パケットの特徴に基づく脆弱性検査の自動解析に関する研究調査

代表研究者	佐 藤 彰 洋	九州工業大学情報基盤センター　助教
共同研究者	中 村 豊	九州工業大学情報基盤センター　教授
共同研究者	福 田 豊	九州工業大学情報基盤センター　准教授

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].例えば,脆弱なパスワードの設定による不正アクセスやウェブサイトの改竄，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センター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，それに対する措置である脆弱性検査と通信制御を関連付けたことにある．これにより，本学ネットワークにおける堅牢性の向上のみならず，現実に即した脆弱性検査とその結果の解析が可能となる．

本稿の構成は次の通りである．先ず，2 章で本学のキャンパス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 3 章で紹介する．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,5 章で 12 ヶ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 章で本稿の貢献を纏める．

2 九州工業大学のキャンパスネットワーク

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 6000 人を超える学生と職員が利用している．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 FortiGate 1000-C を設置している[3]．留意すべき特徴は，我々が属す情報基盤センターがコアネットワー

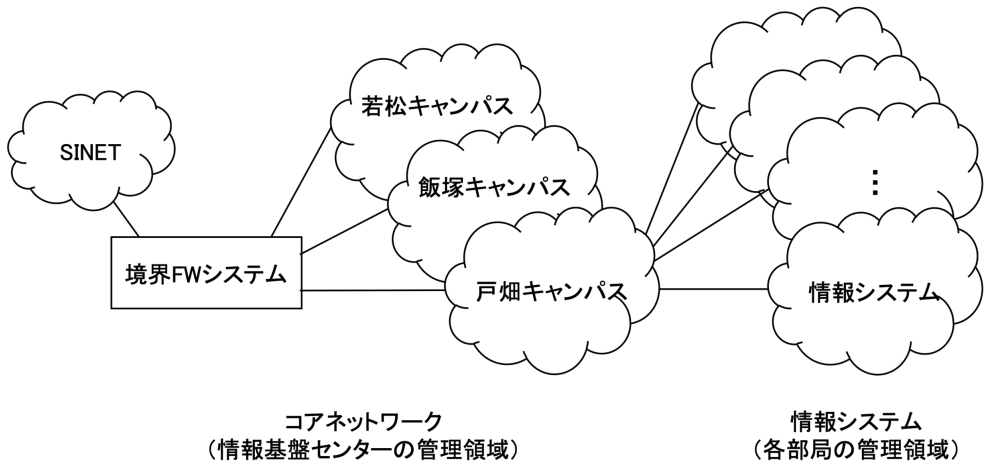

図 1：九州工業大学のネットワーク構成

公益財団法人電気通信普及財団
研究調査助成報告書　第37号　2022年度

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う点である．この情報システムの独立性により，これまでの 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センターが受け，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.ネットワークの構成から明らかな様に，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であり，学内からの通信には影響を及ぼすことはない.

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センター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センター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，情報基盤センター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.その調査の時点では，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 4883 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 4883 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[4]．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潜在的な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 に検査結果を示す．565 台の機器が有す脆弱性の総数は，Low が 1510，Medium が 4328，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，脆弱性が全く無い機器は 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(Mail Transfer Agent) Open Mail Relay など，設定の見直しを要するもの，UPnP(Universal Plug and Play)や SMB(Server Message Block)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.

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.

表 1：機器が有す脆弱性の総数（事前調査時）

Critical	High	Medium	Low	None
370	679	4328	1510	19181

表 2：脆弱性の深刻度と機器の数（事前調査時）

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（事前調査時）

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

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．先ず，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[5]．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[6].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[7],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[8]．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[9]，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[10]．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[11]．

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

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通りである．

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センター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センターによる承認の実施
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．先ず，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．

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センターとの間で共有することである．この学外公

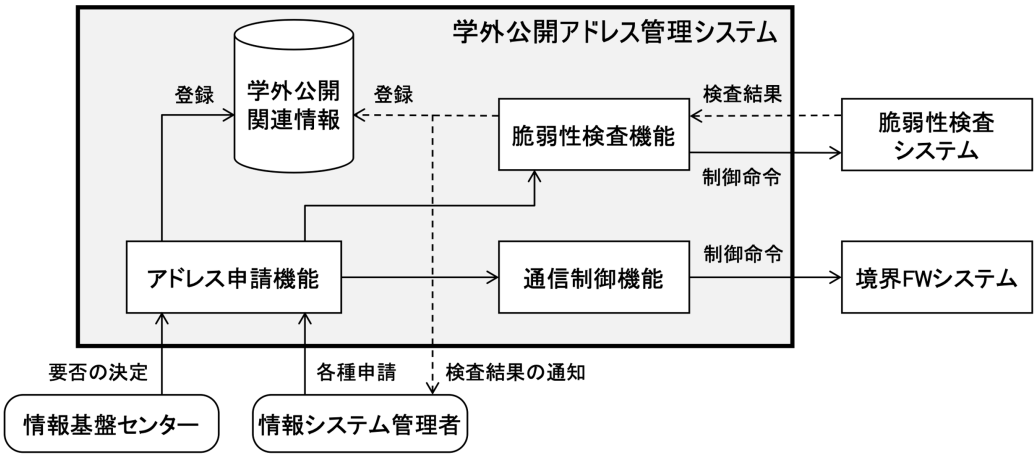

図 2：学外公開アドレス管理システムの概要

開関連情報を参照することで，情報基盤センター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い合わせ後に境界 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

