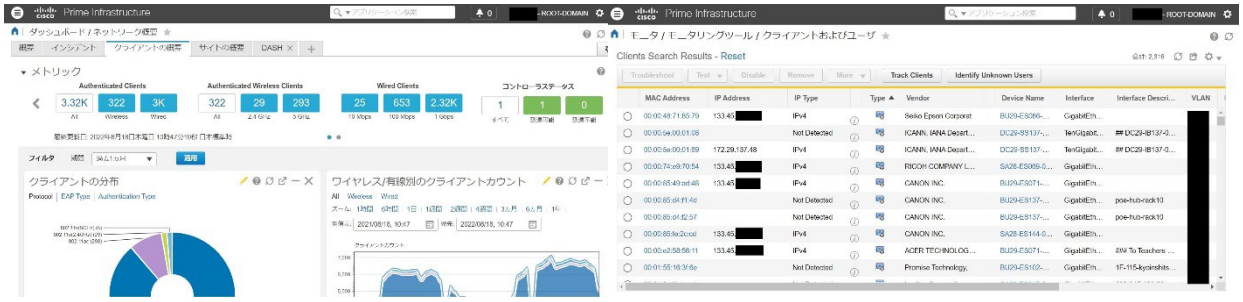
本学において、成績等を扱う学務情報システムなどは、直接学外からはアクセスできず、VPN を経由する必要があります。COVID-19 の影響により、リモート授業や在宅勤務が増加しました。システムごとに精査し、安全に公開できるものはそのまま公開、また、安全上 VPN を経由することが必要なものも残ることから、予算を確保し、VPN 接続ライセンスを追加調達するとともに、事務系については、FW の VPN 接続機能も活用し、電子証明書の利用を必須としました。

新たに、VPN を経由して研究室等のプライベートネットワーク環境に接続できる構成も構築し、一部の部局で試験運用を行っています。

また、クラウドサービスを活用した、VPN 経由の必要がない業務体制についても推進しています。

3.5. 統一認証環境及びネットワーク一元管理装置の導入

前システムにおいても、接続認証記録は残しておりましたが、何らかのインシデントが生じた際に、その機器を特定するために記録の突き合わせ等で時間を要し、また、個々の BBR の配下に接続されている等、特定できないこともありました。そこで、新システムでは統一認証環境 Cisco Identity Services Engine 及び一元管理ソリューション Cisco Prime Infrastructure を導入し、有線・無線・VPN 等ネットワーク利用時の機器・個人の統合的な認証を行うとともに、接続記録や認証記録を集約することにより、インシデント発生時に、事態の早急な対応（状況把握、通信遮断等）が可能となりました。また、利用数・接続数の正確な把握による、ICT 環境に関する将来計画策定等へのデータの取得も意図しています。



(a) 接続数・接続方法　　(b) 接続場所・IP アドレス)

図 4：一元管理ソリューションによる把握状況

図 4 に示すように、プライベートネットワーク環境配下の状況も把握できています。

将来的には、セキュリティ強化のため、利用者の属性（学生・教職員や所属部局等）により、認められた範囲のリソースのみが利用できるように制御する予定です。

3.6. フロー情報を用いたインシデント検知システムの導入

本学はこれまで主に対外接続点等において FW や IDS による生トラフィックの監視によるインシデント検知を行ってきました。脅威やネットワーク利用の形態が変化するなかで、より早急なインシデントやその端緒の検知が求められます。将来的なトラフィックの増加や、学内のインシデントの端緒を検知するためには、学内を流れるトラフィックをすべて収集する必要があり、生トラフィックを直接分析する形態の IDS での更新は費用的にも性能的にも現実的ではありませんでした。

そこで、新システムの調達では、末端全てのポートにおいてフロー情報を取得できることを必須要件としました。入札の結果 Cisco System 社製品を主とするネットワークシステムが納入されたため、フロー情報を活用してインシデント検知を行うシステムとして、Cisco Secure Network Analytics を選定し、システム本体とは別に調達しました。

NUNET 内の各ネットワーク機器を流れるトラフィックのフロー情報を利用できることから、図 5 のように、プライベートアドレス空間においても、インシデント検出や機器特定が可能となっています。また、収集するフロー情報のデータ量は、トラフィックそのものに比べて十分小さいため、一定期間に遡ってどのような通信が行われたかを確認することができ、インシデントが検知された際に、その機器から学内に対してどのような影響があったのか、というような把握にも使用できるようになりました。

