デジタルプラクティス　Vol.11 No.3(July 2020)

一般投稿論文

学外公開アドレス管理システムの設計と評価

佐藤 彰洋[1]　福田　豊[1]　和田 数字郎[1]　中村　豊[1]

[1]九州工業大学

国立大学法人において，サイバー攻撃によるセキュリティインシデントが多発している．その攻撃に抗するため，我々が属す九州工業大学情報基盤運用室では学外公開アドレス管理システムを構築した．本システムの特徴は，学外公開，すなわち学外から到達可能なIPアドレスを付与した機器に関する情報共有と，それに対する措置として脆弱性改善と通信制御を実現したことにある．その導入により，本学のネットワークにおいて高い堅牢性の実現を確認した．本稿では，学外公開アドレス管理システムの設計と，12カ月にわたるシステムの運用による有効性の評価，そこから得られた知見について報告する．

1. はじめに

昨今，国立大学法人において，サイバー攻撃によるセキュリティインシデントが多発している[1]．たとえば，脆弱なパスワードの設定による不正アクセスやWebサイトの改竄，ネットワークに接続する複合機の不備による情報漏洩などの事案である．このようなセキュリティインシデントが発生した場合，法人としての信用失墜を招くだけでなく，その法人を取り巻く関係者に多大な影響を及ぼすことになる．故に，セキュリティインシデントの発生防止に向けた対策の推進は，法人全体として取り組むべき責務となる．

九州工業大学では，情報セキュリティの更なる強化を図るため「情報セキュリティ対策基本計画」を2016年に策定し，その実施に取り組んでいる．この基本計画で定められた一項目「情報機器の管理状況の把握及び必要な措置の実施」に則り，我々が属す情報基盤運用室では学外公開アドレス管理システムを構築した．本システムの特徴は，学外公開，すなわち学外から到達可能なIPアドレスを付与した機器に関する情報共有と，それに対する措置として脆弱性改善と通信制御を実現したことにある．本稿の構成は次のとおりである．まず，第2章で本学のネットワークの現状と，その調査で判明した問題点を整理する．次いで，アドレス管理に関する他組織の取り組みを第3章で紹介する．第4章で学外公開アドレス管理システムの設計について述べた後，第5章で12カ月に渡るシステムの運用から得られた知見について報告する．最後に6章で本稿の貢献をまとめる．

2. 九州工業大学のネットワーク

本章では，学外公開アドレス管理システムの設計と構築に先んじて，九州工業大学におけるネットワークの現状について説明する．2.1節と2.2節でネットワークの構成とIPアドレスの利用について述べた後，その調査により判明した問題点を整理する．

2.1　ネットワークの構成

図1に九州工業大学のネットワークの構成を示す[2]．本学は戸畑，飯塚，若松の3つのキャンパスに対応するコアネットワークと，それに接続する情報システムから成り，それら情報システムを計6,000人を超える学生と職員が利用している．本学が接続するSINETは，全国の高等教育機関や研究機関の学術情報基盤として，国立情報学研究所が整備した学術情報通信ネットワークである[3]．また，学内外を分ける境界FW（Firewall）システムとして，米国Fortinet社のFortiGate1000-Cを設置している[4]．本学では，我々が属す情報基盤運用室がコアネットワークの管理を，各部局がそれに接続する情報システムの管理を担当している．これは大学組織の業務が教育・研究・事務など多岐に渡るため，情報システムの運用に柔軟性を持たせる必要があることに起因する．この情報システムの独立性により，2017年までのIPアドレスの学外公開は，情報システムの管理者からの依頼を情報基盤運用室が受け，境界FWシステムにおいて当該アドレスに対する学外からの通信を許可することで実現していた．議論の簡単化のため，境界FWシステムで制御するのは学外から情報システムへの通信のみとして，それ以外の通信には影響を及ぼさないものとする．

