Vol.2020-IOT-48 No.4
2020/3/2

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

三島和宏[†1]　根本貴弘[†1]　萩原洋一[†1]　辻澤隆彦[†1]

概要：大学のキャンパスネットワークの運用に際し，標的型攻撃による情報漏洩や脆弱性に対するアタックによる不正アクセスなど，さまざまな脅威にさらされている．本学を含む多くの大学での BYOD 化や必携化などキャンパスネットワークに接続される端末環境にも変化が生じている．これまで本学では検疫・認証システムなどを用いて接続端末のセキュリティ向上に努めてきたが，検疫のすり抜けなど十分に対策されているとは言えない状況となっており，新たなキャンパスネットワークのセキュリティ対策として，ネットワークモニタリングに基づく自動遮断をベースとしたシステムを導入した．本システムは学外に向けたネットワークトラフィックをキャンパスネットワーク側でモニタリングし，セキュリティリスクが高いと判断された端末は自動的にキャンパスネットワークから遮断する．これにより，セキュリティリスクの高い機器からキャンパスネットワークを保護し，自動化により運用やサポートにかかるコストをなるべく下げることが可能となる．本稿では，これらシステムの詳細と本学における実運用の状況を概説する．

キーワード：キャンパスネットワーク，脆弱性検出，自動遮断，BYOD

Security Measure System with Automatic Isolation of High Security Risk Device using Network Monitoring

KAZUHIRO MISHIMA[†1]　TAKAHIRO NEMOTO[†1]
YOICHI HAGIWARA[†1]　TAKAHIKO TSUJISAWA[†1]

Abstract: In operation stage in campus network, there are various threats such as information leaks due to targeted attacks and unauthorized access due to attacks on vulnerabilities. The environment of campus network, which is connected large variety of devices, is also changing, such as the transition to BYOD. Our university tried to improve the security level by using a quarantine / authentication network system. Although, it was not sufficient measures for new style of campus network. For this situation, we design and implement the automatic isolation system based on network monitoring. This system has a monitoring system for campus network, and automatically isolating devices judged to have high security risks. As a result, it is possible to protect the campus network from devices with high security risks, and to reduce the operation and support costs by isolation cancellation automation. This paper introduces the details of our system and the status of actual operation.

Keywords: Campus Network, Vulnerability Detection, Automatic Isolation, BYOD

1. はじめに

コンピュータの低価格化に伴い，多くの情報機器が活用され，キャンパスネットワークに接続されている．これに合わせて，学校や企業において各自の機器を利用する BYOD(Bring Your Own Device)が広まっている．このような状況下において，ネットワークには様々な種類の機器が接続されることとなる．大学におけるキャンパスネットワークでも BYOD 化が進むとともに，接続される機器の多様化が進んでいる．東京農工大学（以下，本学）では，2016 年度に教育用電子計算機システムを更新すると同時に BYOD 化を実施した．電子計算機システムはこれを前提に構築され，持ち込まれる機器によらず共通の演習環境を提供している．すでに多くの個人用の機器が持ち込まれ，利用されてはいたが，全学の BYOD 化により，さらに多くの機器が大学に持ち込まれることとなった．

2. 検疫・認証ネットワークによるセキュリティ対策とその限界

本学では，以前から検疫・認証ネットワークを構築[1]し，各機器の 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に接続させる仕組みを運用してきた．検疫・認証は，図 2 に示すように，ユーザがネットワークに接続した際に Web 認証ページ（図 1）を通じてエージェントプログラムをダウンロードし，そのエージェントがユーザの機器を検疫し，問題がない場合に Web 認証を通過させるというものである．他大学においても同様の検疫ネットワークの導入も行われている[2][3].

