Vol.2017-IOT-38 No.2
2017/6/24

不正端末検出のためのネットワークトラフィックモニタ型キャンパスネットワークの設計

櫻田武嗣[†1]　辻澤隆彦[†1]　萩原 洋一[†1]　三島 和宏[†1]

概要：本稿では，ネットワークトラフィックを監視し，セキュリティリスクの高い端末を検出する仕組みを持つキャンパスネットワークシステムの設計について述べる．東京農工大学（本学）では，昨年から本格的に BYOD 化が行われ，持ち込まれる端末の数や種類が増えている．これまで検疫・認証システムなどを構築し，運用してきてはいるが，この検疫・認証システムをすり抜けるなどの問題が発生してしまっている．このため，これにかわるシステムが必要となり，新しいキャンパスネットワークシステムを設計することとした．

キーワード：キャンパスネットワーク，脆弱性検出，BYOD

Design of Network Traffic Monitor Type Campus Network System that Detects Vulnerable Terminals

TAKESHI SAKURADA[†1]　TAKAHIKO TSUJISAWA[†1]
YOICHI HAGIWARA[†1]　KAZUHIRO MISHIMA[†1]

Abstract: In this paper, we describe the design of a new campus network system with a mechanism to monitor network traffic and detect vulnerable terminals. In our university (Tokyo University of Agriculture and Technology), BYOD (Bring Your Own Devices) began from last year. Various computers are being connected to the campus network. Various computers are being connected to the campus network. Various computers are being connected to the campus network.

Keywords: Campus Network, Vulnerability detection, BYOD

1. はじめに

現在様々なコンピュータがネットワークに接続され，利用されている．東京農工大学（以下本学と記す）においても昨年から BYOD 化が本格的に始まり，以前にも増して大学内に持ち込まれ，キャンパスネットワークに接続されるコンピュータが増えている．企業等と異なり，大学においては様々な種類のコンピュータが使用され，使われている OS やソフトウェアも多岐多様であるため全学で統一して管理することは難しい．我々は 2010 年から検疫・認証ネットワークを構築し[1]，各コンピュータの OS のアップデート状況やウィルス対策ソフトウェアの稼働状況を確認した上でキャンパスネットワークへ接続させる仕組みをとっていた．他大学においても検疫ネットワークの導入は進んでいる[2][3]．しかしながら，本学においてはこの検疫・認証ネットワークをすり抜ける端末が近年多くなってきたこともあり，今回機器の老朽化に伴い機器更新を行うタイミングで新たなキャンパスネットワークの仕組みを設計することとした．

2. 本学での以前の取り組みと課題

前述のように本学では，2010 年からキャンパスネットワークに接続されるコンピュータに対して，検疫・認証システムを構築し，運用を行ってきた．この検疫・認証システムでは，キャンパスネットワークに接続しようとする端末の OS のセキュリティアップデート状態，ウィルス対策ソフトウェアのインストールとパターンファイルの更新状況をスキャンし，更新されていなければ接続させない．このチェックを行った後に ID とパスワードによる認証を行いキャンパスネットワークに接続させるものである．この検

図 1　キャンパスネットワーク接続用検疫認証システム

†1 東京農工大学
Tokyo University of Agriculture and Technology

疫部分にはエイチ・シー・ネットワークス株式会社の QuOLA Adapter を利用しているが，検疫に対応している OS が Windows と macOS であり，そのままでは例えば Linux や Chrome OS などのその他の OS が稼働している端末を接続することができない．そこで検疫を行わないで認証だけ行うモードをこの検疫システムへ付加し運用を行ってきた(図 1). また，測定機器のような組み込み機器の場合認証するための入力すらも出来ないことがあるため，これらの機器に対しては MAC アドレスをあらかじめ登録させることでキャンパスネットワークに接続させている．