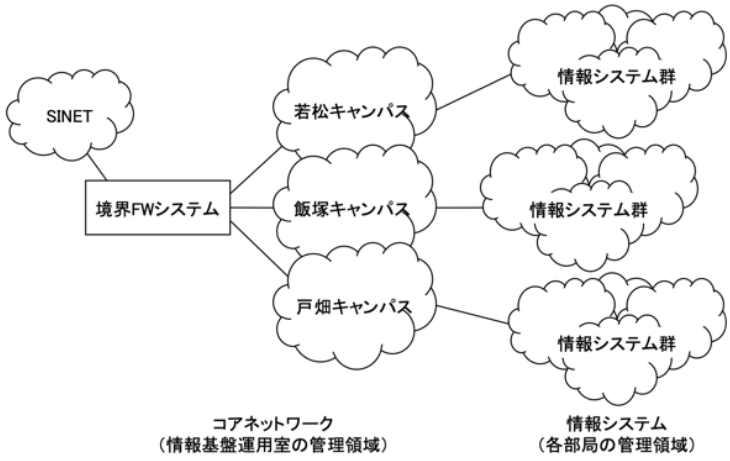

図1　九州工業大学のネットワーク構成

セキュリティインシデントの発生時は，コアネットワークを管理する情報基盤運用室と情報システムを管理する部局との連携が必須となる．しかしながら，IPアドレスを学外公開する目的や機微情報の有無などを情報基盤運用室側で把握できないことが問題となっていた．また，ポートやプロトコルなど，サービス単位の通信制御は各部局に委ねられているため，機器の堅牢性は部局の取り組みに大きく依存することになる．故に，情報基盤運用室と部局で学外公開アドレスを付与した機器に関する情報を共有する仕組み，学外公開する目的と照らし合わせ適切なサービスに対する通信のみを許可する仕組みが求められる．

2.2　IPアドレスの利用

学外公開アドレス管理システムの構築に先立って，本学におけるIPアドレスの利用状況の調査を実施した．2017年10月時点では，30の部局が管理を担う計122の情報システムが運用されていた．それら情報システムの管理者が学外公開を依頼しているIPアドレスの総数は4,883であった．一方，調査の結果，機器への割り当てが予想されるIPアドレスの数は4,883の内，565のみであった．565のアドレスは，部局の情報システム側で通信を遮断しているもの，テレビ会議システムなどの常時起動していないものを含まないため，厳密な数ではない．結果に多少の誤差が含まれるとしても，IPアドレスの利用数は依頼数の12%程度であることが明らかになった．この原因は，多くの管理者が煩わしさから必要以上のIPアドレスの学外公開を依頼していること，不要となったIPアドレスの非公開を依頼をしないことであると推察される．この不用意な学外公開が，ネットワーク全体の堅牢性を低下させる要因となっていることは明白である．

次いで，IPアドレスの割り当てが予想される565台の機器に対して脆弱性検査を実施した．その検査には，米国 Tenable Network Security社のNessusを用いた[5]．Nessusは，エージェントプログラムのインストールを必要とせず，ネットワークを介した通信のみから機器の脆弱性を検出することが可能である．その脆弱性の検出に併せて，その5段階の深刻度，および改善方法などを提示するなどの機能を有す．**表1**と**表2**に検査結果ををを示す．565台の機器が有す脆弱性の総数は，Lowが1,510，Mediumが4,328，Highが679，Criticalが370であった．また，各機器において最も高い深刻度は，20台がLow，277台がMedium，53台がHigh，40台がCriticalを有しており，脆弱性がまったくない機器は175台のみであった．その結果における代表的な脆弱性の数と詳細を**表3**に示す．これらHighとCriticalの脆弱性は，その機器のオペレーティングシステム自体，またはApache，OpenSSL，PHP，Sendmailなど，主要なアプリケーションのバージョンが古いことが原因であった．加えて，MTA Open Mail Relayなど，設定の見直しを要するもの，UPnPやSMBなど，学外からの通信を遮断すべきものの存在が明らかになった．部局の情報システムにおいて学内外の通信で異なる制御を適用している可能性があるため，一概にこれらの脆弱性が学外に露呈していると判断することはできない．この誤差を加味したとしても，HighとCriticalを合わせた約100台の機器が非常に危険な状態で運用されていることが判明した．

