学術情報処理研究 No.21
2017年9月

アクセス制限機能を提供するキャンパスネットワークの実装と評価

Implementation and Evaluation of Campus Network System providing Access Control Function

近堂 徹, 田島 浩一, 吉田 朋彦, 岸場 清悟, 岩田 則和, 西村 浩二, 相原 玲二

Tohru Kondo, Koichi Tashima, Tomohiko Yoshida, Seigo Kishiba, Norikazu Iwata, Kouji Nishimura, Reiji Aibara

{tkondo, tashima, tyoshi, kishiba, norita, kouji, ray}@hiroshima-u.ac.jp

広島大学情報メディア教育研究センター
Information Media Center, Hiroshima University

概要

外部からの不正侵入アクセスによる情報漏洩・データ改ざん等のセキュリティインシデントに対する対策が強く求められている。大学等の高等教育機関ではグローバル IP アドレスを付与した機器が多く存在しているが，これらを管理する構成員に対して適切な設定を徹底することが困難な面が存在する。広島大学ではキャンパスネットワークにおける IP アドレスや VLAN 等のネットワーク資源を一元管理することで，ネットワークに接続されるホストの把握を徹底してきた。さらに，ホストに対するアクセス制限機能をネットワーク側で提供することで，簡易な操作設定でアクセス制限を適用することを可能としている。本論文では，インターネットに公開されるグローバルホストのセキュリティ対策のひとつとして，アクセス制限機能を提供するキャンパスネットワークの実装と評価について述べる。脆弱性診断サービスの分析結果から，本アクセス制限機能の有効性について述べる。

キーワード

キャンパスネットワーク，グローバル IP アドレス, アクセス制御リスト, 自動設定, 脆弱性診断

1 はじめに

大学などの高等教育機関におけるキャンパスネットワークは，教育研究活動から管理運営業務に至る様々な活動を支える主要インフラとして必要不可欠なものとなった。研究室におけるネットワーク利用のみならず，モバイル端末等を活用した授業支援や学外者も含めた BYOD(Bring Your Own Device) 環境の提供，事務系の基幹業務での利用など，その利用形態は多種多様となっている。単にインターネット接続性を提供するだけでなく，安全かつ安定性を確保しながらも利用者の利便性を損なわないことが求められる。

教育研究を支えるネットワークとしては，一般的なサーバのほか，プリンタやストレージ等のサーバや実験装置・機器なども多数接続されることが前提となる。しかしながら，インターネットからアクセス可能な機器を設置するには，外部からの不正侵入アクセスによる情報漏洩・データ改ざん等のセキュリティインシデントには細心の注意を払うことが必要となる。最近では，プリンタ等の複合機で印刷内容やスキャン内容が外部からアクセスできる状態となっていたケースや NAS（Network Attached Storage）で適切なアクセス制限が行われておらず外部公開されていたケースなど，社会的問題として広く知れ渡ることとなった [1]。このような問題を防ぐためには，結果的に安全性を維持するための多くの時間的コストと知識が必要とされる。機器を所有する学内構成員が適切に管理運用できることが望ましいが，

その対応にばらつきが生じてしまう問題が存在する。

一方，ネットワーク運用管理者の視点でみると，セキュリティレベルが異なる多様なサーバ機器がネットワークに接続される状況になる。この状況に対して，如何に利用状況を確実に把握し，障害発生時やセキュリティインシデント時に迅速かつ適切な初動対応が取れるかが重要になる。また，ネットワーク側でもセキュリティ対策を行う機能を提供することで，接続される機器に対する管理者への管理負担を軽減できることが望ましい。これまでキャンパスネットワークにおける IP アドレスの管理方法 [2] やグローバル IP アドレスに対するアクセス制限 [3] に関する取り組みなど，数多く行われてきている。またネットワーク接続ログを分析することで利用状況を適切に把握することも日常的に行われるようになってきている [4]。

本論文では，サーバ機器の適切な把握と運用を目的としたキャンパスネットワークの設計と評価について述べる。具体的には，ネットワークの一元管理によりサーバ機器の利用者を適切に把握する仕組み，利用申請に基づきサーバ機器に対してアクセス制限リストを自動適用する機能，さらにはサーバ機器に対する定期的またはオンデマンドの脆弱性診断機能の提供，によるサーバの運用管理を支援する仕組みについて述べる。さらに，実際に広島大学キャンパスネットワークでの運用を通して得られた効果と課題についてまとめる。広島大学では，インターネットからアクセス可能な学内ホスト（以下，グローバルホストとよぶ）に対して，ホスト側とネットワーク側の両ポイントでの適切なアクセス制限を求めており，2017 年 5 月からはネットワークによるアクセス制限機能の有効化を導入した。本論文では特に，本アクセス制限機能（以下，ACL 機能とよぶ）の有効化によるグローバルホストのセキュリティ向上に対する効果を中心にまとめる。これらの取り組みを通して，キャンパスネットワークにおけるグローバルホストの管理手法の有効性について述べる。

