Vol.2016-IOT-35 No.6
Vol.2016-SPT-20 No.6
2016/9/23

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

嶋田 創[1,a)]　山口 由紀子[1,b)]　加藤 芳秀[2,c)]　渥美 紀寿[2,d)]　田上 奈緒[3]　太田 芳博[3]　石原 正也[3]
中務 孝広[3]　川田 良文[3]

概要：研究を活発に行っている多くの大学においては、歴史的経緯により、グローバル IP アドレスを付与した機器が多く、また、個々の研究室の裁量においてそれらの機器のアクセス制限がされていることが多い。これは、研究のために各種サーバを利用したデータ自動集積やデータ共有が多用する事例が多く、また、特殊なサーバ利用形態も多いためである。そのため、このような大学における全学ファイアウォールの導入には多くの障害や混乱が伴うと予想された。そこで、段階的なファイアウォールの導入により、利用者/管理者双方を段階的に習熟させた。これにより、申請数の集中が少ない、混乱の少ない形での導入を実施した。

Phased Installation and Operation of University-Wide Firewall in Nagoya University

Hajime Shimada[1,a)]　Yukiko Yamaguchi[1,b)]　Yoshihide Kato[2,c)]　Noritoshi Atsumi[2,d)]
Nao Tanoue[3]　Yoshihiro Ohta[3]　Masaya Ishihara[3]　Takahiro Nakatsukasa[3]
Yoshifumi Kawata[3]

Abstract: Due to historical background, many research devoting university have many information appliances or servers which utilizes global IP address. Moreover, access controls to those appliances and servers are often authorized to individual laboratories because they often utilize several servers to collecting data or data sharing or some special usage. Thus, there is many possible obstacles and confusion when we installing university-wide firewall to those university. To overcome this problem, we applied phased installation and operation to familiarize both user and administrator of the firewall. We achieved installation with less confusion which does not show converged applications.

1. はじめに

従来の大学の基幹ネットワークにおいては、グローバル IP アドレスを利用した機器に対してファイアウォールによる公開ポートの遮断などを実施する所は少なかった。これは、基幹ネットワークを提供する側 (名古屋大学においては情報基盤センター) に制約されることなく研究に関する情報を公開したり、研究においてネットワークを介した新たなフレームワークを作成することを自由に実施できることを目的としていた。このような自由の担保は、学問の自由、研究の自由に関係するため、ネットワーク基盤を提供する上で重要視されていた。

しかしながら、現在では、情報機器の設定ミスによる情報漏洩やサイバー攻撃による被害が大学組織にとっても大きな問題となってきている。これらのインシデントは様々なメディアに取り上げれるようになってきており、様々な組織の評判に大きな影響を及ぼすようになってきている。

1 名古屋大学情報基盤センター
Information Technology Center, Nagoya University, Furo-cho, Chikusa-ku, Nagoya-Shi, 464–8602, Japan
2 名古屋大学情報戦略室
Information Strategy Office, Nagoya University, Furo-cho, Chikusa-ku, Nagoya-Shi, 464–8602, Japan
3 名古屋大学情報推進部
Information and Communications Technology Services Department, Nagoya University, Furo-cho, Chikusa-ku, Nagoya-Shi, 464–8602, Japan
a) shimada@itc.nagoya-u.ac.jp
b) yamaguchi@itc.nagoya-u.ac.jp
c) yoshihide@icts.nagoya-u.ac.jp
d) atsumi@nagoya-u.jp

Vol.2016-IOT-35 No.6
Vol.2016-SPT-20 No.6
2016/9/23

情報機器の設定ミスによるインシデントについては、特に、ウェブインターフェスを持つデジタル複合機において顕著であり、通信元制限や認証を適切に行わなかったことにより、印刷した内容やスキャンした内容がインターネットに広く公開されるインシデントが多数発生した [1]。このような通信元制限をしていないデジタル複合機は、Shodan[2] や Censys[3] などの検索サービスから情報機器の機器名、OS、ポート公開状態、公開ポート利用しているサービスなどを検索可能であるため、比較的大きな社会問題となった。また、サイバー攻撃による被害については、不用意なネットワークサービスの設定により、単に当該組織に対しての被害を引き起こすのみならず、DDoS 攻撃への参加など、外部に対して被害を発生させるという問題も増えている [4]。

このような現状を踏まえ、名古屋大学においても、SINET と接続する対外接続部において意図しないインバウンド通信の遮断を主目的とした、全学ファイアウォール (以下、FW) の運用を開始した。運用開始にあたって大きな課題となった点は 3 点ある。1 つ目の点は、研究の自由度や即応性を阻害しない FW 運用である。具体的には、研究の過程でに新たにサーバを立てて外部に公開する必要がある場合において、ポート公開の申請の手間の最小化、および、申請から 1 営業日程度で申請に対する承認/却下の結果が得られるシステムと運用体制を実現する必要がある。2 つ目の点は、FW の運用を担うネットワーク担当技術職員の労力の削減である。名古屋大学において運用中のグローバル IP アドレスを付与した機器は 1 万台程度あり、導入開始時の申請の集中、および、新規情報機器の導入が増える年度末/年度始めにおいて技術職員が申請処理に忙殺されることを防ぐ必要がある。3 つ目の点は、IP アドレス管理者に対する FW 申請の周知と申請における混乱防止である。IP アドレス管理者の中には、アウトバウンド通信についても申請が必要と誤解する者、および、管理している機器の公開しなくてはならないポートを正確に把握していない者も数多く存在すると考えられる。そのため、一度に全ポートに対する遮断の実施を行った場合、必要な申請が実施されないことによる弊害、不要な申請が多数されることによる技術職員の負荷増大、不安を感じた管理者による IT ヘルプデスク等への問い合わせの増大、などの混乱が発生することが想定された。