表1　機器が有す脆弱性の総数（2017年10月時点）

Critical	High	Medium	Low	None
370	679	4328	1510	19181

表2　脆弱性の深刻度と機器の数（2017年 10月時点）

Critical	High	Medium	Low	None	Total
40	53	277	20	175	565

表3　代表的な脆弱性の数と詳細（2017年 10月時点）

Critical	Unix Operating System Unsupported Version Detection	25
Critical	macOS < 10.13 Multiple Vulnerabilities	164
High	ESXi 6.0 U1 < Build 5251621 / 6.0 U2 < Build 5251623 / 6.0 U3 < Build 5224934 Multiple Vulnerabilities	3
Critical	Apache 2.2.x < 2.2.15 Multiple Vulnerabilities	20
Critical	PHP Unsupported Version Detection	8
Critical	PHP 7.0.x < 7.0.21 Multiple Vulnerabilities	38
Critical	PHP 5.6.x < 5.6.31 Multiple Vulnerabilities	75
Critical	OpenSSL Unsupported	7
High	OpenSSL 'ChangeCipherSpec' MiTM Vulnerability	28
Critical	Sendmail < 8.12.10 prescan() Function Remote Overflow	3
Critical	Sendmail headers.c crackaddr Function Address Field Handling Remote Overflow	1
High	MTA Open Mail Relaying Allowed	33
Critical	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows RCE	24
High	SNMP Agent Default Community Name (public)	4
High	Microsoft Windows SMB Shares Unprivileged Access	2

以上の調査結果から，不要なIPアドレスが学外公開され続けていること，学外公開中のIPアドレスが非常に脆弱な機器に付与されていることが明らかになった．故に，不適切なIPアドレスの学外公開を改善または停止することで，ネットワークの堅牢性を低下させる要因を除外する仕組みが求められる．

3. 関連研究

本章では，他組織におけるアドレス管理，その関連技術である通信制御と脆弱性検査の取り組みについて述べる．まず，高エネルギー加速器研究機構は，IPアドレスの管理台帳から不要機器の廃止と管理者情報の更新を実現するための手順を紹介している[6]．加えて脆弱性検査に関しては，その複雑性を緩和するため，自組織のセキュリティモデルを参照して必要な機能のみを提供する仕組みを構築している[7]．広島大学では，管理者からの利用申請に基づき機器に対して自動的な通信制御の適用を[8]，その機器の脆弱性検査結果の効率的な通知と共有を実現している[9]．また，名古屋大学では，初期の混乱の低減を目的とした段階的な全学FWシステムの導入を[10]，鹿児島大学では，各機器における脆弱性の改善状況の可視化を試みている[11]．その他にも，堅牢性を重視したネットワークの構築について，京都大学の取り組みが報告されている[12]．

アドレス管理と通信制御，脆弱性検査の機能を実現するために，各組織で独自のシステムを構築・運用していることが見て取れる．これは各組織の規定や背景が大きく異なるため，他組織で構築したシステムを転用することの難しさに起因している．

4. 学外公開アドレス管理システム

第2章の調査により明らかになった，本学のアドレス管理に関する問題は次のとおりである．

（a）IPアドレスとそれを付与した機器に関する情報を情報基盤運用室と各部局で共有できていないこと
（b）ポートやプロトコルなど，サービス単位の通信制御が各部局の取り組みに委ねられていること
（c）不適切なIPアドレスが学外公開され続けていること

これらの問題を解決するために，学外公開アドレス管理システムでは次の要件の実現を目指す．

（a）情報システムの管理者による申請と情報基盤運用室による承認の実施
（b）申請内容に基づくサービス単位の通信制御の適用
（c）情報システムの管理者への脆弱性検査機能の提供

図2に，学外公開アドレス管理システムの概要を示す．本システムは，（1）アドレス申請機能，（2）通信制御機能，（3）脆弱性検査機能により構成される．まず，次節から各機能の詳細について述べた後，4.4節で本システムを用いた申請処理について述べる．

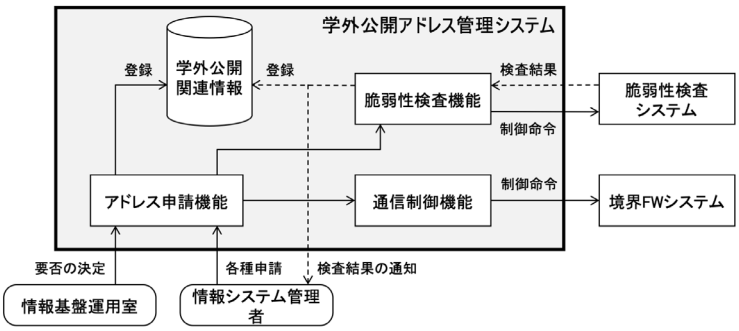

図2　学外公開アドレス管理システムの概要

4.1　アドレス申請機能

本機能の役割は，管理者からの学外公開アドレスに関する各種申請を受理すること，その申請内容と脆弱性検査結果から成る学外公開関連情報を部局と情報基盤運用室との間で共有することである．この学外公開関連情報を参照することで，情報基盤運用室において当該アドレスの学外公開の要否を審議する．加えて，その情報はセキュリティインシデント発生時の対応のために活用される．