以降，2 章では広島大学キャンパスネットワークの概要とグローバルホストの管理方法について述べる。3 章では，利用者からの申請に基づく ACL の自動設定について示す。4 章では，本 ACL 機能による効果と課題について，グローバルホストに対する脆弱性診断の傾向の分析と考察を行い，最後に 5 章でまとめを行う。

2 広島大学キャンパスネットワーク HINET

本章では，広島大学のキャンパスネットワーク HINET について概説し，主にグローバルホストの管理方法について述べる。

2.1 HINET2014 の概要

HINET2014[5] は広島大学で 2014 年 8 月より運用しているキャンパスネットワークである。データセンターに設置するコアネットワーク装置でレイヤ 3 の機能を集約し，学内はレイヤ 2 フラットなスター型のネットワークとなっている。2007 年度に整備した約 450 台の建物集約スイッチ・フロアスイッチの各ポートの設定までを情報メディア教育研究センターが集中管理している。

HINET では，一般の利用者でも容易に理解できることを狙って，学内外からのアクセス拒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。図 1 に主要なゾーン構成を示す。ゾーン A（グローバルゾーン）はインターネットからアクセス可能なゾーン，ゾーン B（ファイアウォールゾーン）とゾーン D/HINET Wi-Fi（公衆ゾーン）は学内限定アクセスのゾーンである。ゾーン A とゾーン B は固定 IP アドレスに対して MAC アドレスを登録し利用する有線接続，ゾーン D は DHCP による動的 IP アドレスとウェブ認証で利用する有線接続，HINET Wi-Fi は WPA2/PEAP 認証で利用する無線接続を提供している。したがって，学外公開が前提となるホストはゾーン A, 複数のゾーン C やゾーン D から利用するプリンタや NAS 等の学内限定ホストはゾーン B に設置し，BYOD 等のクライアントはゾーン D/HINET Wi-Fi の利用を想定している。ゾーン C（ローカルゾーン）は研究室単位での利用を想定したゾーンであり，ひとつのゾーン C につき/24 のプライベード IP アドレスを利用する。

次にこれらのゾーンを実現するためのファイアウォール構成について説明する。HINET のレイヤ 3 論理構成を図 2 に示す。コアネットワーク装置として，L3 スイッチには Cisco Catalyst 6807-XL(VSS 構成)，IPS/IDS およびファイアウォールには Cisco ASA5585-X/SSP60(Active-Standby 構成) を利用している。L3 スイッチは VRF 機能により 3 つの独立した仮想 L3 スイッチを定義し，L3 スイッチ間の相互通信はファイアウォール経由で行う。全学ファイアウォールではゾーン A およびインターネットとの通信に対するフィルタリングを行う。個別ファイアウォールでは NAPT によるアドレス変換を行い，ゾーン C あたり/24 のプライベード IP アドレスを 1 つのグローバル IP アドレスに変換して外部アクセスを行うとともに，通信に対するフィルタリングを行う。あらかじめゾーン C を 2,000 作成し，対応する 2,000VLAN の収容および個別ファイアウォールへのルーティングは部局 L3 スイッチが行う。

HINET は全学的に統一された明確なポリシーでゾーンを提供し，ファイアウォール設定の個別対応などを行わないことを基本方針としている。これにより，利用者自身が各ゾーンのポリシーを理解したうえで，必要なセ