しかしながらここ数年で大きな問題がでてきた．本学ではキャンパスネットワークには各部屋に設置されている情報コンセントに直結が原則となっているが，主に家庭用に用いられるブロードバンドルータをキャンパスネットワーク内に設置して NAT 接続にて学内ネットワークへ接続する研究室が出始めた．この場合，NAT の内側にいるすべてのコンピュータの通信はキャンパスネットワーク側からはブロードバンドルータ 1 台が通信しているように見える．このため NAT の内側のコンピュータが 1 台でも検疫・認証を通過してしまうと，その他の NAT 配下のコンピュータは検疫・認証無しで通信できてしまう．NAT の内側のコンピュータのセキュリティ対策が十分であれば他への被害は少ないが，実際にはセキュリティ対策が十分では無いコンピュータがこの NAT 配下に持ち込まれ，利用されてしまっている．これがかなり目立つようになり，実際にコンピュータウィルスに感染して不正通信を行うなどの影響が出始めてしまっている．従ってこれらの対策を行っていく必要がある．

3. 新キャンパスネットワークの設計

3.1 設計方針

キャンパスネットワークの機器のメーカーによる保守可能期限が迫っていることもあり，キャンパスネットワークを更新することとした．これに合わせてこれまで課題であった点を解決すべく新キャンパスネットワークの設計を行った．

検疫・認証システムは OS のアップデートやウィルス対策ソフトウェアなどのアップデートを怠らないようにするというユーザの意識付けには十分に役立っていると考えられる一方で，前述のようにすり抜けの問題がある．そこでこのすり抜けをできる限り防止するために次のような方針で設計を行う．

(1) 不正な通信(脆弱性のある)端末をキャンパスネットワークから隔離
(2) キャンパスネットワークに接続される端末の OS 等の種類を選ばない
(3) 隔離は自動で行われ，人手を要しない
(4) 隔離された端末が利用者から分かるようにし，利用者自身で初期対応が可能なようにする
(5) 誤検出時に，隔離されないようにできるようにする

3.2 システムの設計

まず要件(1)の不正な通信(脆弱性のある)端末を隔離するためには，どの端末を隔離するかを検出しなくてはならない．接続する端末にセキュリティ対策ソフトウェアなどのエージェントを入れる方法が考えられるが，これは要件(2)の OS の種類を問わないに反する．従ってキャンパスネットワーク側を流れるパケットを監視して挙動を見極めるしかない．そこでキャンパスネットワーク側に流れるパケットをミラーリングして IDS/IPS に入力し，セキュリティリスクの判断を行う．セキュリティリスクが高いと判断した場合には，パケットの送受信元となっているエッジスイッチの当該ポートにて MAC アドレスによる端末の隔離やポートシャットダウンなどを行う．キャンパスネットワークにログインしているログイン情報を使って ID ベースで隔離する方法も考えられるが，本学ではユーザが複数デバイス使っていることが想定されるため，端末単位で隔離することを考える．セキュリティリスクが高い場合には即時隔離することが望ましい．24 時間人員を配置することは本学では現実的に難しいため要件(3)のように自動的に隔離するようにする．

端末が隔離されてしまうと，ユーザ側は突然通信が停止してしまうため，何が起こったか把握できない．窓口対応する部署が開いている時間であれば問い合わせは可能かもしれないが，夜間も隔離される可能性がある．このため要件(4)に示すように，ユーザが隔離された原因を隔離された端末以外から自身で確認できるようにする．

誤検出の発生や，大学という特性上セキュリティの研究等をしている場合も考えられるため，IDS/IPS で検出しても隔離を自動で行わない処置が要件(5)のように必要である．ホワイトリストを整備し，隔離しないようにする．

実際の設計にあたり，予算面の問題からも検討する必要がある．予算が限られていることから，これまでの検疫・認証システムに加えて前述のような新しい仕組みを導入することは難しい．そこで検疫をやめて認証だけとし，それに新しい仕組みを導入することとする．システムの概要を図 2 に示す．

また各建物や各フロアに設置するエッジスイッチごとに IDS/IPS を設置することが末端で処理できるため理想的ではあるが，設置コスト，保守コストの面から難しい．そこでエッジスイッチの上流にあたるポートをコアスイッチ側でミラーリングし，それを高性能な IDS/IPS へ入力する．本学の場合にはキャンパスバックボーンは 10Gbps のリング構成となっているため，それに対応する必要があるため，いくつかの IDS/IPS へ分散して入力して処理してセキュリティリスクの自動分析を行う．