		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	✓	✓	—	—	—
	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，情報基盤センター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．ここで留意すべきは，境界 FW システムの設定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．

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共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共に，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．ここで留意すべきは，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．

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，その具体例と共に説明する．先ず，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，情報基盤センター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．情報基盤センターによる承認後，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センター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 ヶ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．先ず，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．先ず，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，その年度末に，それ以降も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なった．ここで留意すべきは，約 5000 のアドレスが学外公開中であることを勘案して，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点である．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，半年後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，年度末から開始した．

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，(b)脆弱性再検査時，(c)年度更新の完了直後である．

5-2 システムへの移行完了直後の分析結果

学外公開アドレス管理システムへの移行に伴い，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 節で述べた通り，これまでに学外公開中であった IP アドレスの数は 4883，実際に機器への割り

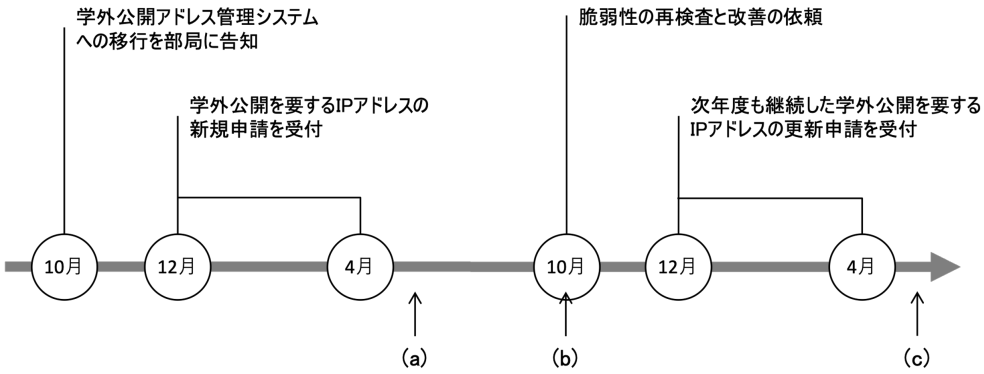

図 3：学外公開アドレス管理システムの移行と運用のスケジュール

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 の全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，その利用の是非を情報基盤センターで審議することで，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，脆弱性が全く無い機器は 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無いことから,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留意されたい．故に，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センターによる審議に加え，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．

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．

表 5：機器が有す脆弱性の総数（システム移行完了直後）

Critical	High	Medium	Low	None
0	10	409	297	11649

表 6：脆弱性の深刻度と機器の数（システム移行完了直後）

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（システム移行完了直後）

High	CGI Generic SQL Injection (blind)	8
Medium	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)	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

5-3 脆弱性再検査時の分析結果

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時点で,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，脆弱性が全く無い機器は 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，これまでには無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，幾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（脆弱性再検査時）

Critical	High	Medium	Low	None
7	45	531	306	12256

表 9：脆弱性の深刻度と機器の数（脆弱性再検査時）

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（脆弱性再検査時）

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 年度更新の完了直後の分析結果

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.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ことを留意されたい.

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,脆弱性が全く無い機器は 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,僅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（年度更新完了直後）

Critical	High	Medium	Low	None
0	9	450	289	13239

表 12：脆弱性の深刻度と機器の数（年度更新完了直後）

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

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，学外公開アドレス管理システムの設計と 12 ヶ月に渡る運用の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，それに対する措置である脆弱性検査と通信制御を関連付けたことにある．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ことに加え，現実に即した脆弱性検査とその結果の解析が可能となったと言える．脆弱性の改善状況については，今後も様々な場を通じて定期的な報告を予定している．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既に改善されていることを特筆しておく．

【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] Fortinet: FortiGate — Next-Generation Firewalls (NGFW), https://www.fortinet.com/products/next-generation-firewall.html.
[4] Tenable Network Security: Nessus Professional, https://tenable.com/products/nessus.
[5] 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).
[6] 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).
[7] 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).
[8] 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).
[9] 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).
[10] 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).
[11] 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).
[12] 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, http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/kenkyu.htm.

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
学外公開アドレス管理システムの設計と評価	情報処理学会デジタルプラクティス	July 2020
A Word-Level Analytical Approach for Identifying Malicious Domain Names Caused by Dictionary-Based DGA Malware	MDPI Electronics	April 2021
DGA マルウェアにより自動生成された悪性ドメインの判別	情報処理学会論文誌	May 2021
An Approach for Identifying Malicious Domain Names Generated by Dictionary-Based DGA Bots	IEICE Transactions on Information and Systems	May 2021