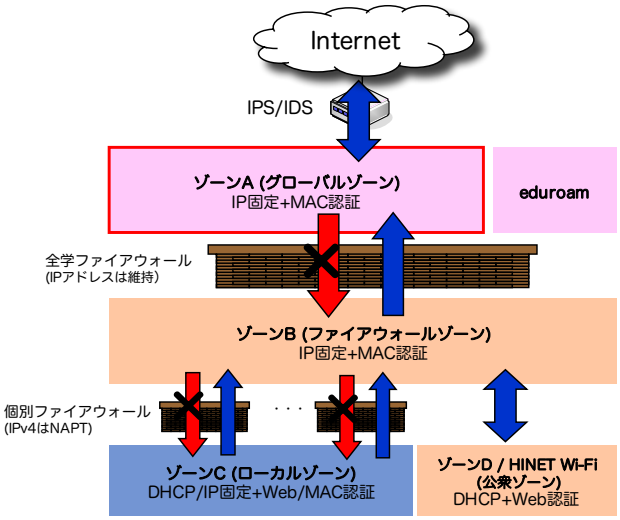

図- 1: HINET におけるゾーン構成

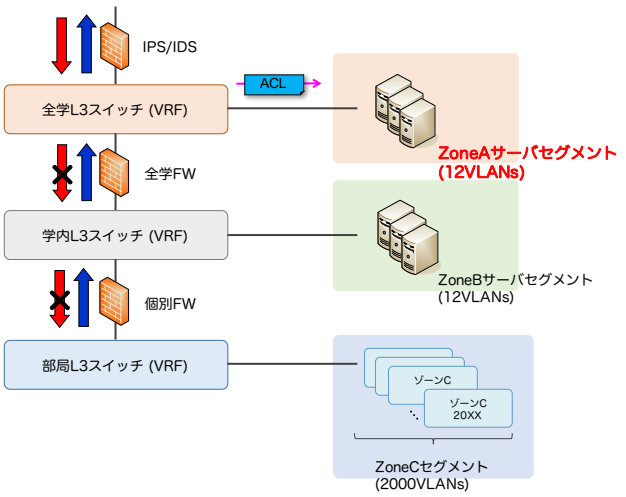

図- 2: HINET のレイヤ 3 論理構成

キュリティ対策を実施することを目指している。

本キャンパスネットワークの大きな特徴が「ネットワーク構成と資源の一元管理」と「設定の自動化」である。IP アドレス（IPv4, IPv6）や VLAN ID などのネットワーク資源はメディアセンターで全学一元管理となっており，利用者からの申請をオンライン申請により直接受付け，希望するフロアスイッチのポート設定（VLAN や認証設定）や IP アドレスの割当等の処理を自動で行う。自動設定の要件として，約 450 台のフロアスイッチと L3 コアネットワーク装置に対する自動設定を，申請から完了まで 3 分以内で実施することを目標に構築している [6]。

2.2 グローバルホストの管理運用

前節で示した HINET の主要ゾーンのうち，インターネットからアクセス可能なゾーンはゾーン A となる。ゾーン A は，IPS/IDS と全学ファイアウォールの間の L3 スイッチ（VRF）がルーティングポイントとなり，12 の VLAN（1 つの VLAN あたり /24 のネットワーク）を用意することで，合計で約 3,000 のグローバルホストを収容することが可能な設計になっている[1]。ゾーン A にグローバルホストを設置する場合，利用者（管理者）がネットワーク利用申請サービス（後述）で申請することにより，IP アドレスの割当が行われると同時に，接続を希望するフロアスイッチのポートに対して VLAN の設定と MAC アドレス認証の設定が行われる。登録された MAC アドレス・IP アドレスと管理者の学内 ID と紐づけることで「いつ・どこで・誰が管理する・どの IP アドレスのグローバルホストが接続されたか」をネットワーク管理者側で迅速に把握できることが可能となっている。

[1] ネットワーク資源が一元管理のため，今後拡張することも可能

2.3 脆弱性診断の導入

ゾーン A はインターネットから常にアクセスが可能なゾーンであり，そこに設置するホストにも確実なセキュリティ対策が求められる。セキュリティホールや設定の不備などによる脆弱性を塞ぐことが必要となるが，全ての管理者に対して自身の判断で対応を求めることは難しく，また徹底することも容易ではない。そこで，グローバルホストを対象とした脆弱性診断サービスを提供することで，管理者に対して問題となる箇所を正しく認識させ，適切な対策の実施を進めている。脆弱性診断は広島大学外のネットワークセグメントに設置したサーバから実施することで，インターネットからのアクセスに対する脆弱性を発見することができる。月 1 回の定期診断のほか，管理者がオンデマンドに実施することが可能であり，客観的な評価基準に基づいたグローバルホストの安全性を確認することができる。診断結果は，ネットワーク利用申請サービスの管理情報から該当ホストの管理者に対してフィードバック可能である。脆弱性診断の取り組みについては文献 [7] を参考いただきたい。

3 グローバルホストに対する ACL 機能の実現

3.1 利用申請サービスによる自動設定

グローバルホストに対するセキュリティ対策としては，ホスト単体でのセキュリティ対策はもちろんのこと，複数箇所での対策を講じることで安全性を高めることができる。HINET ではこの考えに基づき，ネットワーク境界で導入する IPS/IDS に加え，ゾーン A に対してネットワーク側で設定する ACL 機能を提供し，ホストに対する通信を制御できるようにした。これによ