しかし，情報機器の多様化によって，検疫・認証ネットワークでは十分に対策が行えない状況が発生していた．検

†1 東京農工大学 総合情報メディアセンター
Information Media Center, Tokyo University of Agriculture and Technology

疫・認証ネットワークでは，接続を行って問題ないというシステムの定義データベースを持っている．近年の OS ではアップデートが従来のものと異なるようになっており，この定義データベースが最新の環境に追従しにくくなってきていた．また，大学では研究に主要な OS を搭載しない組み込み機器などを利用する場合もあり，これらへの対応も十分とは言えない状況であった．これらの機器に対しては，検疫・認証ネットワークを一時的に回避する設定を行うしかできなかった．エージェントが対応しない OS は，検疫認証画面にて特殊な機器である旨を明示するリンクをクリックすることで，一切の検疫を不要とする．この抜け道を利用してエージェントが対応した OS を利用したユーザであっても検疫を回避することが頻繁に行われるようになった．この他に，従来のキャンパスネットワークでは MAC アドレス認証を行うと検疫を必要としなかったため，ブロードバンドルータの MAC アドレスを登録し，その配下の全ての端末を検疫認証から除外するユーザも現れた．

図 1　検疫・認証を行う際の Web インタフェース

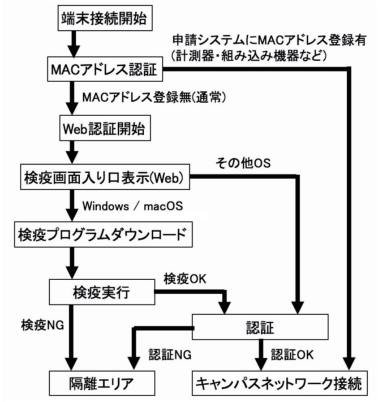

図 2　検疫・認証を行う際の認証フロー

3. 高セキュリティリスク端末の自動遮断

3.1 キャンパスネットワーク構成とモニタリング

本学は，小金井と府中の 2 キャンパスを持つ．各キャンパスにはエッジスイッチの集約を行うスイッチが設置される．インターネットへの接続は府中キャンパスより行う．府中キャンパスに関してはこの集約スイッチがインターネット接続を行う L3 機能も併せ持つ．集約スイッチからエッジスイッチまでの配線は，設置コストの関係で多数のファイバを設置できないため，集約スイッチとエッジスイッチ間でリングネットワークを構成している．

新しいキャンパスネットワークでは，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し，セキュリティ検査システムにて通信のセキュリティリスクを判別する．不正な通信を行う端末の検出にはなるべき接続される機器に近い位置で処理することが望ましい．この場合，エッジスイッチごとにセキュリティ検査システムを設置しなければならない．コストの面から考えて，これは現実的ではない．そこで，集約スイッチとエッジスイッチを結ぶリングポートを集約スイッチ側でポートミラーする形とした．

このように通信パケットを監視し，セキュリティリスクの分析に利用することで，従来の検疫・認証ネットワークではすり抜けを可能としていた一部の機器についても一律に監視を行うことが可能となる．特にセキュリティ対策が甘い組み込み機器が脆弱性に対する攻撃を受け，さらなる攻撃の踏み台などに利用されることを防ぐことができる．また，従来のネットワークでは，ブロードバンドルータと MAC アドレス認証を用い検疫を逃れたネットワークを構築されることがあったが，これについてもキャンパスネットワークに接続するエッジスイッチ側で挙動を確認できるようになるため，同様の遮断処理をおこなうことができる．

また，無線 LAN ネットワークは，シスコスシステムズ社製の無線 LAN システムを導入している．我々のシステムでは，無線端末からの通信は無線 LAN コントローラを経由し，NAT 処理が行われた後，キャンパスネットワークへと接続される．このため，無線アクセスポイント直近では不正通信の検知を行うことができない．そこで，NAT 変換を行う機器の前に無線 LAN 通信をミラーリングするためのエッジスイッチを別途用意し，そこで通信の監視を行う．

3.2 キャンパスネットワーク接続時の認証

キャンパスネットワークに接続される機器は，認証を行うことを前提とする．認証においては，メディアセンターが発行する ID とパスワードを用い，認証を通過した機器について通信を許可する．従来のキャンパスネットワークでは，エージェントプログラムをダウンロードさせるために Web 認証を用いていた．しかし，新しいネットワークではこのダウンロードは不要となるため，Web 認証の代わり

に 802.1x 認証を導入することとした．無線 LAN についてはすでに多くの OS で標準的に 802.1x 認証が可能な環境が整っている．そのため，本学では従来のネットワークから無線 LAN については 802.1x 認証を用いていた．また，有線 LAN に関しても 802.1x 認証の利用環境が徐々に整ってきた．これにより，有線 LAN についても 802.1x 認証を全面的に導入することとした．

