[ポスター発表] 研究報告

広島大学キャンパスネットワークにおける端末管理とネットワーク利用制御手法の導入

近堂 徹[1,a)]　渡邉 英伸[1]　田島 浩一[1]　西村 浩二[1]　相原 玲二[1]

Implementation of terminal management and network usage control method in the HINET2020

1. はじめに

大学におけるキャンパスネットワークは，主要インフラのひとつとしてセキュリティと安定性を確保しつつ，ユーザの利便性を損なわないことが求められる。一方で，多くの大学でキャンパスネットワークの導入から約 30 年経過し，その間何度も更新が行われてきた。時代の変化とともに通信帯域の増速や柔軟なネットワークセグメンテーション化などは充実してきたが，接続端末が多様化・複雑化する中で端末のトレーサビリティのための認証やセキュリティ強化については課題も多い。ネットワーク更新の際，エッジスイッチを含むネットワーク機器を全面的に刷新し，一定水準を満たす機器のみを許可できる方針とすればさまざまなソリューションが存在する。しかしながら，大学のような多様なステークホルダーが存在する組織では，限られた予算の中で更新計画を考えていく必要があり，古い機種も含む複数のネットワーク機器を許容せざるを得ない状況も生まれる。また，多様な機器の接続も求められる中でネットワーク管理技術を確立していく必要がある。

広島大学では，2021 年 3 月にキャンパス情報ネットワーク（以下，HINET2020）の基幹部分の更新を行なった。今回の更新では，500 台を超えるエッジスイッチ（2007 度年導入）の更新は行わず，基幹部分に必要な機能を持たせることで端末トレーサビリティのための認証手法の改善やセキュリティ強化を図った。本稿では，HINET2020 で導入した新機能およびこれらの効果について概説する。

2. HINET2020 の概要

HINET2020 の基幹ネットワーク構成を図 1，基幹サービス構成を図 2 に示す。コアスイッチ装置にはアラクサラネットワークス社 AX8616S, ファイアウォール装置にはパロアルトネットワークス社 PA-5250，VPN 装置にはシスコシステムズ社 Firepower2130ASA を利用している。また，基幹サービスは 3 台の IA サーバ上にコンテナ仮想化により各種サービスをデプロイした構成となっている。以下に主な特徴を示す。

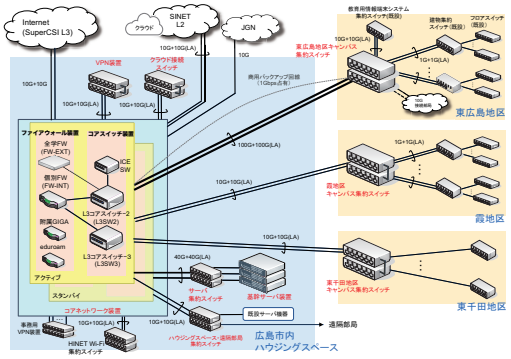

図 1　HINET2020 のネットワーク構成（赤字が今回更新範囲）

2.1 マイクロセグメンテーションの継続

HINET では，L3 機能（ルーティング機能，DHCP サービス機能など）はコアネットワーク装置に集約し，学内外からのアクセス可否パターンおよび利用形態により区別される「ゾーン」という概念を導入している*1。また，VLAN ID や IP アドレスなどの論理リソースも全学一元管理とし，利用者はネットワーク利用申請サービスから申請，管理を行う。本方針は HINET2020 でも継続し，利用者への大幅な変更は伴わない。一方，これまで全学的に導入していた IPv6 については，RA(Router Advertisement) による IP アドレス割当から DHCPv6 によるステートフルアドレス割当とし，IPv4 と IPv6 で統一した管理ポリシーとした。

2.2 認証方式の再検討

多くの組織でネットワーク利用にユーザー認証が求められている。これは内部からの不正アクセスを防ぐ従来の目的はもちろんのこと，ネットワーク内での端末トレー

[1] 広島大学情報メディア教育研究センター, Information Media Center, Hiroshima University, 739-8511, Japan
[a)] tkondo@hiroshima-u.ac.jp

