◇◇◇◇◇◇
特 集 2
◇◇◇◇◇◇

九州工業大学 学外公開 IP 申請システム

佐藤 彰洋[1]
中村 豊[2]
福田 豊[3]
和田 数字郎[4]

1 はじめに

昨今，国立大学法人等において，サイバー攻撃による情報セキュリティインシデントが多発しています．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，インターネットに接続する複合機の設定不備による情報漏洩事案などです．このような情報セキュリティインシデントが発生した場合，本学の信用失墜を招くだけでなく，多くの関係者に多大な影響を及ぼすことになります．

この問題に対するため，平成 28 年度に本学で策定した「情報セキュリティ対策基本計画」により，グローバル IP アドレスの学外公開・非公開を適切に把握・管理することが求められています．このグローバル IP アドレスの把握・管理は情報基盤運用室が担うことになっていますが，日々，高度化・巧妙化するサイバー攻撃の脅威を踏まえると，より厳格な管理体制を敷く必要があります．具体的には，(1) 現行の報告制から情報基盤運用室による承認制への変更，(2) IP アドレス単位に加え，サービス単位（プロトコルやポート）の通信制御，(3) 学外公開の期間を有効期限制へ変更，(4) 機器の脆弱性への迅速な対処です．しかしながら，この管理体制を実現するためには，現在の「学外公開 IP アドレス申請システム」では機能的に不十分であり，新システムへの移行が必須となります．本稿では，旧システムの主要な変更点を中心に，2017 年 12 月から稼働開始した新学外公開 IP 申請システムの概要を述べます．

2 旧学外公開 IP 申請システム

本節では，旧システムの概要と事前調査の結果について述べた後，旧学外公開 IP 申請システムの不足機能について整理します．

2.1 システムの概要

本学のネットワークの概要を図 1 に示します．旧学外公開 IP 申請システムは，各情報システムの管理者からの申請に基づいて境界 FW の設定を変更することにより，学外から学内への通信を制御します．境界 FW の位置から明らかなように，本システムの対象は学外からの通信のみであり，学内からの通信には影響を及ぼしません．

[1]情報科学センター　助教　satoh@isc.kyutech.ac.jp
[2]情報科学センター　准教授　yutaka-n@isc.kyutech.ac.jp
[3]情報科学センター　助教　fukuda@isc.kyutech.ac.jp
[4]情報科学センター　技術職員　swada@isc.kyutech.ac.jp