新しいネットワークでは，有線 LAN・無線 LAN に関わらず，すべて 802.1x 認証となっている．一部の組み込み機器やその他の OS において正しく 802.1x 認証ができないものがまだ存在しているため，このような機器の認証においては MAC アドレス認証を別途用意する．専用の申請管理システムより機器情報と MAC アドレス情報を登録することで，自動的に MAC アドレス認証のデータベースが更新され，登録された機器はキャンパスネットワークに接続できるようになる．エッジスイッチでは，端末の接続が開始されると，まず MAC アドレス認証を実施し，MAC アドレス登録のない機器については 802.1x 認証を段階的に実施する．これらの流れを図 3 に示す．なお，図中に Web 認証が存在するが，これは移行時の措置として導入したものであり，現在は利用していない．

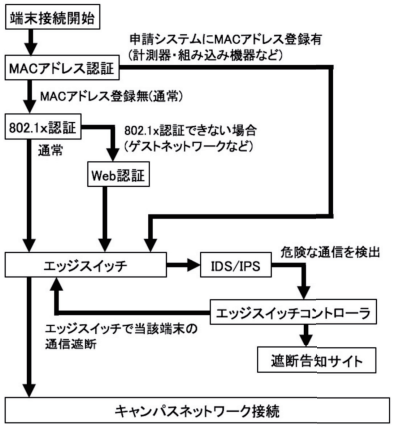

図 3　新キャンパスネットワークでの認証フロー

3.3 不正な機器の遮断処理

不正な通信を行う機器に対する処理はリスク発生後なるべく早く行われるべきである．しかし，これを対応する人員を 24 時間体制で配置することは難しい．そこで，隔離処理は自動で行われる必要がある．実際の自動遮断までのフローは図 4 に示す．もし，不正な通信を行う機器が発生した場合，まずミラーされたリングネットワークのパケットがトレンドマイクロ社製の Deep Discovery Inspector（DDI）[4]にて検出される．DDI では，その通信がどのようなものか，どの程度リスクがあるかを判定し，リスクが高いものに関しては，対象とする機器の情報とともに，トレンドマイクロ社製の Policy Manager（TMPM）[5]にデータが送信される．ここでは，遮断を行うかどうかの処理についてポリシーとマッチし，遮断が必要とされた機器については，その機器情報がアラクサラネットワークス社製の AX-Security-Controller（AX-SC）[6]に対して通知される．AX-SC は，問題のある機器が接続されたエッジスイッチのポート情報を把握しており，当該機器を遮断するようにエッジスイッチの設定を行う．これらの処理を自動的に行うことで，リスクの高い機器の自動遮断を行うことが可能となる．AX-SC では機器の移動についても追従するようになっており，問題のある機器が問題のある状態のまま別のエッジスイッチに移動したとしても，引き続き遮断が行われるようになる．

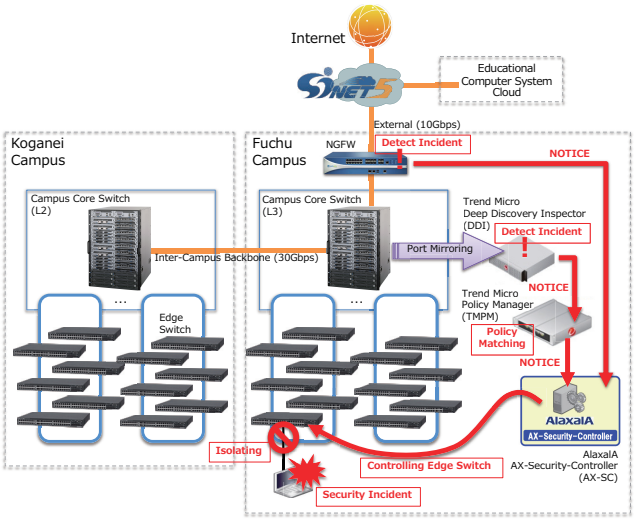

図 4　高セキュリティリスク端末の自動遮断プロセス

本学では，キャンパスネットワークとインターネットとの接続部にパロアルトネットワークス社製の次世代フィアウォールシステムを導入している．ここでも，通信セッション単位での不正通信の検知と遮断が可能となっている．ここまでに説明したエッジスイッチでの通信監視の他に，この次世代フィアウォールシステムで検知した情報を元に AX-SC を通じて不正な機器の遮断が行えるようになっている．このように複数の階層での遮断を行うことでよりセキュリティリスクを低減させる．