表4に各種申請の詳細を示す．ここで，レ点は各種申請において入力の必要な項目を，横線は不要な項目を意味する．申請は，新規・変更・廃止・更新・検査の5種類に分類される．新規は申請内容を学外公開関連情報として新しく登録するため，変更は登録済みの学外公開関連情報を修正するため，廃止は不要な学外公開関連情報を削除をするための申請である．これら学外公開関連情報に対する操作は通信制御機能に通知され，それに応じた通信制御が境界FWシステムにおいて適用される．また，更新は次年度も継続した学外公開が必要となるIPアドレスの報告を目的としたものである．学外公開の期間を年度末までに区切り，年度末に更新申請がないIPアドレスは管理者への問合せ後に境界FWシステムにおいて通信を遮断する．検査は任意の機器に対する脆弱性検査のために用いられ，脆弱性検査機能を介した検査の実施と結果の通知を担う．

表4　アドレス申請機能における各種申請の詳細☆1

		新規	変更	廃止	更新	検査
管理者情報	氏名	✓	✓	✓	✓	✓
	メールアドレス	✓	✓	✓	✓	✓
	電話番号	✓	✓	—	—	—
機器情報	部局	✓	✓	—	—	—
	情報システム名	✓	✓	—	—	—
	機微情報の有無 *1	✓	✓	—	—	—
	設置場所	✓	✓	—	—	—
公開情報	IP アドレス	✓	✓	✓	✓	✓
	プロトコル・ポート	✓	✓	—	—	—
	公開目的	✓	✓	—	—	—
	備考	✓	✓	—	—	—

4.2 通信制御機能

本機能の役割は，情報基盤運用室の審議で承認された学外公開関連情報に基づいて，境界FWシステムを制御することである．具体的には，新規や廃止など，通信制御の変更を伴う申請の学外公開関連情報を制御命令に変換する．その制御命令を境界FWシステムに発行することで，サービス単位の通信制御を実現する．前述のように，境界FWシステムにはFortiGate-1000Cを採用した．ここで注目すべきは，境界FWシステムと学外公開関連情報に齟齬が生じることを避けるため，それらの対応関係の管理を本機能が担う点である．学外公開関連情報においてIPアドレスが一意の値となることに着目し，その値の2進数32桁表記を10進数に変換したものを識別番号に利用することで，境界FWシステムにおける通信制御の設定と学外公開関連情報の一対一の対応付けを行った．

4.3 脆弱性検査機能

本機能の役割は，機器に対する脆弱性検査を実施すること，その結果を管理者へ通知するとともに学外関連情報として保有することである．具体的には，管理者からの検査の申請に基づき脆弱性検査システムに対して命令を発行する．その検査結果を管理者にメールで通知するとともに，学外公開関連情報としてIPアドレスとの対応付けを行う．前述のように，脆弱性検査システムには Nessusを採用した．ここで注目すべきは，学外公開後のIPアドレスのみに限定することなく，公開前のIPアドレスを付与した機器に対しても脆弱性検査を可能とした点である．この機能は，学外公開の要否を判断するために，情報システムの管理者に対して脆弱性の改善を課すが故に不可欠である．

4.4 学外公開アドレス管理システムを用いた申請処理

本節では，学外公開アドレス管理システムを用いた申請処理について，その具体例とともに説明する．まず，情報システムの管理者は，学外公開を希望するIPアドレスを付与した機器に対する脆弱性検査を実施する．また，その検査結果を参照して脆弱性の改善を試みる．脆弱性の改善が成された後，管理者は本システムに対して当該アドレスの学外公開を申請する．

次いで，情報基盤運用室における申請の審議に移る．審議の観点は，（1）本学の業務を勘案して公開目的が適切か否か，（2）公開目的と照らし合わせ，適切なサービスに対する通信のみを公開しているか否か，（3）Medium以上の脆弱性の改善が成されているか否か，（4）機器が機微情報を保有する場合，IPアドレスを学外公開することが適当か否かである．情報基盤運用室による承認後，その申請内容に基づいて境界FWシステムを制御することで，当該アドレスの各サービスに対する学外からの通信を許可する．ここで脆弱性の改善と情報基盤運用室の審議を必要とするのは，境界FWシステムにおいて新たな通信制御を追加する場合，次年度もIPアドレスの学外公開を継続する場合とした．