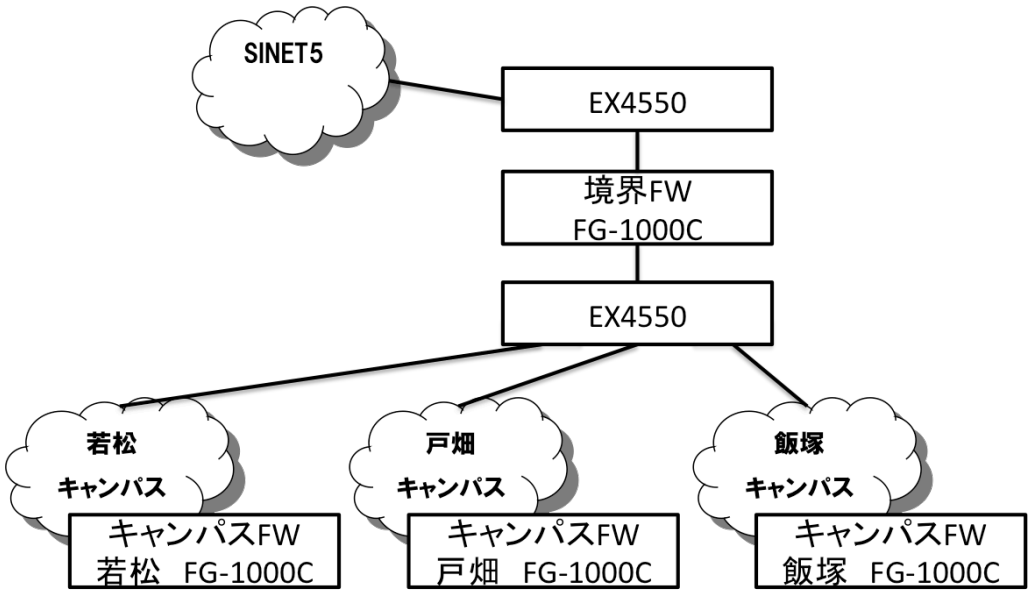

図 1: 本学のネットワークの概要

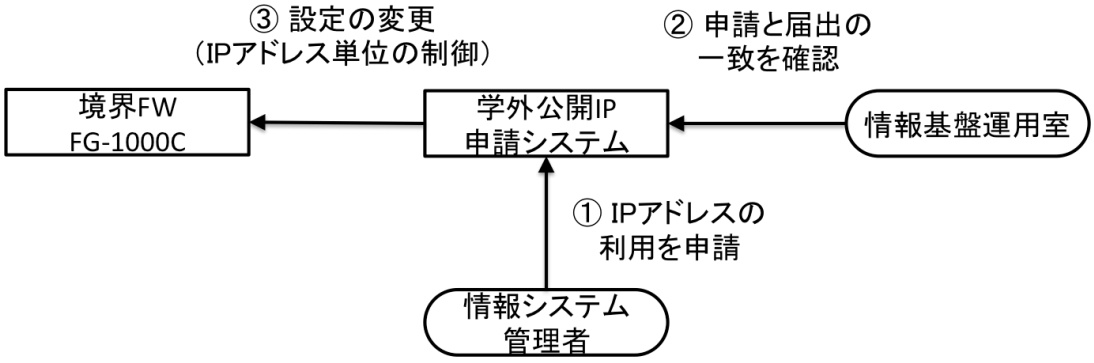

図 2: 旧学外公開 IP 申請システム

旧学外公開 IP 申請システムの処理を図 2 に示します．まず，情報システムの管理者がグローバル IP アドレスの学外公開を申請します．次いで，情報基盤運用室で申請内容と情報システムセキュリティ責任者・管理者届との一致を確認します．申請内容と届出の一致が確認された場合，境界 FW の設定を変更することで当該アドレスに対する学外からの通信を許可します．

旧学外公開 IP 申請システムでは，グローバル IP アドレスを学外公開とする目的や機器が保有する情報を情報基盤運用室側で把握できません．また，サービス単位の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ります．故に，申請内容と照らし合わせ，適切なサービスのみを学外公開する仕組みが求められると言えます．

2.2 グローバル IP アドレスの調査

学外公開 IP 申請システムの改修に先立って，本学におけるグローバル IP アドレスの利用状況について事前調査を行いました．2017 年の時点で，本学では 30 の部局が 122 の情報システムを運用しています．それら情報システムの管理者が学外公開を申請しているグローバル IP アドレスの数は 4883 でした．一方，調査の結果では機器の利用が予想されるグローバル IP アドレスの数は 4883 のなかの 565 の

みでした．この 565 のグローバル IP アドレスは，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使用されていないものを含まないため，厳密な数ではありません．この結果に多少の誤差が含まれるとしても，グローバル IP アドレスを適切に整理することで，学外公開のアドレス数の大幅な削減が期待できます．グローバル IP アドレスの申請数と利用数の差は，多くの管理者が不要となったアドレスの申請をしないことが原因と考えられます．故に，有効期限を導入することで，学外公開を継続の必要がないアドレスを回収する仕組みが求められると言えます．

次に，学外公開中の 565 台の機器について，その脆弱性を検査しました．その結果を表 1 と表 2 に示します．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 でした．また 565 台の機器のうち，Low，Medium，High，Critical までの脆弱性を有す機器の数は，それぞれ 20，277，53，40 であり，脆弱性が全く無い機器の数は 175 でした．学外からと学内からでは，異なる通信制御を適用している可能性があるため，一概に調査結果から機器の脆弱性を判断することはできません．この誤差を加味したとしても，High と Critical を合わせた約 100 台の機器が非常に脆弱な状態で学外公開されていることが明らかになりました．故に，学外公開前や学外公開後に管理者が自身の機器の脆弱性を検査する仕組み，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ます．

3 新学外公開 IP 申請システム

事前調査の結果，明らかになった旧学外公開 IP 申請システムの不足機能は次の通りです．

(a) 学外公開の申請が報告制であること
(b) IP アドレスのみに基づいた通信制御を適用すること
(c) 未使用の IP アドレスが学外公開され続けていること
(d) 脆弱性を有する機器が学外公開されていること

これらの問題を解決するために，新学外公開 IP 申請システムでは主に次の 4 点を改善しました．

(a) 現行の報告制から情報基盤運用室による承認制への変更
(b) IP アドレス単位に加え，サービス単位（プロトコルやポート）の通信制御
(c) 学外公開の期間を有効期限制へ変更
(d) 管理者による脆弱性の検査機能の提供

新学外公開 IP 申請システムの処理を図 3 に示します．まず，情報システムの管理者が学外公開を申請します．申請内容に追加したのは主に，(1) IP アドレスに加え，公開するサービス（ポート番号やプ

表 1: 機器が有す脆弱性の総数.

