1ZD-02

SDN 環境における利用者の状況に応じた動的なアクセス制御に関する一検討

佐々木 優 [†1]　ギリエ ルイス [†2]　和泉 諭 [†3]　阿部 亨 [†1,†4]　水木 敬明 [†1,†4]　菅沼 拓夫 [†1,†4]

[†1] 東北大学大学院情報科学研究科　[†2] 東北大学電気通信研究所
[†3] 仙台高等専門学校　[†4] 東北大学サイバーサイエンスセンター

1　はじめに

近年，教育現場などにおいて情報端末の導入や生徒が自身の情報端末を授業で使用する Bring Your Own Device (BYOD) 環境の導入が進んでいる．このような環境下では，様々な利用者が様々な情報端末でネットワークを利用するため，セキュリティ上のリスクが存在する．その対策の一つとして，アクセス制御がある．

強制アクセス制御 (Mandatory Access Control: MAC) や役割ベースアクセス制御 (Role Based Access Control: RBAC) などの従来のアクセス制御方式 [1] では，ユーザ情報や役割に基づいて制御ポリシーが静的に決定されるため，様々な状況に柔軟に対応することは困難である．一方で，属性ベースアクセス制御 (Attribute Based Access Control: ABAC) では，アクセスする主体であるサブジェクトとアクセスの対象となる資源であるオブジェクトに属性を付与することにより細やかなアクセス制御が可能となる．また，属性には時間や IP アドレスなどのように状況によって動的に変化するものが含まれる．そのため，アクセス可能な資源の範囲も動的に変化する．

しかしながら，これらの制御手法では，ネットワーク内のある端末が他の端末のアクセスに影響を与えることがないように，端末間の状況の変化は未考慮である．そこで本稿では，Software Defined Network (SDN) 技術を利用することにより，端末間の状況の変化も考慮し，同一の利用者であっても状況に応じてアクセス可能な資源の範囲を動的に変更する手法について検討する．

2　関連研究

SDN を利用したアクセス制御の研究として，OpenFlow と認証基盤を連携させたアクセス制御手法が提案されている [2]．この研究では，端末が OpenFlow ネットワークに参加したときに，LDAP サーバへのアクセスが許可され，認証が行われる．認証に成功した場合には，コントローラは端末の IP アドレスと MAC アドレスを基にスイッチにフローエントリを配信する．これにより，端末はコンテンツサーバなど許可された資源にアクセスが可能となる．SDN を利用することにより，物理層からトランスポート層までの制御が可能であるため，細やかなアクセス制御が実現できる．その一方で，IP アドレスや MAC アドレスを基にフローエントリが配信されるため，これらの偽装により不正なフローがフィルタリングを通過してしまう．

Access Control List(ACL) を動的に変更する研究 [3] では，ユーザのネットワークへの参加や離脱に応じて，対応する ACL の追加や削除を動的に行う．ユーザがネットワークに参加すると，対応する ACL ポリシーは有効な ACL ポリシーのリストへ格納される．フローのパスを計算する際には，従来の手法と異なり，全てのポリシーを照合する必要がなく，有効なポリシーの照合のみで済むため，処理時間の短縮や TCAM の節約が実現される．一方で，この研究では，ACL ポリシーが IP アドレスに紐付けされているため，細やかな制御の変更が困難である．

文献 [4] は，SDN 環境に ABAC の拡張モデルを導入することによって，機密性の保持と完全性の確保を両立する．また，アクセスパスを計算するためにスイッチのセキュリティレベルを考慮する．これらは，環境によって値が変わる環境属性であるため，変化に柔軟に対応することを目的として PSO アルゴリズムを利用する．この研究では，機密性や完全性，パスの安全性など，セキュリティに焦点をあてたが，同時に利用者の利便性も考慮する必要がある．

3　提案

3.1　概要

本章では，利用者の状況に応じて動的にアクセス可能な資源の範囲を変更する手法について検討する．具体的には，教育現場を想定し，教室や職員室などの場所，授業中や放課後などの時間帯，生徒端末や教師端末などの端末の状態，また，端末間の状況を考慮する．これらの状況の変化は，従来のアクセス制御においては，場所や時間などの環境属性を導入することによって，動的なアクセス制御を行ってきた．

本研究では，ネットワークへ参加している端末の把握が容易である SDN を利用することによって，

A Study on Dynamic Access Control Depending On User Situation in SDN environment
Yu SASAKI[†1], Luis GUILLEN[†2], Satoru IZUMI[†3], Toru ABE[†1,†4], Takaaki MIZUKI[†1,†4], and Takuo SUGANUMA[†1,†4]
[†1]Graduate School of Information Sciences, Tohoku University
[†2]Research Institute for Electrical Communication, Tohoku University
[†3]National Institute of Technology, Sendai College
[†4]Cyberscience Center, Tohoku University