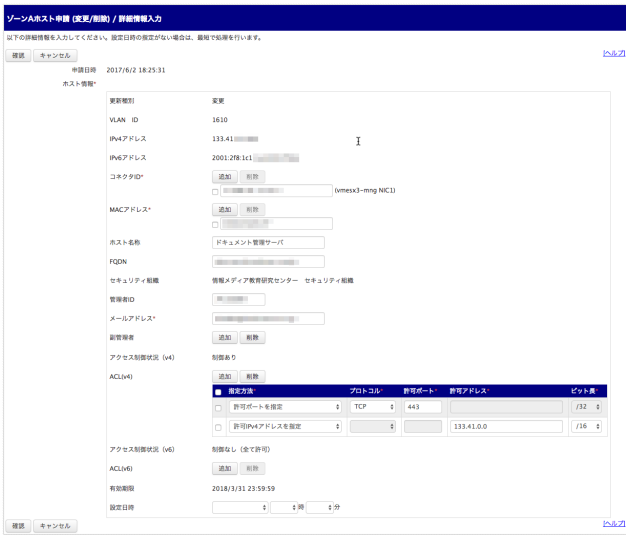

図- 3: ネットワーク利用申請サービスの設定画面例

り，グローバルホスト自体でのアクセス制限の設定に加えて，本 ACL 機能を利用した 2 重のセキュリティ対策が可能となり，ホスト側の設定の不備を防ぐだけでなく，アクセス制限設定が難しい機器等に対してもセキュリティ機能を提供することが可能になる。

本 ACL 機能ではホワイトリスト方式により「指定したネットワークからのアクセスのみを許可（許可 IP アドレス）」「指定したポート番号へのアクセスのみを許可（許可ポート）」を提供する。許可 IP アドレスと許可ポートの併用も可能であり，その場合いずれかの条件にマッチすれば許可される。また IPv4, IPv6 の両プロトコルに対応しており，それぞれで独立した ACL を適用することができる。管理者はネットワーク利用申請サービス（図 3）を通じて各種申請を行う。許可 IP アドレスの指定では，/24 から /32 までのネットワークマスクを指定することで，ホスト単位またはネットワーク単位での指定が可能である。許可ポートの指定は，UDP・TCP・両方から選択して許可ポートを指定する。入力された値はパラメータチェックを行うことで例外を排除し，ACL 生成・適用時のエラーを回避している。

ACL は VLAN 毎に生成され，図 2 に示した全学 L3 スイッチの SVI(Switched Virtual Interface) の outside 方向に対して適用する。制御の流れを図 4 に示す。ネットワーク利用申請サービスで管理者からの申請を受理すると，ACL 記述内容がネットワーク管理サービスに送られ，ACL エントリの生成・確認および L3 スイッチの制御が行われる。ネットワーク管理サービスでは申請情報から生成される各種設定の管理や機器の制御を担っている。

一例として ACL の設定内容を図 5 に示す。ACL は申請された情報に基づき定義されるエントリのほか，内部発の TCP 通信を許可するために「established」オプ

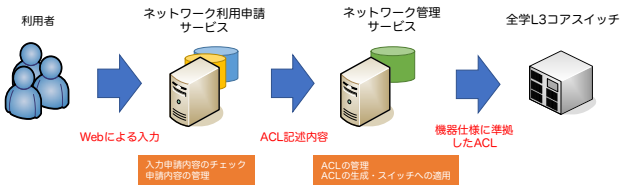

図- 4: 制御の流れ

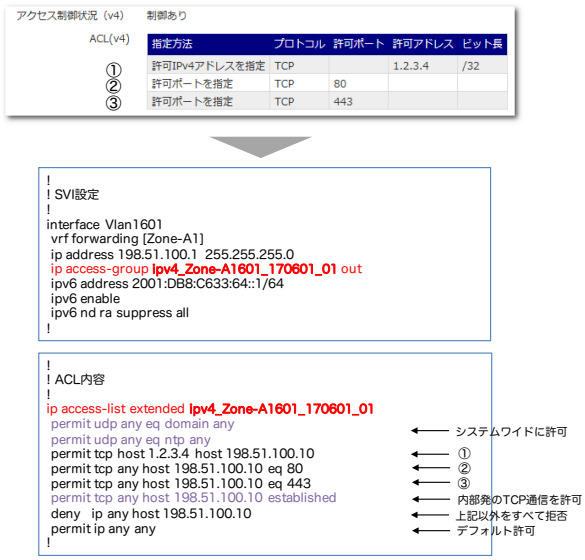

図- 5: ACL の設定例（IPv4 の場合）

ションをつけた ACL とそれ以外を全て拒否するエントリが追加される。つまり，1 ホストあたり申請されたエントリに 2 つのエントリが追加されたものが設定されることになる。また，DNS(53/udp), NTP(123/udp) の戻り通信を許可するためのエントリが ACL に対して標準で設定される。ACL 名称は VLAN 毎にユニークにするために ”ipv4_Zone-A_VLANID_YYMMDD_通し番号” としている。