5. 評価

本章では，12カ月に渡る運用を通じて学外公開アドレス管理システムの有効性を評価する．まず，5.1節で諸元について述べた後，それ以降の節で3時点の調査と分析に加え，それから得られた知見について報告する．

5.1 諸元

図3に，学外公開アドレス管理システムの移行と運用のスケジュールを示す．まず，2017年10月に各部局に対して本システムへの移行を告知した．その告知には，各部局において学外公開中のIPアドレスと，それに対応する機器の脆弱性検査結果を附した．次に，2017年12月から2018年4月までの間，それ以降に学外公開が必要となるIPアドレスの新規申請の受付を行った．しかしながら，2.2節で述べたように2017年10月の時点で約5,000のアドレスが学外公開中であり，それらすべてを本システムから再度申請させることは作業量の点から現実的ではない．その負担を軽減するため，本システムを介さずCSVファイルを用いた一括申請を許容した．これは同一情報システムに関する申請では，表4の公開情報以外の項目が同様の内容になると考えられるが故である．最後に，それら申請内容に基づいた通信制御を適用することで，本システムへの移行を完了した．その後の運用としては，2018年10月に脆弱性の再検査を実施して，情報システムの管理者にその改善を依頼をした．加えて，次年度も継続して学外公開が必要となるIPアドレスの更新申請の受付を，2019年1月から開始した．

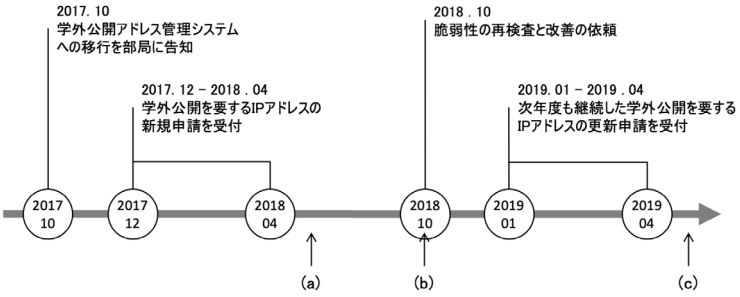

図3　学外公開アドレス管理システムの移行と運用のスケジュール

本システムの評価のため，図中における（a），（b），（c）の3時点について，学外公開中のIPアドレスとそれを付与した機器の脆弱性についての調査と分析を実施した．その3時点は，（a）本システムへの移行完了直後の2018年5月，（b）脆弱性再検査時の2018年10月，（c）年度更新の完了直後の2019年5月である．

5.2　（a）2018年5月時の分析結果

2018年5月に，学外公開アドレス管理システムへの移行が完了した．それに伴い，本学におけるIPアドレスの利用状況についての調査を実施した．2.2節で述べたとおり，これまでに学外公開中であったIPアドレスの数は4,883，実際に機器への割り当てが予想されるIPアドレスの数は565であった．一方，移行完了の時点で，情報システムの管理者らが学外公開を申請したIPアドレスの総数は397であった．ここで，その397のすべてのアドレスが機器に割り当てられていることは確認済みである．故に，情報システムの管理者に対してIPアドレスを利用する目的の見直しを促すこと，その利用のぜひを情報基盤運用室で審議することで，学外公開の必要がないIPアドレスを回収することができたと言える．

表5と**表6**に，学外公開中のIPアドレスを付与した397台の機器に対する脆弱性検査の結果を示す．397台の機器が有す脆弱性の総数は，Lowが297，Mediumが409，Highが10，Criticalが0であった．また，各機器において最も高い深刻度は，66台がLow，70台がMedium，10台がHighを有しており，脆弱性がまったくない機器は251台であった．その結果における代表的な脆弱性の数

と詳細を**表7**に示す．SSL/TLSの暗号強度によるMediumの113，CGIのSQL InjectionによるHighの8とそれに関連するMediumの16は誤検知が原因であった．また，計175のMediumは，SSLの自己証明書，Gitのリポジトリ公開，VPNの共有鍵のそれ自体に起因しており，そのサービスを停止する他に適当な手段がないことから，対処が不要の脆弱性と判断した．ここで，残りのMediumとHighの脆弱性は，それに対する学外からの通信を遮断しているため，学外に露呈しているのはLowの脆弱性のみであることを補足しておく．ゆえに，本システムにおけるアドレス申請機能を通じた情報基盤運用室による審議に加え，脆弱性検査機能と通信制御機能の効果により，ネットワークの堅牢性を低下させる要因を除外できたと言える．

