JACN 学術情報処理研究
Journal for Academic Computing and Networking
No. 27
2023年 pp. 167-173
DOI: 10.24669/jacn.27.1_167

論　文

学外公開アドレス管理システム

佐藤 彰洋，戸田 哲也，和田 数字郎，福田 豊，中村 豊
九州工業大学

A Management System for Institute-Public IP Addresses

Akihiro Satoh, Tetsuya Toda, Sujiro Wada, Yutaka Fukuda, Yutaka Nakamura
Kyushu Institute of Technology

概　要：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．その対策として，我々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．また，長期的な運用を見据え，本システムの運用に介在する人的な作業を可能な限り自動化した．具体的には，学外公開に関する申請の処理と期限の周知である．その結果，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ることを確認した．

キーワード：アドレス管理，通信制御，脆弱性検査，運用自動化

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，不正アクセスによる個人情報の漏洩やウェブサイトの改竄などの事案である．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に向けた体制と対策の整備は，法人全体が一丸となって取り組むべき責務となる．

九州工業大学では，「サイバーセキュリティ対策等基本計画」を策定し，情報セキュリティの向上に努めている．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，我々が属すネットワークセキュリティ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 [2]．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．また，長期的な運用を見据え，本システムの運用に介在する人的な作業を可能な限り自動化した．具体的には，学外公開に関する申請の処理と期限の周知である．その結果，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ることを確認した．なお，本稿は文献 [2] を基として，長期に渡る運用とその負担軽減を中心に加筆したものである．

本稿の構成は次の通りである．先ず，2 章で本学のネットワークの問題点を整理する．3 章で学外公開アドレス管理システムの設計を述べた後，4 章で有効性を評価する．次いで，運用負荷の軽減に向けた本システムの改良とその評価結果を 5 章と 6 章で報告する．最後に，7 章で本稿の貢献を纏める．

2　九州工業大学のネットワーク

本章では，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，それら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

九州工業大学におけるネットワークの構成を図 1 に示す [3]．本学が接続する SINET は，全国の教育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情報通信ネットワークである．また 2017 年の時点では，学内外を分ける境界 FW システムとして米国 Fortinet 社の FortiGate 1000C[1] を設置していた．本学では，我々が属すネットワークセキュリティ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，部局の意向を反映した情報システムの運用が不可欠となることに起因する．ここで特筆すべきは，ネットワークセキュリティ基盤運用室と各部局との一元的な対話のため，部局が情報システムごとに若干名の管理者（以降，情報システムの管理者と表記）を選任する点である．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ネットワークセキュリティ基盤運用室が受け，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学内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．

セキュリティインシデントの発生時は，ネットワークセキュリティ基盤運用室と情報システムの管理者との迅速な連携が必須となる．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ネットワークセキュリティ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情報システム側に委ねられているため，機器の堅牢性は情報システムの管理者の取り組みに大きく依存することになる．故に，ネットワークセキュリティ基盤運用室と情報システムの管理者と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．

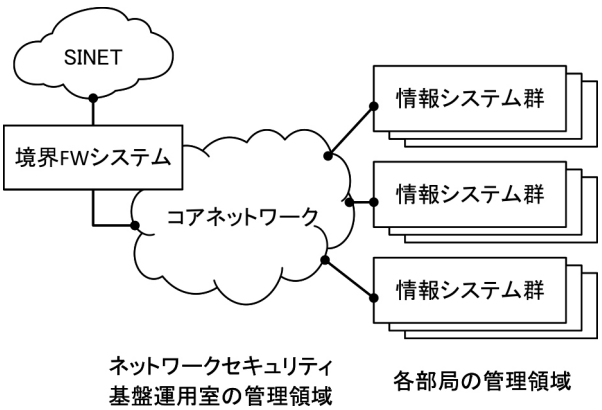

図 1　九州工業大学のネットワーク構成

2.2　IP アドレスの利用

本学における IP アドレスの利用状況について調査を実施した．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 4883 であった．一方，Nmap による調査の結果 [4]，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 IP 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% 程度に留まることが明らかになった．この原因は，情報システムの管理者が依頼の手間を惜しみ将来的な利用見込み分を含めるなど，必要数以上の IP アドレスを学外公開しているためと考えられる．この不用意な学外公開が，情報システムの管理者が意図しない通信の発生に繋がる危険性がある．具体的には, それら未使用の学外公開アドレスを，第三者により暫定的に使用されるなどの事例である．その結果，ネットワークにおける堅牢性の低下を招くことになる．