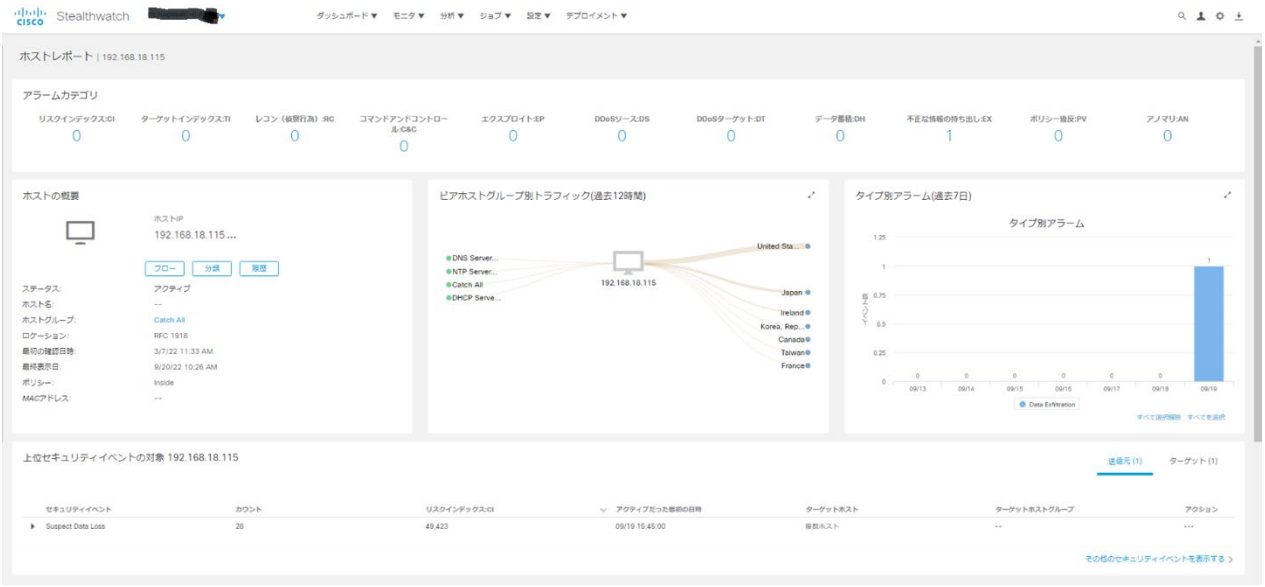


図 5：フロー情報を用いたインシデント検知システムにおける検出事例

4. まとめ

本稿では、本学のキャンパス情報ネットワーク更改について、更改の背景、新システムの特徴や機能等のポイントについて述べました。

キャンパス情報ネットワークのセキュリティ・利便性を向上するため、ネットワーク構造を大幅に変更し、また、プライベートネットワーク環境、統一認証環境や一元管理・監視装置等の導入により、ネットワーク管理の効率化・高度化とセキュリティ向上を図りました。

システムは令和 2 年 10 月に稼働開始しましたが、COVID-19 による社会状況の変容（授業形態、登学禁止等）と重なり、更新前後の性能の差異を単純に評価することはできません。

本稿については、センターレポートの執筆時期の関係で、内容としては少々古くなっています。すでに、次のキャンパスネットワーク更新に向けて、ネットワークそのものやセキュリティに関して、他大学や関係業界の動向の収集を行っているところです。クラウド化やサブスク化によるサービスライセンス費の高騰、半導体不足、為替の動向等、各大学やセンターの努力だけではどうにもならないことが増えているのも現実ですが、セキュリティ・利便性・コストに十分配慮した運営に努めて参りますので、ご支援をどうぞよろしくお願い申し上げます。

参考文献

[1] 柳生 大輔, 上繁 義史, 鶴 正人, “長崎大学キャンパスネットワークの更改”, 国公立大学情報システム研究会, Vol. 25, pp.44-53, Dec. 2022.

[2] 柳生 大輔, 上繁 義史, “長崎大学キャンパス情報ネットワーク(NUNET)の更改”, 情報系センター協議会第 26 回学術情報処理研究集会・発表論文集, Sep. 2022.