表5　機器が有す脆弱性の総数（2018年5月時点）

Critical	High	Medium	Low	None
0	10	409	297	11649

表6　脆弱性の深刻度と機器の数（2018年5月時点）

Critical	High	Medium	Low	None	Total
0	10	70	66	251	397

表7　代表的な脆弱性の数と詳細（2018年5月時点）☆2☆3

High	CGI Generic SQL Injection (blind) *2	8
Medium	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST) *3	113
Medium	SSL Certificate Cannot Be Trusted	76
Medium	SSL Self-Signed Certificate	64
Medium	SSL Certificate Expiry	21
Medium	SSL Certificate with Wrong Hostname	8
Medium	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key	5
Medium	Git Repository Served by Web Server	1

脆弱性検査において，誤検出だけでなく対処が不要と考えられるものが検出された．また，脆弱性には偏りがあり，複数の機器間で同一の脆弱性が多数検出される傾向にあった．このことから，各脆弱性についての対処の要否や改善の推奨設定を共有する仕組みを構築することで，その作業負担の大幅な低減が期待できる．

5.3　（b）2018年10月時の分析結果

学外公開アドレス管理システムの運用が約半年を迎えた2018年10月に，本学におけるIPアドレスの利用状況についての再調査を実施した．情報システムの管理者らが学外に公開しているIPアドレスの数は403で，前述の結果と比較しても大きな変化は見られなかった．

表8と**表9**に，学外公開中のIPアドレスを付与した403台の機器に対する脆弱性検査の結果を示す．403台の機器が有す脆弱性の総数は，Lowが306，Mediumが531，Highが45，Criticalが7であった．また，各機器において最も高い深刻度は，52台がLow，77台がMedium，29台がHigh，4台がCriticalを有しており，脆弱性がまったくない機器は241台であった．その結果における代表的な脆弱性の数と詳細を**表10**に示す．その機器のオペレーティングシステム自体，またはApache，OpenSSL，PHPなど，主要なアプリケーションのバージョンが古いことが原因で，こ

れまでにはなかった脆弱性が検出されている．このことから，約半年という短い期間でも新たな脆弱性が発見されていることが見て取れる．また，いくつかの脆弱性は新しいものではなく，管理者による設定変更に起因するものと予想される．具体的には，UPnPのBuffer OverflowとMTA Open Mail Relayは，2.2節で述べたものと同一の脆弱性である．この問題を解決するためには，管理者に機器の現状を定期的に通知する仕組みが求められると言える．

表8　機器が有す脆弱性の総数（2018年10月時点）

Critical	High	Medium	Low	None
7	45	531	306	12256

表9　脆弱性の深刻度と機器の数（2018年10月時点）

Critical	High	Medium	Low	None	Total
4	29	77	52	241	403

表10　代表的な脆弱性の数と詳細（2018年10月時点）

Critical	Unix Operating System Unsupported Version Detection	4
High	PHP 7.0.x < 7.0.28 Stack Buffer Overflow	4
Medium	Apache 2.4.x < 2.4.35 Multiple Vulnerabilities	24
Medium	OpenSSL 1.0.x < 1.0.2m Multiple Vulnerabilities	8
Critical	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows RCE	3
High	MTA Open Mail Relaying Allowed	4

5.4　（c）2019年5月時の分析結果

2019年1月から同年4月まで，学外公開アドレス管理システムにおいて次年度の更新申請の受付を行った．その完了と併せて，本学におけるIPアドレスの利用状況についての調査を実施した．なお，情報システムの管理者には，その申請時にMedium以上の脆弱性の改善を依頼している．

表11と**表12**にIPアドレスの利用状況ついての調査結果を示す．情報システムの管理者らが学外に公開しているIPアドレスの数は416で，そのアドレスを付与した機器が有す脆弱性の総数は，Lowが289，Mediumが450，Highが9，Criticalが0であった．また，各機器において最も高い深刻度は，60台がLow，81台がMedium，9台がHighを有しており，脆弱性がまったくない機器は266台であった．このHighとMediumの多くは，5.2節で述べた誤検出と対処不要の脆弱性であり，その残りに対しても学外からの通信の遮断を実施している．この結果からは，IPアドレスの数と機器の脆弱性に関する特徴的な動向は確認できなかった．ここで注目すべきは，わずかながらではあるが，学外公開中のIPアドレスに関して廃止と変更の申請をされたことである．この申請は，管理者の離職や部局の移動によるものであった．故に，IPアドレスの学外公開を継続する必要性を定期的に確認することで，それに関する情報の更新を誘起できると言える．