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[2] を用いた．Nessus は，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機能に加え，その脆弱性の深刻度および改善法を提示する機能を有する．表 1 に検査結果を示す．565 台の内，53 台で High，40 台で Critical の脆弱性が検出された．部局の情報システム側で通信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 93 台の機器が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 アドレスが脆弱

表 1　脆弱性検査結果（2017 年 10 月時点）

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

表 2　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 [3]	✓	✓	—	—	—
	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	✓	✓	—	—	—
備考情報	備考	✓	✓	—	—	—

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　学外公開アドレス管理システムの設計

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，(a) IP アドレスとそれを付与した機器に関する情報をネットワークセキュリティ基盤運用室と情報システムの管理者と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情報システムの管理者の取り組みに依存すること，(c) 不適切な IP アドレスが学外公開され続けていることである．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，(a) 情報システムの管理者による申請とネットワークセキュリティ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の実現を目指す．

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．なお，前述のように境界 FW システムには FortiGate 1000C[1] を，脆弱性検査システムには Nessus[2] を採用している．以降，各機能の詳細について述べる．

3.1　アドレス申請機能

本機能の役割は，情報システムの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ネットワークセキュリティ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，

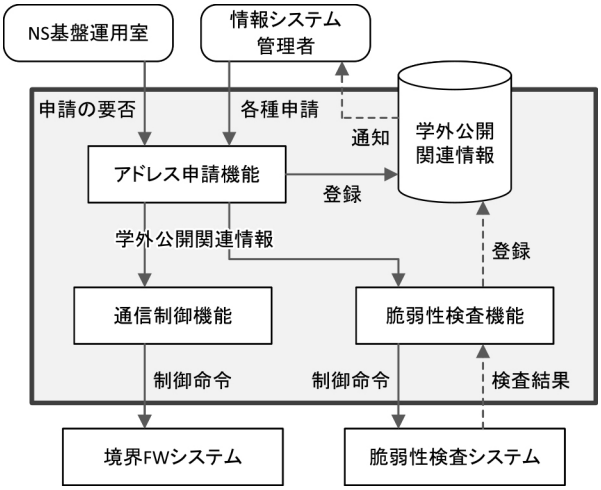

図 2　学外公開アドレス管理システム

ネットワークセキュリティ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．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[3] 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．なお，直近 2 週間以内の検査結果が存在しない場合，ネットワークセキュリティ基盤運用室により改めて脆弱性検査を実施するものとする．

表 2 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．学外公開の有効期限を年度末までに区切り，年度末に更新申請がない IP アドレスは情報システムの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．

3.2　通信制御機能

本機能の役割は，ネットワークセキュリティ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．

3.3　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，情報システムの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．なお脆弱性検査は，学外公開後の IP アドレスのみに限定することなく，学外公開前の IP アドレスを付与した機器に対しても許可している．これは，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である．

4　有効性の評価

本章では，学外公開アドレス管理システムの有効性を評価する．4.1 節で諸元について述べた後，4.2 節と 4.3 節で本システムの運用による効果と課題について議論する．

4.1　諸元

2017 年 10 月に各部局に対して学外公開アドレス管理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を受け付けた．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，毎年度末の 1 月 1 日から 3 月 31 日までの間に，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を受け付けた．ここで未更新の IP アドレスは，情報システムの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ことになる．

本システムの評価のため，移行完了直後の 2018 年 5 月において，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関する調査を実施した．また，その後 4 年に渡る運用経験に基づいて，本システムの運用上の課題を明確化する．

4.2　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当てが予想される IP アドレスの数は 565 であった．この公開数と利用数の乖離は，情報システムの管理者が依頼の手間を惜しみ，必要数以上の IP アドレスを学外公開していたことが原因と考えられる．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．その 397 の全ての IP 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，その利用の是非をネットワークセキュリティ基盤運用室で審議することで，学外公開の必要がない IP アドレスの回収に成功したと言える．

表 3 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 台の内，66 台で Low，70 台で Medium，10 台で High の脆弱性が検出された．High の 80% を占める SQL Injection の脆弱性は，その検査結果が誤りであることを確認している [4]．また，Medium の 74% は，SSL/TLS の暗号強度，SSL の自己証明書，Git のリポジトリ公開，VPN の共有鍵に起因しており，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．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．故に，本システムにおけるアドレス申請機能を通じたネットワークセ

表 3　脆弱性検査結果（2018 年 5 月時点）

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

表 4　各年度における申請数の内訳

	新規	変更	廃止	更新	合計	検査
2018 年度	48	33	10	378	469	176
2019 年度	29	40	8	361	438	258
2020 年度	58	32	24	374	488	296
2021 年度	29	42	57	348	476	388

