◇◇◇◇◇
解　説
◇◇◇◇◇

学外公開 IP 申請システムと脆弱性の推移

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，グローバル IP アドレスの厳格な管理体制を敷く必要があります．

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」に則り，情報基盤運用室では学外公開 IP 申請システムを一新しました．具体的な改善は，(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．本稿では，平成 29 年 12 月から稼働開始した学外公開 IP 申請システムの概要と効果について述べます．

2　学外公開 IP 申請システムの概要

本学のネットワークの概要を図 1 に示します．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学内への通信のみであり，学内から学外への通信には影響を及ぼしません．

学外公開 IP 申請システムの一新により，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

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学外公開を申請します．申請内容は主に，(1) 管理者の問い合わせ先，(2) IP アドレスに加え，公開するサービス（ポート番号やプロトコル番号），(3) 機器が保有する情報の区分，(4) 学外公開する目的です．次いで，情報基

[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

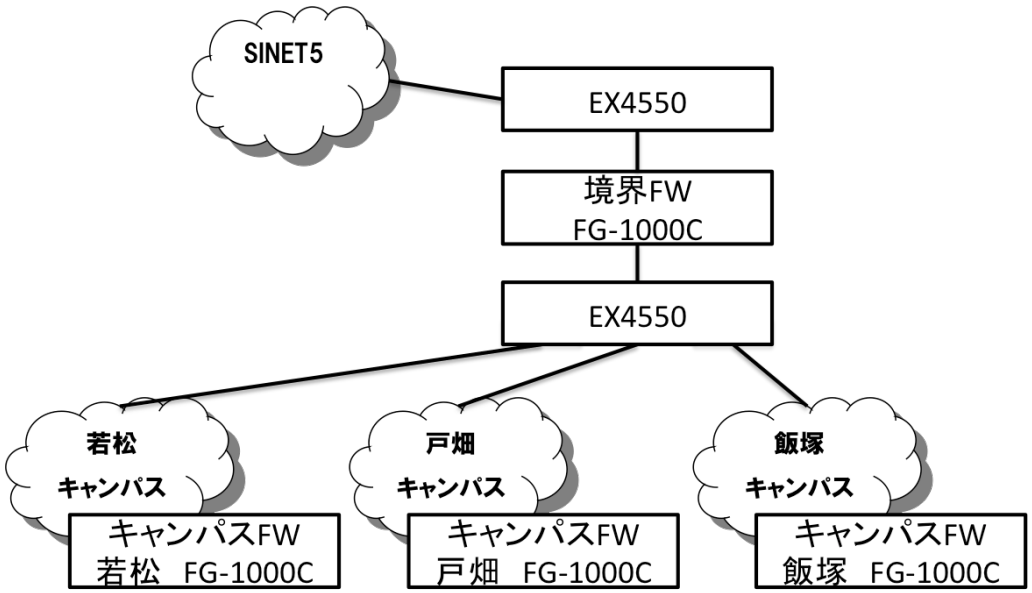

図 1: 本学のネットワークの概要

盤運用室において，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．審議により承認された後，申請内容に基づいて境界 FW の設定を変更することにより，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．

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．

3　学外公開 IP 申請システムの効果

本章では，学外公開 IP 申請システムの効果を，グローバル IP アドレス数と機器の脆弱性の観点から検証します．先ず，学外公開 IP 申請システムの移行前と移行後について比較します．次いで，これまでの運用を通じて定期的な脆弱性の改善が必要なことについて言及します．

3.1　平成 29 年 11 月（移行前）

学外公開 IP 申請システムの移行に先立って，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．平成 29 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ら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