ホスト毎に ACL 更新が発生した場合，該当する VLAN で ACL 名称を更新して再作成し，再作成した ACL を SVI に対して再適用する。SVI への ACL の差替えが成功した場合、古い ACL は削除する。一方，ACL 差し替えが失敗した場合、古い ACL の削除は実施せずエラーを返す。なお，ACL を重複して同時適用することがないように，ネットワーク管理サービスにて ACL 適用のキューイング制御が行われる。

3.2 ACL 機能の有効化

広島大学では本 ACL 機能を 2014 年 12 月より提供し，管理者に対してグローバルホストに対するアクセス制限の促進に取り組んできた。しかしながら，設定については任意としてきたため，十分に浸透させることが

できていなかった[2]。その一方で，TELNET ポートが稼働する IoT 機器の普及やこれらを踏み台にするボットネット等の拡大等，インターネットからアクセス可能なホストに対してより強固なセキュリティ対策が求められるようになってきた。

このような背景から，2017 年 4 月より本 ACL 機能の初期有効化を導入し，さらに既存のグローバルホストに対しても本機能によるアクセス制限設定の徹底を図った。初期有効化については，ゾーン A の新規申請時に学内限定（IPv4, IPv6）のアクセス制限が設定された状態を初期状態とし，申請者（管理者）自身で適切なアクセス制限設定を求めた[3]。また既存ホストの有効化については，各管理者に対して複数回の設定依頼の案内を行なったのち，期日までに IPv4, IPv6 のいずれの ACL エントリも存在しないホストに対してはメディアセンター側で一律学内限定の設定を実施することとした。具体的には以下のスケジュールで進めた。

2017 年 4 月 1 日 新規申請に対する初期有効化の実施

2017 年 4 月 5 日 既存ホストに対する有効化の周知と除外申請受付の開始（設定期限：4 月 30 日まで）

2017 年 4 月 18 日 管理者への DM による再周知の実施

2017 年 5 月 1 日 ACL 未設定のホストの管理者に対する最終通知（設定期限：5 月 7 日まで）

2017 年 5 月 8 日 ACL 未設定のホストに対する学内限定 ACL の適用

なお，本 ACL 機能で満たすことのできないアクセス制限が必要と申告されたホストについては，除外申請を受け付けることで本適用から除外されている。

4 月 5 日の周知開始時点で適用対象となる既存グローバルホストは 466 であった。上記スケジュールからもわかるように既存ホストに対するアクセス制限の有効化作業は，周知から適用まで約 1ヶ月の期間で行った。これにより，除外申請分を除いたゾーン A のホストに対してアクセス制限が適用された。各ホストに対して管理者 ID に紐づけた管理をシステム側で行なっていたため，管理者個人に対する DM による事前周知が徹底され，大きな混乱はなかった。DM にはメディアセンターウェブページに用意した設定例や操作方法に関する説明ページ[4]へのリンク情報を含めることで，管理者自身での設定作業を促した。

一方で，上記期間中にヘルプデスク宛に 10 件の問い合わせがあった。主な内訳としては，本 ACL 機能の機能改善として，ACL エントリに対するメモ機能の追加とポート範囲の指定機能に関する要望が 2 件，TV 会議システムのための ACL 設定例の確認，他ゾーンでの ACL 適用の必要性の確認，アクセス制御の適用方向の確認等，設定に関する技術的な質問が 7 件，DM に対する設定完了の確認連絡が 3 件であった。

なお，ACL エントリはネットワーク利用申請サービスより変更・修正し，即時反映させることが可能であるため，2017 年 5 月 8 日以降であっても管理者の権限で設定し直すことが可能である。