*1 https://www.media.hiroshima-u.ac.jp/services/hinet/about-hinet/

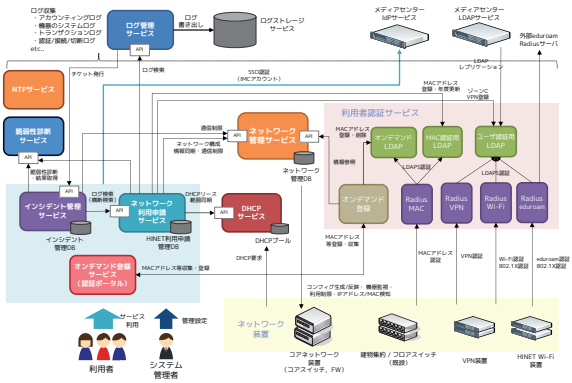

図 2　HINET2020 の基幹サービス構成

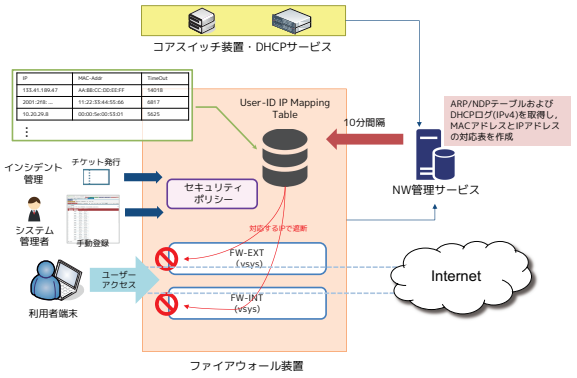

図 3　ファイアウォール装置における通信制限

サビリティを確保するための手段としての役割が大きい。HINET では，これまで，ネットワークスイッチに具備されるウェブ認証もしくは MAC アドレス認証による認証機能を利用してきたが，500 台を超えるネットワークスイッチを運用するなかで，特にウェブ認証はウェブブラウザの進化への追従が困難となり，ユーザービリティの低下が課題となっていた。恒久的には 802.1X 認証への移行が必要と考えているが，EAP フレームを透過できないスイッチや研究室に設置した部局無線 LAN アクセスポイントでの認証との競合などの問題が残っている。そこで，過渡期への対応として，ユーザー認証に基づき端末の MAC アドレスをユーザーの手動入力を求めることなく登録し，その情報を用いてエッジスイッチでの MAC アドレス認証が可能な「オンデマンド登録方式」を新たに設計，導入した。本方式は，図 2 における認証サービス（ユーザー認証および端末トレーサビリティ機能）やネットワーク管理サービス（ネットワーク機器の自動設定機能）が相互に連携することで実現している。

2.3　セキュリティ機能の強化

国立情報学研究所が提供する NII-SOCS やファイアウォール装置，外部からの通知等に基づくセキュリティトラブルへの対応コストの低減を目的として，インシデント管理サービスやコアネットワーク（ファイアウォール）装置での端末制限機能を新たに導入した。これは，前述の認証サービスおよびネットワーク管理サービスによる端末トレーサビリティを積極的に活用した機能で，通信時間と対象 IP アドレスなどの情報をキーに端末と利用者の特定から，ファイアウォール装置での通信制限の実行，および対応管理のためのチケット管理を行う機能である。

本稿では通信制限機能（図 3）の詳細を説明する。本機能における通信制限ポイントは L3 機能を集約している点を考慮し，ファイアウォール装置（図 1 中の個別 FW, 全学 FW）としている。これは，既存手法 [2] でも採用されているエッジスイッチでの通信制限と比較して制御ポイントがネットワーク上位になってしまうものの，端末移動時の制限設定の継続性やマルチベンダ構成を考慮した結果である。一方でファイアウォール装置にて端末単位の制御を行うためには，セグメントを超えて MAC アドレスによる端末識別と制御が求められる。これを実現するために，今回はファイアウォール装置が具備する User-ID（ユーザー識別）機能を用いた。MAC アドレスを User-ID として保持し，セキュリティポリシーを適用する User-ID を動的に制御することで，対応する機器の通信を制限している。ファイアウォール装置内の User-ID IP Mapping Table には，ARP/NDP テーブルや DHCPv4 ログから MAC アドレスと IPv4/v6 アドレスの対応関係を示す情報が保持される（キャッシュは 4 時間に設定）。現在，授業期 1 日のピークで約 5 万エントリが格納されている。通信制限はシステム管理者による MAC アドレスの手動登録かインシデント管理サービスからのチケット発行のいずれかをもとに行われる。MAC アドレスを登録してから通信制限が適用されるまで約 87 秒要していることを実測にて確認している。

3.　おわりに

本稿では，2021 年 3 月に更新した広島大学キャンパス情報ネットワークについて概説し，マイクロセグメンテーション化されたネットワークにおける端末認証，特定と通信制限への対応としてファイアウォール装置における MAC アドレスベースの制限手法について示した。今後，インシデント管理サービスとの連携による不正端末管理の運用と課題抽出を進めていく予定である。

謝辞　本キャンパスネットワークの構築および運用に尽力いただいている広島大学情報メディア教育研究センター，ネットワンシステムズ株式会社，株式会社プロキューブの関係者各位に感謝いたします。

参考文献

[1] 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.998-1007, 2016.

[2] 三島和宏, 根本貴弘, 萩原洋一, 辻澤隆彦, ”ネットワークモニタリングによる高セキュリティリスク端末の自動遮断システムとその運用”, 情報処理学会研究報告, Vol.2020-IoT-48, No.4, 2020.