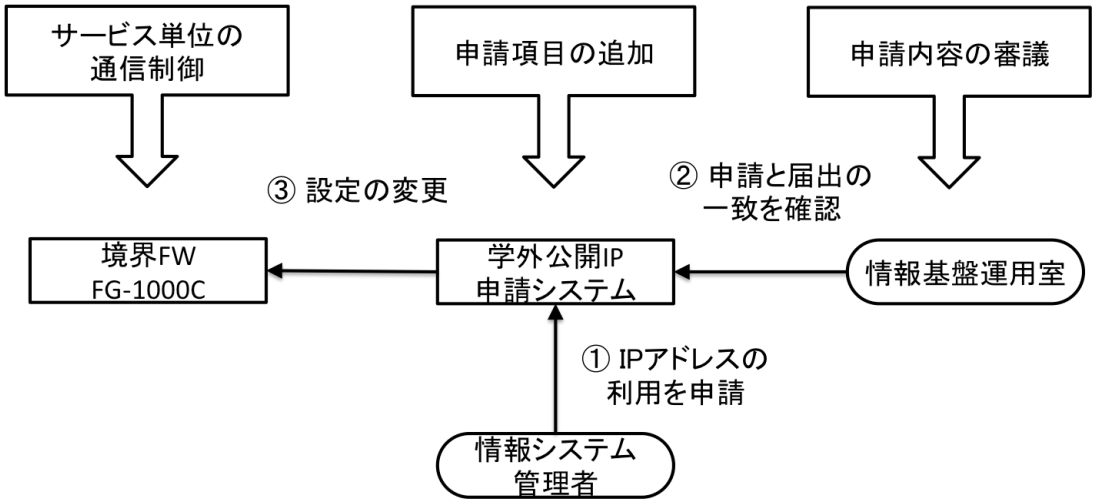

図 2: 新学外公開 IP 申請システム

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削除申請をしないことが原因と考えられます．

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．これら Critical の脆弱性は，OS 自体，または Apache，PHP，Sendmail などの主要なサービスのバージョンが古いことが原因でした．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．

3.2 平成 30 年 5 月（移行後）

平成 30 年 5 月に，学外公開 IP 申請システムの移行作業が完了しました．それに伴い，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再度調査を行いました．情報システムの管理者らが学外に公開しているグローバル IP アドレスの数は 397 でした．故に，グローバル IP アドレスを利用する目的

表 1: 機器が有す脆弱性の総数（平成 29 年 11 月）．

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（平成 29 年 11 月）．

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

表 3: 機器が有す脆弱性の総数（平成 30 年 5 月）.

Critical	High	Medium	Low	None
0	10	409	297	11649

表 4: 各レベルまでの脆弱性を有す機器の数（平成 30 年 5 月）.

Critical	High	Medium	Low	None	Total
0	10	70	66	251	

を見直すことで，学外公開の必要がないアドレスを回収することができたと言えます.

次に，学外公開中の 397 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 3 と表 4 に示します．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 でした．Medium の 282 件は自己証明書によるもの，High の 8 件は誤検知と思われるものです．その他は，学外公開されていないサービスに起因する脆弱性でした．また 397 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 66，70，10，0 であり，脆弱性が全く無い機器の数は 251 でした．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を導入することで，脆弱性を大幅に改善することができたと言えます.

3.3 平成 30 年 11 月（運用半年後）

学外公開 IP 申請システムの運用が約半年を超えた時点で，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再度調査を行いました．情報システムの管理者らが学外に公開しているグローバル IP アドレスの数は 403 で，大きな変化は見られませんでした.

次に，学外公開中の 403 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 5 と表 6 に示します．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 でした．また 403 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 52，77，29，4 であり，脆弱性が全く無い機器の数は 241 でした．これら Critical は，OS のサポート切れと UPnP のバッファオーバーフローによる脆弱性です．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ます．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

表 5: 機器が有す脆弱性の総数（平成 30 年 11 月）.

Critical	High	Medium	Low	None
7	45	531	306	12256

表 6: 各レベルまでの脆弱性を有す機器の数（平成 30 年 11 月）.

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

的に通知する仕組みが求められると言えます.

4　おわりに

本稿では，平成 29 年 12 月から稼働開始した学外公開 IP 申請システムの概要と効果について述べました．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.

現在，管理者に機器の現状を定期的に通知する仕組み，次年度利用するアドレスを申請する仕組みを導入しており，それにより本稿で記述した脆弱性は改善されていることを特筆しておきます．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.