3.4 エンドユーザによる遮断解除処理

システムによって自動で遮断を行う場合，メディアセンターでの対応が出来ない時間帯（例えば深夜）であっても当然のことながら遮断処理が行われる．遮断が行われた後はユーザによるセキュリティリスクのある状況への対応が行われ，問題がなくなった場合に遮断状態を解除する必要がある．これらの処理についても自動で行えなければ，対応をする人員を配置する必要がある．遮断処理同様に，この人員の配置も難しい．そこで，ユーザ自身が遮断されている状況を確認し，自身で対処を行える仕組みが必要である．そこで，遮断状態を確認し，遮断状態の解除をユーザ

から申請できる仕組み（図 5，図 6）を用意している．

遮断された機器の情報は，学内のアカウントを持つユーザがアクセス可能な Web サイトに遮断が行われると自動的に掲載される．本学では Google 社の G Suite を契約しているため，遮断情報を掲載するサイトは G Suite の Google サイトおよび Google Apps Script を用いて構築している．この方式を取ることで，キャンパスネットワーク外からでも学内のアカウントを持っている人を限定したサイトを構築できる．キャンパスネットワークから遮断された機器を Web サイト等の閲覧に利用していた場合，その機器からは情報提供サイトにアクセスできなくなるが，他の機器（たとえばキャリア回線に接続された個人のスマートフォンなど）を経由して遮断情報を確認することも可能となる．

情報提供サイトには，その時点で遮断されている機器の情報として，IP アドレス，MAC アドレス，接続されていた場所などが掲載されている．遮断されたユーザはこの情報を閲覧し，当該機器に対するセキュリティ対応（例えばマルウェアの除去など）を行う．そして，セキュリティ的な脅威が取り除かれた場合に遮断解除申請を同サイトからユーザが行う．申請を受け付けた後の遮断状態の解除は自動で行う．定期的に隔離を一時的に解除して再度セキュリティ検査システムにパケットを送り，不正な通信が再度発見されれば再度遮断を行う．

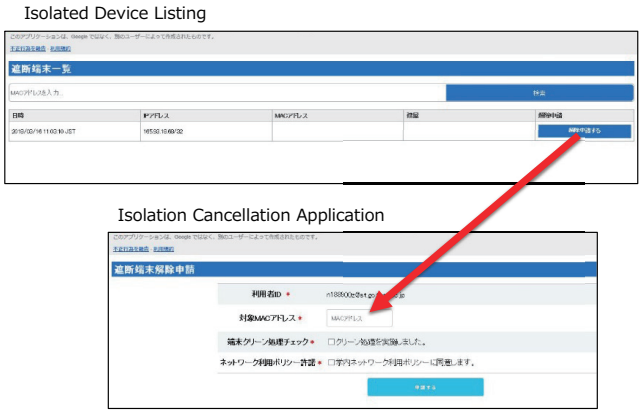

図 5　遮断状態の確認と解除申請フォーム

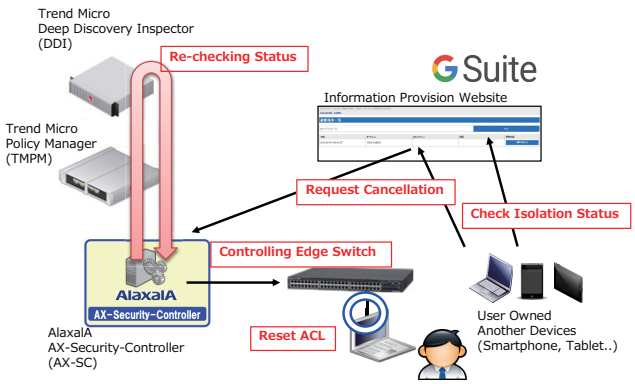

図 6　遮断解除のフロー

3.5 ホワイトリストによる例外処理

本システムでは，特殊な考慮をすべき危機への対応も可能としている．たとえば，セキュリティや P2P の研究にネットワークを利用する際，このシステムで問題のある通信と判定されてしまう可能性がある．本システムではホワイトリストによる例外通信を設定できる．しかし，この設定を行うことは全学ネットワークに対してセキュリティレベルを低下させてしまうことになるため，安易に設定を行うことは難しい．以前にこのような研究を行う際には，キャンパスネットワークとは別に独自のネットワークを敷設し研究を行うことを原則としていたことから，例外を認めるのか，独自にネットワークを敷設してもらうのか，といった判断を都度行う必要がある．