Critical	High	Medium	Low	None
370	679	4328	1510	19181

表 2: 各レベルまでの脆弱性を有す機器の数.

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

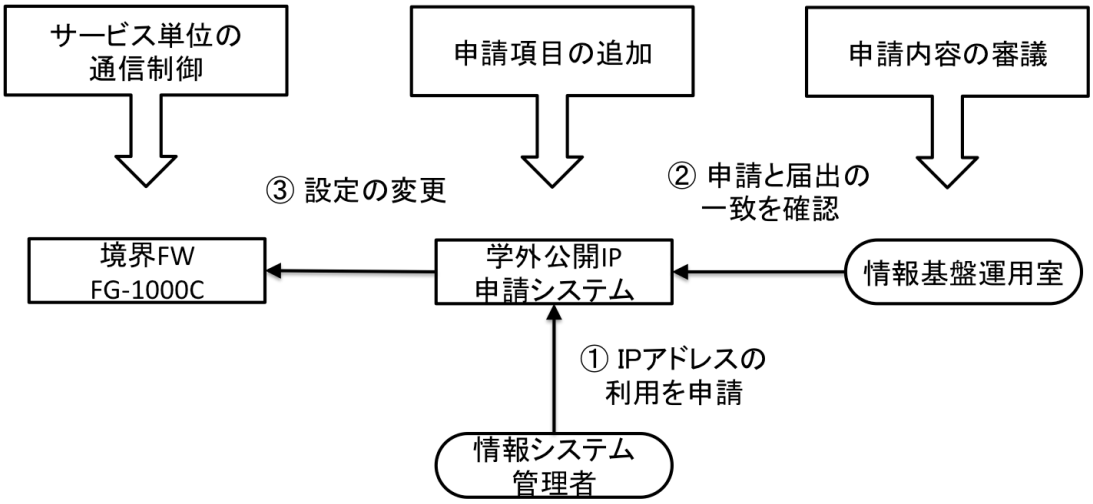

図 3: 新学外公開 IP 申請システム

ロトコル番号），(2) 機器が保有する情報の区分，(3) 学外公開する目的です．次いで，情報基盤運用室で，申請内容と情報システムセキュリティ責任者・管理者届との一致を確認します．申請内容と届出の一致が確認された場合，情報基盤運用室での審議に移ります．審議する項目は，(1) 公開目的が本学の業務として適切か否か，(2) 公開目的と照らし合わせ，適切なサービスのみを学外公開しているか否か，(3) 機器が脆弱性を有しているか否か，(4) 機器が機密情報や個人情報を保持する場合，学外公開することが適当か否かです．審議が可決された後，境界 FW の設定を変更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します．これにより，学外からの通信制御は情報基盤運用室が大学の境界で行い，学内からの通信制御は各部局で行うなど，役割を明確に別けることができるようになります．

上述の変更に加え，システムに新たに導入した 2 つの機能について説明します．まず，学外公開の期間を有効期限制へ変更しました．具体的には，学外公開の期間を年度末までに区切り，年度末の更新申請がないアドレスは，管理者への問い合わせ後に通信を遮断します．次いで，管理者に対して脆弱性の検査機能を提供しました．これにより，学外公開前に脆弱性を検査することや，公開後に管理者に現状を通知することで，高い堅牢性を維持することが期待できます．

4 おわりに

本稿では，旧学外公開 IP 申請システムの問題点を踏まえ，新システムの変更点を説明しました．新システムの導入により，本学のグローバル IP アドレスが適切に管理され，情報システムが高い堅牢性を維持できると考えています．また，脆弱性の改善状況については，広報の場を利用して定期的に報告することを予定しています．

最後に，管理者の皆様には，脆弱性の定期的な対応など，多くのご負担をおかけすることになりますが，ご協力よろしくお願い致します．