4 考察

本章では，ACL 機能の有効化による効果と課題について，脆弱性診断サービスの分析結果も踏まえて考察する。

4.1 ACL 機能の有効化による効果

図 6 に本 ACL 機能によるアクセス制御の設定率の推移を示す。設定率は，ゾーン A に登録済のグローバルホストのうち 1 行以上の ACL エントリを設定したホスト数の割合を示している。IPv4 と IPv6 でそれぞれ独立して設定可能であるため，ぞれぞれの設定率を求めた。この結果からもわかる通り，2017 年 3 月まではおおよそ 10%程度 (IPv4 の場合) の設定率で推移してきており，必ずしも設定を徹底できている状態とはいえなかった。一方，2017 年 4 月 5 日のの周知以降に設定率が向上していることがわかる。前節でも述べた通り，4 月 5 日から 5 月 8 日までの間，DM にて管理者に対して複数回の連絡を行なっているため，その直後に若干まとまって設定が行われた傾向がみられたが，5 月 7 日の時点で登録済ホストの約 50%に対して管理者自身でのアクセス制限が設定されている。5 月 8 日には，ACL 未設定ホストに対して学内限定 ACL の適用をメディアセンター側で実施したため，設定率が 90.04%となった。設定率が 100%でない理由は，事前の除外申請により ACL 適用を行わなかったホストが存在するためである。なお，IPv4 と IPv6 の比較を行うと，IPv6 の ACL 設定率が 10%程度低くなっている。これは管理者自身で設定したエントリが IPv4 のみのホストが存在することを意味している。実際，ゾーン A ではホストに対して IPv4 アドレスと IPv6 アドレスの割当が行われるが，IPv6 を利用しない場合に ACL 適用の必要性がなかったためと考えられる。

また自動設定に要する時間を調べるため，4 月の 1ヶ月間の申請のうちで単一ホストに対して IPv4 と IPv6 の両方で ACL を適用した申請（86 件）について，申請

[2] ホスト側でのアクセス制限については本学セキュリティポリシーでも定めている

[3] エントリを削除することでアクセス制限ルールの変更が可能

[4] http://www.media.hiroshima-u.ac.jp/services/hinet/ZoneA-ACL (2017-7-19 参照)

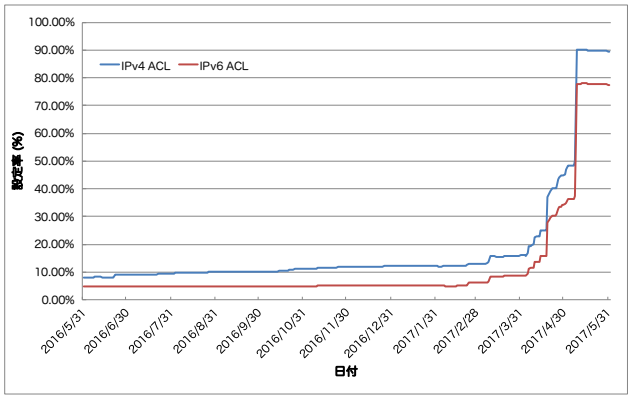

図- 6: アクセス制御設定ホスト数の推移

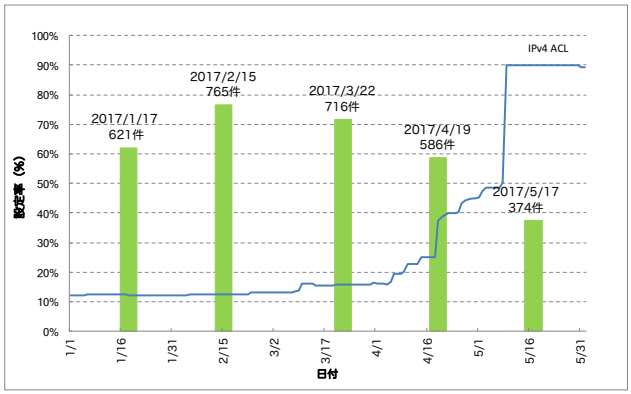

図- 7: IPv4 ACL 設定率と脆弱性診断サービスでの警告数の推移（線グラフ：設定率，棒グラフ：警告数）

から適用までに要した時間を計算した結果，平均で 4 分 4 秒であった。これは複数の同時申請により生じた待ち時間も含まれている。おおよそ 6 割の申請が 3 分以内で完了しており，定常時であれば同様の時間で自動設定が行われることも確認している。