表 5　各年度における未更新の IP アドレス数

2018 年度	2019 年度	2020 年度	2021 年度
54	95	84	89

キュリティ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の除外に成功したと言える．

4.3　課題

学外公開アドレス管理システムの導入により，本学のネットワークにおいて堅牢性の向上を達成した．運用当初は，情報システムの管理者から本システムの使用方法や脆弱性の改善方法についての頻繁な相談が寄せられていた．しかしながら，それらの数は運用が長期に渡り情報システムの管理者の習熟度が向上するにつれ，年間で 5 件を下回るほどになっている．一方で，本システムにおける運用負担の大部分を次の作業が占めることが明らかになった．先ず，短期間に集中する多量の申請の処理である．表 4 に各年度における申請数の内訳を示す．2018 年度から 2021 年度までの検査を除いた申請数はそれぞれ 469，438，488，476 と減少の兆候が見られないことに加え，これらの 90% 以上が年度末の 3 ヶ月間に集中していることを確認した．なお検査に関しては既に申請処理の自動化が成されているため，ここでは参考値としての掲示である点に留意されたい．

次に，次年度の継続した学外公開が必要となるか否かの確認である．表 5 に各年度における未更新の IP アドレス数を示す．2018 年度は未更新の IP アドレスが 54 に留まっているものの，2019 年度から 2021 年度の間は 80 以上の IP アドレスが未更新であった．未更新の IP アドレスは，境界 FW システムにおける通信の遮断に先んじて情報システムの管理者の意思確認が必須となる．これは通信の遮断が組織の運営や業務に甚大な影響を及ぼす可能性があることに起因する．故に，これら学外公開アドレス管理システムの運用を自動化する仕組みが求められる．

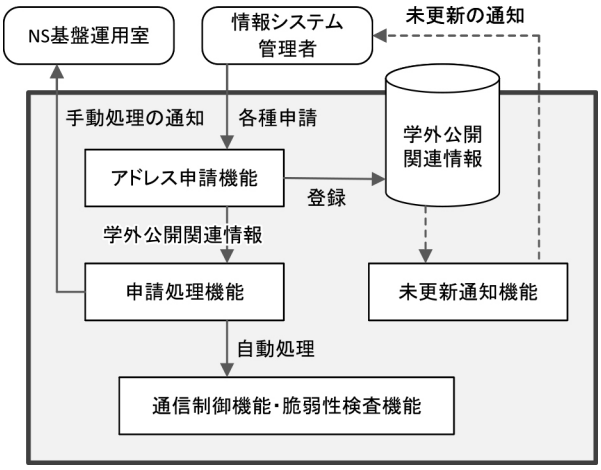

図 3　学外公開アドレス管理システムにおける自動化

5　学外公開アドレス管理システムの改良

4.3 節で述べたように，学外公開アドレス管理システムにおける運用負担の大部分を占めるのは，(a) 短期間に集中する多量の申請の処理，(b) 次年度の継続した学外公開が必要となるか否かの確認である．これら作業のために多くの人的資源を投じる必要があった．その運用負担の軽減に向けて，可能な限りこれら作業の自動化を試みる．

図 3 に，新しい学外公開アドレス管理システムの概要を示す．本システムに，(1) 申請処理機能，(2) 未更新通知機能を追加することで自動化を試みる．以降，各機能の詳細について述べる．

5.1　申請処理機能

本機能の役割は，申請の種類と内容に基づいて，その申請処理を自動化することである．具体的な方針は次の通りである．新規は，ネットワークセキュリティ基盤運用室における審議が必要であるため，公開情報の変更は，境界 FW システムにおいて新たな通信制御が適用されるため，管理者情報の変更は，情報システムの管理者であるか否かの確認が必要であるため，自動化の対象から除外する．更新は，その機器が Medium 以上の脆弱性を有している場合でも，その申請の棄却を自動化しないものとする．これは，検査結果に誤検出や対処不要の脆弱性が含まれるが故である．これら条件に該当しない申請は，ネットワークセキュリティ基盤運用室に許諾を求めることなく，本システムにおける次の機能に処理が渡される．

5.2　未更新通知機能

本機能の役割は，情報システムの管理者に対して，学外公開の有効期限に関する周知を徹底することである．

具体的には，有効期限の 3 ヶ月前からその 1 ヶ月後まで，更新が必要な IP アドレス一覧と，有効期限 1 ヶ月の超過で IP アドレスを非公開とする旨を定期的に通知する．それら通知の頻度は 1 週間に 1 回とした．

