MAC アドレスの登録による学内有線 LAN 利用申請制の導入

石田 元気 [1)]

1) 鹿屋体育大学 スポーツ情報センター

ishida@nifs-k.ac.jp

Introduce of Cumpus Wired LAN Usage System by Registering MAC Address

Genki Ishida[1)]

1) Information Technology Center for Sports Sciences, National Institute of Fitness and Sports in Kanoya

概要

大学では、利用者の柔軟かつセキュリティを確保できるキャンパスネットワークが求められる。セキュリティを確保するためには、管理者が利用者の端末を把握しておく必要がある。この要件を確保するため、鹿屋体育大学では 2018 年 3 月に行われたキャンパネットワークの更新の際に、学内有線 LAN の利用には MAC アドレスの登録を必要とする学内有線 LAN 利用申請制を導入した [1]。本稿では、大学におけるキャンパスネットワークへの利用端末の接続に関する課題について述べ、それらの課題を達成するために鹿屋体育大学で導入した申請制と、鹿屋体育大学での申請状況について報告する。

1 はじめに

大学などの高等教育機関では、研究教育活動のため、利用者の利便性を損なわない柔軟なキャンパスネットワークの構築、運用が求められる。しかし、教職員や学生が所有する端末のキャンパスネットワークへの自由な接続は、ネットワークセキュリティを確保するうえで大きな問題となる。

まず、脆弱性を抱えた機器のキャンパスネットワークへの接続が問題となる。ウイルス対策ソフトウェアが導入されていない端末やベンダーによるサポート期限が切れ、脆弱性を抱えている端末がネットワーク管理者の知らぬ間にキャンパスネットワークに接続する可能性がある。

また、インシデント発生時における当該端末の追跡の困難さも問題となる。ネットワーク管理者の把握していない端末がセキュリティインシデントを引き起こした場合、その端末および所有者を迅速に特定するための手段を用意しておく必要がある。

鹿屋体育大学では、2018 年 3 月に情報基盤システムを更新し、キャンパスネットワークの見直しも行われた。この際、上述の問題を解決するためのシステムをネットワーク設計に盛り込んだ。まず学内無線 LAN については、更新前のシステムと同様に、IEEE802.3X によるアカウント認証方式を採用し、インシデント発生時における当該端末利用者の特定を迅速に行うための手段とした。次に、学内有線 LAN については、更新前に導入されていた Web 認証方式を廃し、MAC アドレスの登録による学内有線 LAN 利用申請方式を導入した。

本稿では、学内有線 LAN の情報セキュリティ確保のために導入した MAC アドレスの登録による利用申請について報告する。

2 改善すべき課題

更新後のシステムでは、Web 認証方式を利用できない端末への接続の提供、有線 LAN 接続端末のネットワーク管理者による把握、インシデント発生時における端末所有者追跡の迅速化の 3 つの課題の改善を目指した。

まず、Web 認証方式を利用できない端末への接続の提供である。有線 LAN に接続している機器の中には Web 認証方式を利用できないネットワーク複合機や NAS があり、利用者の利便性を損なっていた。更新後のシステムでは、このような端末の接続性を確保するシステムが必要であった。

次に、有線 LAN 接続端末のネットワーク管理者による把握である。Web 認証方式採用時では、アカウントを所有していれば利用者の持ち込み端末などを学内有線 LAN に接続することができ、どのような端末が

有線 LAN に接続されているかの把握が困難であった。更新後のシステムでは、有線 LAN に接続されている端末をネットワーク管理者が把握できるシステムを構築する必要があった。

最後に、インシデント発生時における端末所有者の明確化である。Web 認証方式採用時においては、有線 LAN 接続端末の MAC アドレスから認証に用いられたアカウントを追跡することが可能であり、インシデント発生時には、接続アカウントから所有者を特定することができた。更新後のシステムにおいても、インシデント発生時における端末所有者の追跡を可能とするシステムが必要であった。

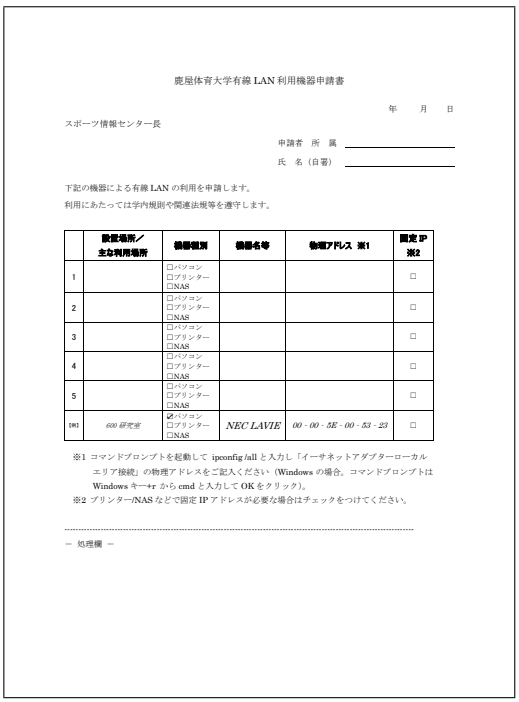
3　MAC アドレスの登録による利用申請方式の導入

前述の目的を達成するため、鹿屋体育大学では更新後のキャンパスネットワークにおける学内有線 LAN 接続に関して、MAC アドレスの登録による利用申請方式を導入した。