4.2 セキュリティ脆弱性診断結果の分析

次に，本 ACL 機能の導入による外部からのアクセスに対するセキュリティ対策の効果を示すために，学外に設置したサーバからの脆弱性診断サービスの定期診断結果を用いた評価について述べる。図 7 に，ACL 設定率と 2017 年 1 月から 5 月に実施した計 5 回の脆弱性診断サービスでの警告数の推移を示す。警告数は，本サービスで利用している Nessus[5]により Security Warning もしくは Security Hole として検出された数を合計したものである。この結果から，2017 年 1 月から 5 月までの間で，ACL 設定率が 12%から 90%まで増加したのに対して，警告数は 765 件から 374 件と約半分にまで減少する結果となった。外部からのアクセスによる脆弱性に対して適切な ACL 設定が効果的に機能していると考えられる。

ACL の効果をより詳細に確認するために，2017 年 1 月時点での警告数上位 18 台のグローバルホストを対象とした警告数の推移を表 1 に示す。なお，表中の最右列は ACL が未設定から変更された（初めて ACL エントリが記述された）日付を示しており，(*) が付いている箇所は，期限内に管理者による設定が行われず，メディアセンター側で一律に学内限定設定を実施したことを表している。この結果から，管理者による ACL 設定により警告数が 0 となったホスト（A, D, F, L, Q）やメディアセンターによる一律設定で警告数が 0 となったホスト（J, K）が見られることがわかる。また，0 とはならないものの，多くのホストで脆弱性の警告数を低減できていることが確認できた。必ずしも警告数が 0 とならないのは，例えば 80 番と 443 番を許可するような Web サービス内で存在する脆弱性への対応ができていない等，プログラム内部の脆弱性を検知しているためである。現状のアクセス制限では難しい脆弱性に対してはホスト側での対応が必要となるものの，事前にネットワーク側で不必要なアクセスを拒否することによる効果が確認できた。

一方，ACL 初回設定後に警告数が上昇しているホスト（C, E）も存在する。これは初回設定日以降に管理者自身がアクセス制限を緩和する設定を行ったことで，効果が低減したことを意味している。ホストの設定状況を適切に把握することで，管理者に対する ACL 機能の利用の周知徹底を進めていくことが必要となる。

4.3 課題

本 ACL 機能の導入により，ホスト管理者自身がネットワーク利用申請サービス（ウェブインタフェース）からの簡易な操作によりネットワーク側でアクセス制限を実施することが可能になった。その一方で，現時点でいくつかの課題が残されている。

1 点目に ACL 記述方法の拡充である。現時点では許可ポートの範囲指定ができないため，TV 会議システム等での範囲指定が必須な ACL を表現することができず，これが除外申請を受け付けた理由のひとつとなっている。実際，利用者からもこの点に関する機能改善の要望があり，改修を実施した。また，現状のホワイトリスト方式に加えて，ブラックリスト方式による拒否 IP アドレス，拒否ポートの列挙ができると，より細かい制御が可能になる。しかし，ホワイトリストとブラックリストの混在は ACL 適用順序を意識したエントリ記述と ACL 生成が必要となるため，ネットワーク側の機能としてどこまで提供するかの見極めが必要となる。

[5] https://www.tenable.com/products/nessus-vulnerability-scanner (2017-6-5 参照)

表- 1: セキュリティ診断結果の推移（2017 年 1 月時点での警告数上位 18 台のホストを対象）

ホスト	脆弱性診断による警告数					ACL 初回設定日
	1 月 17 日	2 月 15 日	3 月 22 日	4 月 19 日	5 月 17 日	
A	63	64	29	0	0	3 月 7 日
B	47	47	45	23	23	4 月 10 日
C	45	50	50	11	32	4 月 18 日
D	32	33	33	0	0	4 月 18 日
E	30	33	32	30	33	5 月 8 日 (*)
F	29	34	34	34	0	5 月 3 日
G	29	29	29	29	29	5 月 8 日
H	26	30	30	30	6	5 月 3 日
I	20	22	20	20	20	5 月 8 日
J	17	18	18	18	0	5 月 8 日 (*)
K	17	20	20	18	0	5 月 8 日 (*)
L	16	17	0	0	0	3 月 10 日
M	15	17	17	17	0	5 月 8 日 (*)
N	14	14	12	14	0	5 月 8 日 (*)
O	14	16	16	16	15	4 月 20 日
P	14	15	15	15	5	5 月 8 日 (*)
Q	11	10	10	0	0	4 月 9 日
R	10	10	10	10	9	5 月 8 日 (*)