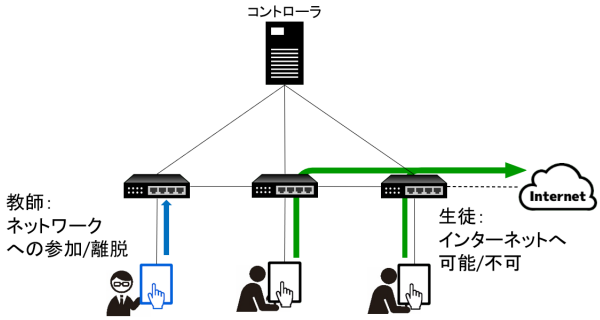

図 1: 教育現場におけるアクセス制御の動的な変更

ネットワーク内のある端末が他の端末のアクセス制御に影響を与える状況に焦点を当てる．様々な状況を考慮することによって，利用者のアクセス可能な資源を最大化しつつ，インターネットトラブルや情報漏えいなどを防止する．

3.2 想定するシナリオ

SDN を利用して，ネットワーク内のある端末が他の端末のアクセスに影響を与える状況を図 1 に示す．ここでは，教育現場を想定し，教師と生徒がいるものとする．授業中など教師がいる環境では，生徒はインターネットなどにアクセスが可能であり，インターネットを利用した調べ物学習などを行うことができる．一方で，放課後などの教師がいない環境では，生徒のインターネットなどへのアクセスを制限することによってトラブルを防止する．

これらは，ある端末のネットワークへの参加や離脱を検知することにより，他の端末のアクセス範囲を動的に変更する．図 1 で示すように，教師端末がネットワークへ参加すると，コントローラがそれを検知し，生徒端末のアクセス範囲を変更し，生徒のインターネットなどへのアクセスを許可する．同様に，教師端末のネットワークから離脱を検知した場合も，生徒のアクセス範囲を変更し，インターネットなどへのアクセスを制限する．

本研究は，授業中や放課後の区分を時間の属性を利用して動的にアクセス範囲を変更する従来の手法と比較して，より細やかな制御が可能となる．教科によって指導する教師が変わる状況では，数学の場合では生徒はシステム A にアクセスが可能，理科の場合では生徒はシステム B にアクセスが可能というように，生徒のアクセスを状況に応じてより細かく分割することができる．

3.3 設計

本稿では，教育現場において，状況に応じて動的にアクセス範囲を変更する手法について検討を行った．しかしながら，具体的なシステム設計については未検討であり，システム設計にあたり，検討・考慮しなければならない点が多く存在する．今後，検討予定の点を以下に示す．

(1) SDN 環境におけるインターネットのアクセス制御の手法，及び制御の変更の手法について検討する必要がある．また，従来のフィルタリングの手法と比較する必要がある．
(2) 図 1 では，教師端末や生徒端末は有線でのネットワークへの接続を想定した．しかしながら，一般的には無線環境がほとんどであるため，無線接続を検討する必要がある．
(3) 端末のネットワークへの参加や離脱を判定する方法，及びその端末が教師であるか生徒であるかを判別する方法については未検討である．そのため，MAC アドレスや IP アドレスを利用した機器認証や LDAP サーバを利用したユーザ認証などの具体的な認証方法について検討する必要がある．
(4) 教師がより機密性の高い（教師専用の）資源にアクセスできるように，教師と生徒では階層構造が成立する．階層構造を提案に取り入れることにより，アクセス制御の柔軟性の向上や簡易化を検討する．
(5) ABAC は細やかなアクセス制御が可能であるが，属性の増加により制御の複雑化が懸念される．ABAC と RBAC の両方の利点を活かすことができるようなアクセス制御モデルの検討を行い，より細やかで柔軟な制御の実現を目指す．

4 おわりに

本稿では，時間や場所，端末間の状況に応じて，利用者のアクセス可能な資源の範囲を動的に変更する手法について検討した．特に，ネットワーク上のある端末が他の端末のアクセス制御に影響を与える状況を考察した．今後は，3.3 節で述べた点を検討するとともに，具体的なシステムの提案・検討・設計を行う予定である．

参考文献

[1] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su and B. Fang : “A Survey on Access Control in the Age of Internet of Things,” IEEE Internet of Things Journal, pp. 4682-4696, 2020.
[2] 橋本直樹, 園生遥, 牛込翔平, 菊田宏, 永園弘, 廣津登志夫, 新村正明 : “OpenFlow による認証基盤と連携したネットワークアクセス制御の実現,” 電子情報通信学会技術研究報告, pp. 133-138, 2014.
[3] M. Ali, N. Shah and M. A. K. Khattak : “DAI: Dynamic ACL Policy Implementation for Software-Defined Networking,” 2020 IEEE 17th International Conference on Smart Communities, pp. 138-142, 2020.
[4] D. Chang, W. Sun, Y. Yang, T. Wang : “An E-ABAC-Based SDN Access Control Method,” 2019 6th International Conference on Information Science and Control Engineering (ICISCE), pp. 668-672, 2019.