4. 実際の運用状況

本システムは 2018 年 5 月 7 日より運用を開始している．ここでは運用開始から 2019 年 3 月 26 日までの期間の運用に関連する状況を報告する．本学では，セキュリティリスクがきわめて高い通信（Critical なものにある程度限定）について自動遮断するように設定している．

4.1 遮断状況

当該期間に検知された不正な通信に対して本システムでの処理状況と端末の接続形態を図 7 に示す．システムで検知された不正な通信は 1140 件，このうち，自動遮断された通信は 150 件(13%)であった．遮断された端末のうち，122 件(81%)は有線 LAN に，残りの 28 件(19%)が無線 LAN に接続された状態であった．

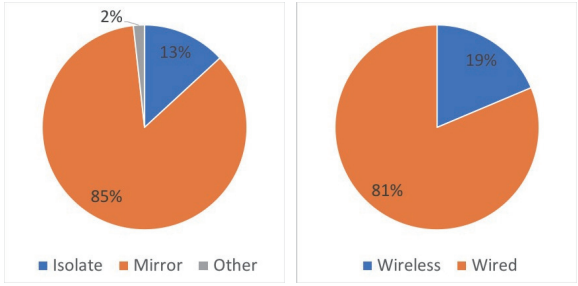

図 7　処理状況と端末の接続形態

当該期間の検知状況を週毎のタイムラインベースで図 8 に示す．年間を通じて週に 5 件程度，検知し自動遮断された通信が発生していることが分かる．数ヶ月に一度，特に多く検知されていることが分かる．5 月 13 日の週は運用開始段階であり，最初に多くの不正通信が検知されたことによる．10 月 28 日の週は特に検知数が多くなっており，グラフでは表現できていない．実際には，Wired が 38 件，Wireless が 1 件の計 39 件検知されている．すべての通信相

