一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

ネットワーク装置のトラヒックパターンにもとづくキャンパスネットワーク挙動の推定

中西　裕哉†　　阿多　信吾†

† 大阪市立大学 大学院工学研究科　〒558-8585 大阪府大阪市住吉区杉本 3-3-138
E-mail: †nakanishi_y@c.info.eng.osaka-cu.ac.jp, ††ata@info.eng.osaka-cu.ac.jp

あらまし　昨今の ICT 化、とりわけ大学においては遠隔授業等の教育の ICT 化および BYOD (Bring Your Own Device) の拡大に伴い、キャンパスネットワークはそのインフラとしてますます重要性が高まっている。特に集中管理に適さない BYOD の増加は一方でキャンパスネットワークの安全性・安定性を低下させる要因ともなっており、ネットワーク内の異常の早期発見、予兆検出の技術確立が求められている。しかしながら、キャンパスネットワーク全体の挙動把握を行うためには、膨大なログデータを分析する必要があり、リアルタイムで処理を行うためには効率的な分析手法が求められる。本研究では、キャンパスネットワークの異常の早期発見のトリガとなる事象を、ネットワークスイッチのトラヒックパターンデータの学習により検出する手法について検討し、その有効性を検証する。
キーワード　異常検知、機械学習、ネットワークトラヒック、キャンパスネットワーク、トラヒックパターン

Analysis of Behaviors in Campus Network based on Traffic Patterns at Network Switches

Yuya NAKANISHI† and Shingo ATA†

† Graduate School of Engineering, Osaka City University
3-3-138 Sugimoto,Sumiyoshi-ku,Osaka-shi,Osaka,558-8585 Japan
E-mail: †nakanishi_y@c.info.eng.osaka-cu.ac.jp, ††ata@info.eng.osaka-cu.ac.jp

Abstract　In recent growth of ICT, especially in Universities, the enhancement of education by ICT such as remote lectures and the increase of BYODs (Bring Your Own Devices) of students, leads the importance of campus network as infrastructure of educational and/or research activities. On the other hand, the spread of BYODs, which are not suitable to be contralled centrally, may degrade safety and stability of network bahavior due to anomally traffic from such devices. It is therefore important to realize a detection of anomalies at the very early stage. However, to follow the behavior of campus network accurately, it is necessary to collect huge log data from network switches, so a light-weight method to detect the event of anomalies is promising for real-time detection. In this study we consider a method to detect anomalies based on traffic patterns of network switches using a learning-based approach, and perform a feasilibity through numerical evaluations.
Key words　Anomaly Detection, Machine Learning, Network Traffic, Campus Network, Traffic Pattern