隔離された情報をユーザへ提供する方法としては，学内

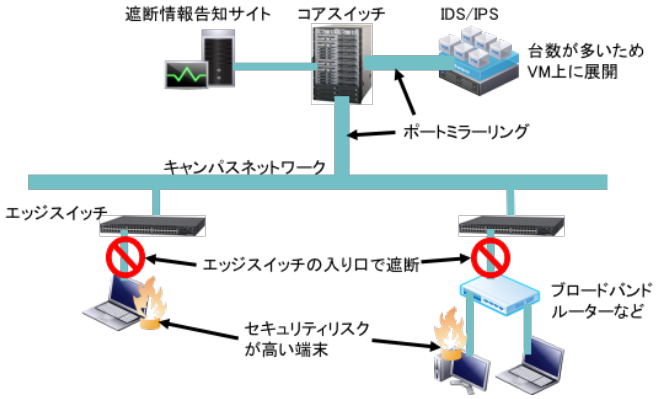

図 2　新システムの概要

者がログインできる Web サイトなどに掲示する．本学では Google 社の G Suite を契約しており，これは学内者だけが閲覧できるページを作成できるため，このようなサービスを用いることとする．

認証に関しては，これまで検疫を行う関係上，検疫プログラムのダウンロードを行わせるために Web 認証となっていたが，新システムでは検疫を行わないため，Web 認証である必要が無い．認証方式として 802.1X 認証も普及してきており，本学の無線 LAN システムも 802.1X 認証を用いていることから，キャンパスネットワークの利用のためのユーザ認証には 802.1X 認証を用いる．ユーザ認証できない組み込み機器などはこれまで通り，MAC アドレスによる認証を用いる．エッジスイッチの各ポートの認証の順番は，MAC アドレス認証，802.1X 認証とし，それぞれ認証できない場合に次の認証へ移行する．ゲストネットワークも提供する場合には，802.1X 認証が出来ない場合にさらに Web 認証を行う形とする．

4.　今後の計画

本稿で述べたシステムは実現に向け，キャンパスネットワークのスイッチを含めて入札が終わった段階であり，構築に向けて動き出している段階である．どの段階で隔離するのが適切なのかなど，実際の運用を行いつつ調整して行く必要があると考えられる．また，本システムだけでは 100%セキュリティリスクを回避することはできない．そこでまずは本システムの自動隔離や隔離情報提供部分等に関して次世代ファイアウォールシステム等と連携していく予定である．これらを含めて複数の方法を用いてセキュリティリスクの低減を行っていく予定である．

5.　おわりに

本稿では，現在の検疫・認証を行っているキャンパスネットワークを更新するための新しいキャンパスネットワークの設計について述べた．本システムでは，キャンパスネットワークに流れるパケットをミラーリングなどで監視し，セキュリティリスクの高い端末を検出した場合には自動で隔離し，キャンパスネットワーク側への影響を最小限にする．また隔離した端末の情報を学内ユーザが閲覧できるようにし，隔離された理由を各ユーザが分かるようにする．これまでのキャンパスネットワークで検疫・認証ネットワークをすり抜ける端末をこの新たなキャンパスネットワークの仕組みにて減らすことができ，セキュリティを高めていくことが可能となる．

現在は前述のように入札が終わった段階であるため，本設計にもとづいて実際にシステムを構築して運用していく予定である．

参考文献

[1] エイチ・シー・ネットワークス株式会社 導入事例 東京農工大学(2012), [online] http://www.hcnet.co.jp/case/edu/201203_tuat.html (参照 2017-05-15).
[2] 佐藤聡, 横山憲彦, 真中剛司, 中井央, 片岸一起, 板野肯三: 学生宿舎への認証・検疫ネットワークシステムの導入, 研究報告インターネットと運用技術(IOT), 情報処理学会, 2008(72), pp.41-46, (2008).
[3] 藤村丞,奥村勝,中國真教: キャンパスネットワークにおける利用者認証と検疫システムの導入, 研究報告インターネットと運用技術(IOT), 情報処理学会, 2013-IOT-20(9), pp.1-6 (2013).