本方式では、以下の流れにより、利用者が学内有線 LAN に端末を接続できるようになる。まず、利用者は、図 1 に示す有線 LAN 利用機器申請書に必要事項を記入し、ネットワーク管理者へ提出する。この申請書には主に、利用管理者、端末の設置場所、端末の種類、端末の MAC アドレスを記入する。また、利用者が端末の MAC アドレスを記入しやすいよう、Windows に限り、MAC アドレスの確認方法を注釈として申請書に記載している。ネットワーク管理者は、利用申請書を受け取る際、その端末が PC であれば、ウイルス対策ソフトウェアが導入されているか、またベンダーによるサポート期限が切れていないかを確認する。また、NAS であれば必ずパスワードやアカウントによる制御を設定し、機密性を確保するよう依頼する。ネットワーク管理者は利用申請受理後、学内有線 LAN を管理している DHCP サーバへ登録する。DHCP サーバでは、申請された端末に対して学内有線 LAN における固定 IP アドレスが払い出される。DHCP サーバへの登録完了後、利用者は学内有線 LAN を利用することができるようになる。

利用申請がなされないまま端末を学内有線 LAN に接続すると、DHCP によって学外や他の端末へアクセスできない限定的なセグメントの IP アドレスが払い出され、端末の利用を制限するシステムとなっている。

この方式では、以下の 4 つの特徴により、前述の目的を達成するシステムを実現した。



鹿屋体育大学有線 LAN 利用機器申請書

年　月　日

スポーツ情報センター長

申請者　所　属 ＿＿＿＿＿＿

氏　名（自署） ＿＿＿＿＿＿

下記の機器による有線 LAN の利用を申請します。
利用にあたっては学内規則や関連法規等を遵守します。

	設置場所／主な利用場所	機器種別	機器名等	物理アドレス ※1	固定 IP ※2
1		□パソコン □プリンター □NAS			□
2		□パソコン □プリンター □NAS			□
3		□パソコン □プリンター □NAS			□
4		□パソコン □プリンター □NAS			□
5		□パソコン □プリンター □NAS			□
例	630 研究室	☑パソコン □プリンター □NAS	NEC LAVIE	00 - 00 - 5E - 00 - 53 - 23	□

※1 コマンドプロンプトを起動して ipconfig /all と入力し「イーサネットアダプターローカルエリア接続」の物理アドレスをご記入ください（Windows の場合。コマンドプロンプトは Windows キー＋r から cmd と入力して OK をクリック）。
※2 プリンター/NAS などで固定 IP アドレスが必要な場合はチェックをつけてください。

－ 処理欄 －

図 1　有線 LAN 利用機器申請書

まず、学内有線 LAN への接続の可否を DHCP で実現した点である。DHCP によるネットワーク自動設定は広く普及しており、PC だけでなく、NAS やネットワーク複合機においてもほとんどの場合で利用可能である。この DHCP を利用することにより、利便性を確保しつつ、学内有線 LAN への接続の可否を制御することが可能となった。

次に、利用申請制の導入である。利用申請制を導入することにより、学内有線 LAN へ接続する端末をネットワーク管理者が把握するできるようになった。

そして、申請の際の利用者への確認行為である。申請の際に、情報セキュリティの確保について利用者へ確認を行うことにより、ウイルス対策ソフトウェアを導入していない端末やサポート期限切れの端末の学内有線 LAN への接続を防ぐことができるようになった。また、ウイルス対策ソフトウェアの導入やベンダーサポート期限に対する利用者のセキュリティの意識を再確認する機会を作ることができた。

最後に、インシデント発生時における端末所有者の特定の迅速化である。申請により、インシデント発生時に IP アドレスや MAC アドレスから迅速に端末所有者を特定することができるシステムとなった。また、固定 IP アドレスであるため、インシデント発生から長期間後に発覚した場合でも、IP アドレスの変遷をログから追うこと無く、迅速に所有者を特定することができるシステムとなった。

4　申請状況

2018 年 3 月の情報基盤システム更新時には、4 ヶ月前の 2017 年 12 月より学内有線 LAN の利用申請制導入をアナウンスしていたことにより、大きな混乱も無く、更新後のシステムへ移行することができた。申請の周知状況に関して、学内有線 LAN へ接続できない利用者からの問い合わせのうち、原因が未申請であった件数はシステム更新後から 2020 年 10 月までに 5 件であった。

また、システム更新時からの申請台数の推移を図 2 に示す。なお、利用者に対して申請の受付を開始した 2018 年 1 月はパソコン 125 台、ネットワーク複合機 32 台、NAS2 台の申請があったが、視認性の確保のため、2018 年 1 月のみ除外した。

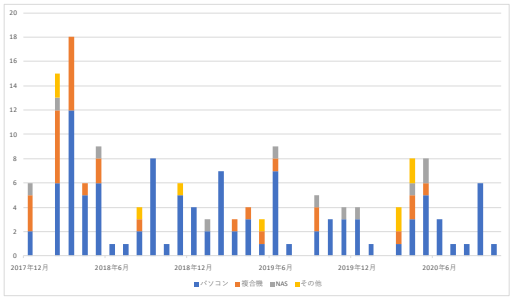


図 2　月ごとの申請台数

5　おわりに

本稿では、鹿屋体育大学で導入した学内有線 LAN 申請制について報告した。特に、キャンパスネットワークの柔軟性を確保しつつセキュリティを確保するための課題と解決方法について、広く普及している DHCP によってこれを解決する試みを中心に紹介した。この方法では、ネットワーク機器による自動的なシステムを用いるだけでなく申請制を利用することにより、利用者に情報セキュリティを意識させることができる。未申請による問い合わせの件数の少なさからも本方式は十分に周知されていると考えられる。また、申請台数は、少人数のネットワーク管理者でも十分に対応可能な台数であると考えられ、学内有線 LAN に接続する端末を管理者が把握する手段としてコストの低い、有用なシステムであると考えられる。

参考文献

[1] スポーツ情報センター広報 第 8 号 2019、https://itec.nifs-k.ac.jp/bulletin/2019.pdf