表11　機器が有す脆弱性の総数（2019年5月時点）

Critical	High	Medium	Low	None
0	9	450	289	13239

表12　脆弱性の深刻度と機器の数（2019年5月時点）

Critical	High	Medium	Low	None	Total
0	9	81	60	266	416

5.5　議論

学外公開アドレス管理システムの構築により，学外公開アドレスを付与した機器に関する情報共有と，それに対する措置として脆弱性改善と通信制御を実現した．これにより，部局におけるIPアドレスの利用を情報基盤運用室で審議すること，すなわち複数組織間で妥当性を確認することでネットワークの堅牢性を向上することができた．その状態を維持すべく，定期的な脆弱性の改善と学外公開関連情報の更新に向けた試みと効果を5.3節と5.4節で報告した．

大学組織では，教育・研究・事務など多岐に渡る業務に柔軟に対応するため，各部局が情報システムの管理を担うことが一般的である[6],[9],[10],[11]．その情報システムの独立性により，組織間におけるコミュニケーションの円滑化はきわめて重要となる．その一方で，本システムの12カ月に渡る運用と評価により，事前調査と要件定義の時点では考慮できていなかったいくつかの課題が明らかになった．他組織で同様の取り組みを推進するにあたり，あらかじめ検討すべき（a）ネットワークの堅牢性維持に向けた脆弱性検査と，（b）IPアドレスの学外公開継続に関する事項を以下に示す．

（a）ネットワークの堅牢性維持に向けた脆弱性検査

- ネットワークの堅牢性を維持するためには，定期的な脆弱性検査と改善が必須である．しかしながら，各管理者は兼務として情報システムの管理を担当しており，本務に与える影響を考慮すると現状の仕組みによる脆弱性検査の実施は年に2回程度が限界であると考えられる．そこで管理者の作業負担を低減するためには，各脆弱性についての対処の要否や改善の推奨設定など，情報基盤運用室から部局への情報提供を促進する機能が必要である．
- 脆弱性の対応の一環として，Amazon Web ServiceやGoogle Cloud Platform，Microsoft Azureに代表されるクラウド事業者のサービスに情報システムの一部を移転することが考えられる．クラウドサービスなど組織外のネットワークで発生するセキュリティインシデントに備え，その詳細を部局と情報基盤運用室とで共有する機能が必要である．
- テレビ会議システムなどの常時起動していない機器は，脆弱性検査の実施に大きな制限が生じる．また，IoT（Internet of Things）デバイスや組み込みシステムなどの機器は，脆弱性検査において十分な精度を期待できない．それらに対しては，ファームウェアのバージョンを報告させるなど，脆弱性検査とは異なる手段で堅牢性を確認する仕組みが必要となる．

（b）IPアドレスの学外公開継続

- IPアドレスの学外公開を継続するために，情報システムの管理者に対してMedium以上の脆弱性の改善を課した．一方，組織の根幹を成す大規模な情報システムにおいて，金銭的な理由から改修が難しいといった事案が起こり得る．その場合，組織の運営や業務に甚大な影響を及ぼすことになる．故に，脆弱性の改善計画や緩和措置を認め，それらの実施を継続的に監査することにより，IPアドレスの学外公開を暫定的に許容する仕組みが必要となる．
- 研究室では，教育的な観点から情報システムの管理を学生が担当することが散見された．このような場合，担当者の入れ替わりに伴い，十分な引き継ぎがなされないことが問題となり

得る．故に，その実情を報告させることで，学生による管理を補助する体制の整備が必要である．

6. おわりに

本稿では，「情報機器の管理状況の把握及び必要な措置の実施」を達成するため，2018年5月から本格的に運用を開始した学外公開アドレス管理システムの設計と効果について述べた．本システムの特徴は，学外公開中のIPアドレスを付与した機器に関する情報共有と，それに対する措置として脆弱性改善と通信制御を実現したことにある．その導入により，IPアドレスの学外公開が適切に管理され，本学のネットワークが高い堅牢性を確保できたと言える．その一方で，本システムの12カ月に渡る運用と評価によりいくつかの課題が明らかになった．まず，ネットワークの堅牢性維持に向けた脆弱性検査の課題として，作業負担の低減のため管理者への情報提供を促進する機能が必要である．また，クラウドサービスなどの組織外システム，テレビ会議システムやIoTデバイスなどの適切な管理を検討すべきである．IPアドレスの学外公開継続の課題としては，公開と非公開を一律に判断せず，改善計画や緩和措置に基づいてIPアドレスの学外公開を暫定的に許容する仕組みに加え，学生など十分な技術力が伴わない管理者を補助する体制の整備が求められる．今後の脆弱性の推移については，さまざまな場を通じて定期的に報告する予定である．最後に，各情報システムの管理者の協力の下，本稿で記述した脆弱性はすでに改善されていることを特筆しておく．