手は同一地域であり，不正通信の多くは同一地域に対して同時多発的に発生することが傾向から見られた．

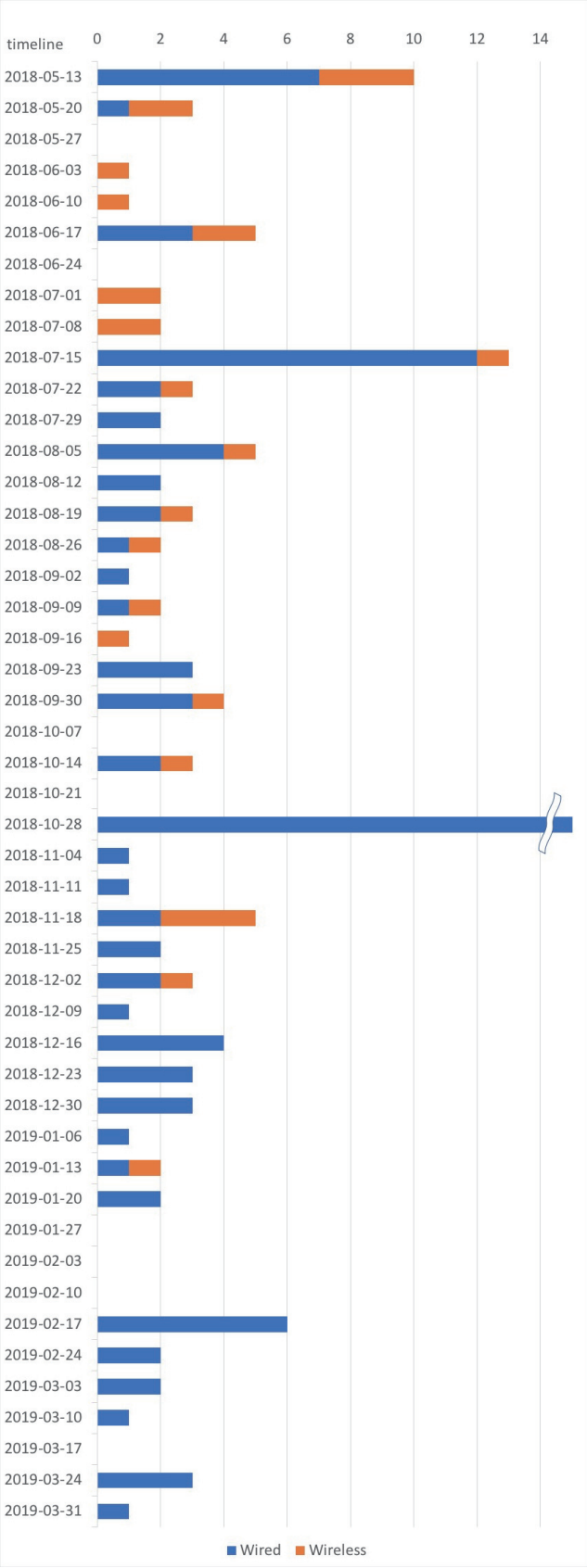

図 8　タイムラインベースの遮断状況

4.2　エンドユーザへの周知

運用を開始するにあたり，ユーザの端末が自動的に遮断されることから，ユーザに対して十分な周知を行う必要があった．そこで，運用開始前から図 9 に示すアナウンス用のポスターを作成し，学内の多くの場所に掲示した．この他，メディアセンターの Web サイトに自動遮断システムに関する FAQ 情報を掲載し，ユーザが確認できるようにしている．

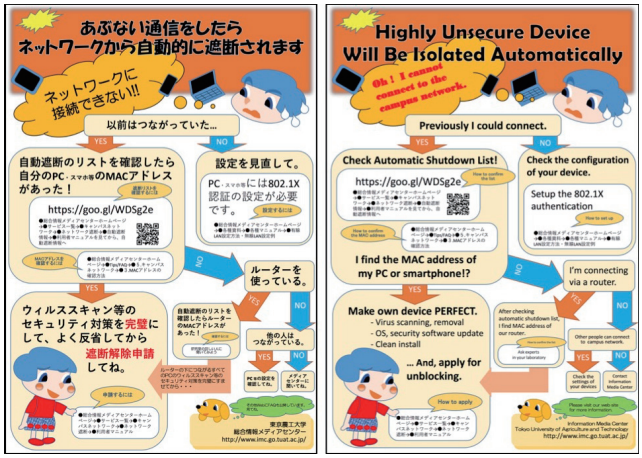

図 9　自動遮断システムに関するアナウンスポスター

5.　まとめ

本論文では，不正な通信をする危険な端末を自動的にキャンパスネットワークから隔離する仕組みを持つ新しいキャンパスネットワークシステムについて述べた．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る上，本システムではネットワーク側で対処するため組み込み機器にも対応でき，セキュリティを高めていくことが可能となる．

本システムでは，検知された不正通信のレベルに応じて遮断を行うかの対処を選択できる．これをどの程度のレベルとして設定するかで，機器に対する負荷や遮断時のユーザ対応のコストに大きく影響する．今後，これらのレベルをどう設定していくかを運用しながら設定していくことになる．

謝辞 本システムの導入にあたって，櫻田武嗣氏，エイチ・シー・ネットワークス株式会社様，トレントマイクロ株式会社様，アラクサラネットワークス株式会社様にご尽力いただきました．また，本稿の作成にあたって，東京農工大学総合情報メディアセンター職員各位に協力をいただいております．謹んで感謝の意を表します．

参考文献

[1] エイチ・シー・ネットワークス株式会社: マルチ OS 対応の大規模な検疫ネットワークを導入, URL: https://www.hcnet.co.jp/case/noukou.html [web] (2020/01 参照)
[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, 情報処理学会研究報告, IOT, [インターネットと運用技術] 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, 情報処理学会研究報告, IOT, [インターネットと運用技術] 2013-IOT-20(9), pp.1-6 (2013).
[4]トレンドマイクロ株式会社: Deep Discovery Inspector, URL: https://www.trendmicro.com/ja_jp/business/products/network/advanced-threat-protection/inspector.html [web] (2020/01 参照)
[5] トレンドマイクロ株式会社: Trend Micro Policy Manager, URL: https://www.trendmicro.com/ja_jp/business/products/policy-manager.html [web] (2020/01 参照)
[6] アラクサラネットワークス株式会社: AX-Security-Controller, URL: http://www.alaxala.com/jp/products/AX-SC/index.html [web] (2020/01 参照)