2 点目に ACL エントリ数の上限値の設定である。現在，設定できるエントリ数の上限を 1 ホストあたり 10 エントリ（IPv4，IPv6 で独立）としている。これは，コアネットワーク装置の TCAM 容量の上限とゾーン A で収容できるホスト数の最大値（約 3,000）から，全ホストで ACL を記述してもネットワーク装置の動作に影響がないことを考慮して決定した数値である。このように，ACL エントリ数については管理者の申請に基づく自動設定を行なっているため，装置のリソースやパフォーマンスを考慮しながら適切に上限を設定する必要がある。しかし，1 点目で述べた許可ポートの範囲指定が可能になれば，現状の上限 10 エントリで現在除外申請により適用を除外しているホストも収容できる見込みである。

3 点目に管理者に対する ACL エントリ適用の可視化がある。現在，設定した ACL が正しく適用されたか（許可されたもの以外がドロップされたか）を確認するには，実際に試してみるしかない。本 ACL が正しく効いているか，アクセスのログも含めて確認する手段を提供することで，より効果的な適用ルールの策定が可能になると考えられる。

最後にアクセス制限で防げない脆弱性への対応がある。本論文で示した ACL 機能は，グローバルホストに対する不要なアクセスに対する対策を目的としたものであるため，プログラムに内在する脆弱性や設定の不備については防ぐことはできない。これについては脆弱性診断サービスの適切なフィードバックにより，管理者によるアップデート等を徹底していくことが必要となる。また，現在学外サーバからの脆弱性診断のため，学内限定 ACL が適用されたホストに対しては潜在的な脆弱性検出ができない。学内サーバからの脆弱性診断を組み合わせることで根本的対策を提示していく必要がある。

5 まとめ

本論文では，インターネットに公開されるグローバルホストのセキュリティ対策のひとつとして，アクセス制限機能を提供するキャンパスネットワークの実装と評価について述べた。

これまで一般的に利用されている Linux や Windows サーバ等の OS だけでなく IoT 機器の普及により，これらを踏み台にするボットネット等が広がっている。セキュリティ対策の基本として，「最低限必要なポート以外への侵入を防止する」「特定の IP アドレスからの接続以外が不要な場合は制限する」といったアクセス制限の重要性は高いが，多種多様な機器が接続されるキャンパスネットワークでは，管理者自身で安全を維持するためのコストも無視できなくなってきている。

広島大学では，キャンパスネットワークにおける IP アドレスや VLAN 等の資源を一元管理することで，ネットワークに接続されるホストの把握を徹底してきた。さらに，グローバルホストに対するアクセス制限機能をネットワーク側で提供することで，簡易な操作設定でグローバルホストに対してアクセス制限を適用することができるようになった。

本 ACL 機能の導入の効果を示すために，定期的に実施している脆弱性診断サービスの診断結果を示すことで，導入後に警告数が大きく減少したことが確認した。特に，これまで多数の警告が出ており対策が進んでいないと考えられた一部のホストで，アクセス制限設定後に警告数の大きな減少が見られたことで導入の効果が確認された。

今後は，4.3 節でも示した通り，本 ACL 機能のさらなる機能拡張を図っていく。さらに，脆弱性診断サービ

スとの連携よる対応が十分でないホストに対する適切な ACL エントリの提示やセキュリティ対策のフォローも検討していく予定である。

謝辞

日頃よりキャンパスネットワークシステムの管理運用にご尽力頂いている，情報メディア教育研究センターユーザーサービス部門のスタッフ各位をはじめ，関係者の皆様に感謝致します。またシステム開発および日々の運用にご尽力頂いている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致します。

参考文献

[1] 情報処理推進機構, ネットワーク対応機器を利用する際のセキュリティ上の注意点, https://www.ipa.go.jp/security/announce/20150317-netdevice.html (参照：2017-6-5)

[2] 清水さや子 ほか, キャンパスネットワークにおけるネットワーク監視機能の運用評価と今後の展開, 学術情報処理研究 No.19, pp.3-11, 2015.

[3] 嶋田創 ほか, 名古屋大学における全学ファイアウォールの段階導入と運用, 情報処理学会研究報告, 2016-IOT-35(6), pp.1-8, 2016.

[4] 鳩野逸生, ネットワーク接続記録収集によるネットワーク利用状況把握の試み, 情報処理学会研究報告, 2016-IOT-35(15), pp.1-7, 2016.

[5] 近堂徹 ほか，クラウドコンピューティング活用のための大規模キャンパスネットワーク, 情報処理学会 インターネットと運用技術シンポジウム (IOTS)2014 論文集, pp.101-108, 2014.

[6] 近堂徹 ほか, 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, 57(3), pp.998-1007, 2016.

[7] 田島浩一 ほか，広島大学におけるセキュリティ脆弱性診断の実施とその評価, 学術情報処理研究 No.18, pp.16-23, 2014.