謝辞　本研究は電気通信普及財団の助成を受けたものである．また，各情報システムの管理者には，本システムの運用にあたり多大な協力を頂いた．ここに深く謝意を示す．

参考文献

1）独立行政法人情報処理推進機構：情報セキュリティ白書
2018，https://www.ipa.go.jp/files/000070313.pdf
2）中村　豊 他：九州工業大学における全学セキュア・ネットワークの導入について，情報処理学会研究報告，Vol.IOT-28, No.20, pp.1–6 (2015)．
3）国立情報学研究所：学術情報ネットワーク SINET5 — Science Information NETwork 5,
https://www.sinet.ad.jp
4）Fortinet : FortiGate — Next-Generation Firewalls (NGFW),
https://www.fortinet.com/products/next-generation-firewall.html
5）Tenable Network Security: Nessus Professional,
https://tenable.com/products/nessus
6）鈴木　聡他：粗い分割のキャンパスネットワークにおけるIPアドレス棚卸作業，情報処理学会研究報告，Vol.IOT-40, No.11, pp.1–5 (2018)．
7）村上直 他：DMZネットワークのサーバ管理者自身による脆弱性診断，インターネットと運用技術シンポジウム論文集，pp.41–48 (2016)．
8）近堂　徹 他：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，学術情報処理研究，Vol. 21, No. 1, pp.36–43 (2017)．
9）田島浩一 他：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，Vol. 18, No. 1, pp.16–23 （2014）．
10）嶋田創 他：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，Vol. IOT-35, No.6, pp.1–8 (2016)．
11）相羽俊生 他：学内サーバの脆弱性診断と診断結果の解析方法，学術情報処理研究，Vol. 20, No. 1, pp.105–111 (2016)．
12）高倉弘喜 他：安全なギガビットネットワークシステム KUINS.IIIの構成とセキュリティ対策，電子情報通信学会論文誌，Vol.J86-B, No.8, pp.1494–1501 (2003)．
13）総務省：行政機関・独立行政法人等における個人情報の保護，

https://www.soumu.go.jp/main_sosiki/gyoukan/kanri/kenkyu.htm

脚注

☆1　九州工業大学情報格付け基準に則するものであり，たとえば，独立行政法人等の保有する個人情報の保護に関する法律で定められた個人情報などが含まれる[13]
☆2　検査結果にも “Note that this script is experimental and may be prone to false positives.”の記載あり
☆3　改善のためにはTLSv1.0を無効にする必要があるが，この時点ではTLSv1.0による暗号化がいまだ一般的に利用されていたため

佐藤彰洋（正会員）satoh@isc.kyutech.ac.jp
九州工業大学情報科学センター助教．情報基盤運用室兼任．2011年東北大学大学院情報科学研究科博士後期課程修了．博士（情報科学）．ネットワーク運用技術，ネットワークセキュリティに関する研究に従事．電子情報通信学会会員．

福田豊（正会員） fukuda@isc.kyutech.ac.jp
九州工業大学情報科学センター助教．情報基盤運用室兼任．2005年九州工業大学情報工学研究科博士後期課程修了．博士（情報工学）．情報ネットワーク，無線LANに関する研究に従事． IEEE，電子情報通信学会会員．

和田数字郎（非会員）swada@isc.kyutech.ac.jp
九州工業大学飯塚キャンパス技術部技術専門職員．情報基盤運用室兼任．2003年九州芸術工科大学大学院芸術工学研究科博士前期課程修了．修士（芸術工学）．ネットワークの運用に関する業務に従事．

中村豊（正会員） yutaka-n@isc.kyutech.ac.jp
九州工業大学情報科学センター教授．情報基盤運用室長兼任．2001年奈良先端科学技術大学情報科学研究科博士後期課程修了．博士（工学）．インターネット計測技術，ネットワーク運用技術，ネットワークセキュリティに関する研究に従事．電子情報通信学会会員．

投稿受付：2019年11月1日
採録決定：2020年3月4日
編集担当：東野輝夫（大阪大学）