6　運用性の評価

本章では，学外公開アドレス管理システムの運用性を評価する．6.1 節で諸元について述べた後，6.2 節で本システムの自動化による効果について議論する．

6.1　諸元

運用負担の特に大きい年度末を見据え，2022 年 11 月に新しい学外公開アドレス管理システムへの移行を完了した．移行完了直後の 2022 年 11 月から翌年 5 月までの申請に関する調査を通じて，運用負担の軽減に対する申請処理機能と未更新通知機能の効果を明らかにする．4.3 節と同様に，脆弱性検査に関しては本システムの改良前に申請処理の自動化が成されているため，ここでは参考値としての掲示である点に留意されたい．

6.2　結果

表 6 に 2022 年 11 月から翌年 5 月までの申請数の内訳を示す．4.3 節で述べた通り，2018 年度から 2021 年度までの申請数はそれぞれ 469，438，488，476 であった．一方，2022 年 11 月から翌年 5 月までの申請数は 488 件であり，その内 346 件の処理を自動化することができた．特に更新に着目すると，その申請処理の自動化は 359 件の内 281 件という結果であった．この結果は，申請処理機能における条件次第で更なる改善が期待できる．具体的には，Medium 以上の脆弱性が学外に露呈しているか否か，その脆弱性が誤検出や対処不要のものか否かなどである．以上の結果から，短期間に集中する多量の申請の処理を全体の 30% 未満まで低減できることを示した．

表 7 に未更新の IP アドレス数を示す．4.3 節で述べた通り，2019 年度から 2021 年度の間は 80 以上の IP アドレスが未更新であった．2023 年は 4 月 1 日の時点で 55 の IP アドレスが未更新であったものの，5 月 1 日の時点では 4 の IP アドレスまで未更新が減少していた．この 4 件中の 3 件の IP アドレスに関しては，情報システムの管理者から事前に期限延長の申し入れがあったことを補足しておく．残りの 1 件について学外公開を継続する必要性を確認したところ，その管理者は既に本学を退職済みとのことであった．以上の結果から，次年度の継続した学外公開が必要となるか否かの確認を 1 件のみに低減できることを示した．

表 6　2022 年度における申請数の内訳

	新規	変更	廃止	更新	合計	検査
申請数	35	56	38	359	488	370
自動化	0	27	38	281	346	370

表 7　2022 年度における未更新の IP アドレス数

2023 年 4 月	2023 年 5 月
55	4

これまで学外公開アドレス管理システムのために，多くの人的資源を投じる必要があった．申請処理機能と未更新通知機能の追加により，それら作業の大部分を自動化すること，延いては運用負担を軽減することに成功したと言える．

7　むすび

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．また，長期的な運用を見据え，本システムの運用に介在する人的な作業を可能な限り自動化した．具体的には，学外公開に関する申請の処理と期限の周知である．その結果，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ることを確認した．今後，本学のネットワークを支える基盤システムとなることを期待している．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．

謝　辞

本研究は JSPS 科研費 JP21K11848 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．

注

1）2017 年度の時点で境界 FW システムは米国 Fortinet 社の FortiGate 1000C であったが，2019 年度の更新で米国 Fortinet 社の FortiGate 600E と米国 PaloAlto Networks 社の PA-5220 に置き換わっている

2）2017 年度の時点で脆弱性検査システムは米国 Tenable Network Security 社の Nessus であったが，2019 年度の更新

で同社の Tenable.io，その後のバージョンアップにより Tenable Vulnerability Management に置き換わっている

3） 九州工業大学情報格付け基準に則するものであり，例えば，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 [5]

4） 検査結果に “Note that this script is experimental and may be prone to false positives.” の記載がある

参考文献

[1] Trend Micro：被害事例とリサーチから見る教育機関を狙うサイバー攻撃の動向，https://www.trendmicro.com/ja_jp/jp-security/23/e/securitytrend20230502-01.html（2023 年 7 月 10 日参照）.

[2] 佐藤 彰洋他：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，Vol. 11, No. 3, pp. 624–635 (2020).

[3] 中村 豊他：九州工業大学における全学セキュア・ネットワークの更新，情報処理学会研究報告，Vol. 2020-IOT-48, No. 28, pp. 1–6 (2020).

[4] Nmap: the Network Mapper - Free Security Scanner, https://nmap.org（2023 年 9 月 22 日参照）.

[5] 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（2023 年 7 月 10 日参照）.