前述した問題に対し、以下の解決策を実施した。1 つ目および 2 つ目の課題に対しては、IP アドレスデータベースシステム (以下、IPDB) と連携したポート公開の申請/承認システムの構築によって問題の緩和を図った。IPDB とは、名古屋大学内において IP アドレスとそれを割り当てた情報機器を登録するデータベースであり、IP アドレス管理者がその更新の義務を負うものとなっている。この IPDB を拡張し、IP アドレス管理者がグローバル IP アドレスに対して公開するポートを申請可能とし、また、技術職員が承認画面からその申請の承認と FW へのアクセス制御リスト (以下、ACL) の投入を可能とすることにより、紙ベースでの申請を不要とした。この構成により、申請者や承認者の申請/承認処理の負荷を緩和するとともに、申請から承認までの即応性に優れたシステムを実現した。2 つ目および 3 つ目の課題に対しては、インシデントが多発するサービスのポート番号からの順次遮断による、IP アドレス管理者へのポート公開申請の習熟、および、申請を処理する技術職員側の習熟を目的として、3 段階に分けた段階導入を実施した。これは、第 1 段階として不用意に起動したウェブサーバによる情報漏洩インシデントの防止を目的とした 80/tcp と 443/tcp ポートの遮断、第 2 段階としてセキュリティインシデントに関係することが多い 14 個のポートの遮断、第 3 段階として全ポート遮断という形でポートの遮断を実施するものである。この段階的な導入により、順次に申請が実施されることによる承認者の負荷の集中を緩和した。本論文では、運用側の話に集中するため、IPDB と連携したポート公開の申請/承認システムについては一般ユーザ側のインタフェースのみを説明し、遮断ポートの段階設定による段階導入について詳細を説明する。

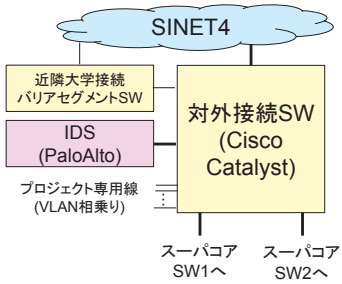

図 1 FW 導入前の対外接続 SW 周りの構成

2. ファイアウォール導入以前のネットワーク構成と利用ポリシ

FW 導入以前の対外接続スイッチ (以下、対外接続 SW) 周りのネットワーク機器構成を**図 1** に示す。図の中央部の対外接続 SW は学外 (SINET4) と学内に跨る部分のルーティングを行う L3 SW である。学内のルーティングについては、別途、コアスイッチが担当しており、対外接続 SW はコアスイッチの一部であるスーパコアスイッチのみと接続されている。対外接続 SW とスーパコアスイッチはスーパバイザを多重化してあり、耐障害性の高い機材としてある。学内では SINET L2VPN サービスを利用するプロジェクトがいくつか存在するが、これらの VLAN 相乗りによる SINET 接続も対外接続 SW が担当している。セキュリティ監視のため、IDS が対外接続 SW に接続されている。また、セキュリティ確保を目的とした ACL が対外接続 SW に投入されている。

Vol.2016-IOT-35 No.6
Vol.2016-SPT-20 No.6
2016/9/23

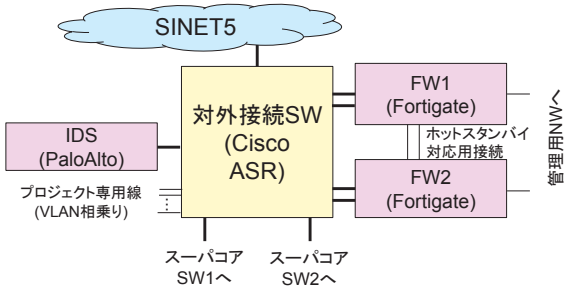

図 2 FW 追加および SINET5 接続後の対外接続 SW 周りの構成

学内ネットワーク利用に関するポリシのうち、セキュリティ確保やインシデント・レスポンス向上を目的とした物に以下のものがある。まず、学内でグローバル IP アドレスを利用する場合、グローバル IP アドレスを割り降った情報機器を IPDB に登録する必要がある。これは、グローバル IP アドレス、MAC アドレス、情報機器名、情報機器の種類、OS、IP アドレス管理者の緊急連絡先、などを登録するデータベースであり、インシデント発生時には、グローバル IP アドレスや MAC アドレスから機器情報/管理者などの検索に利用される。IDS については、インシデント発生時に問題を追跡することを可能とするためのログ保持を主目的とした運用をしており、遮断処理は実施していない。対外接続 SW においてはいくつかのセキュリティ目的の ACL 設定されている。代表的な物としては、グローバル IP アドレスが割り振られた複合機に対する遮断処理、一般的な利用が少ない割にセキュリティインシデントに関係することが多いポートに対するインバウンド通信の遮断処理がある。これらの規則は名古屋大学 情報セキュリティガイドライン [*1] および名古屋大学 情報セキュリティポリシー [*2] において明文化されており、規則に従った運用が行われている。

3. ファイアウォール導入に関連するネットワークの変更

図 2 に FW 導入後のネットワーク構成を示す。図 1 と比較して、FW 機器である Fortinet 社製機器が追加されているのが見て取れる。FW の不具合は対外通信に大きく影響するため、FW 機器は 2 台準備して相互監視を行う冗長構成を取った。また、FW の段階的な導入の途中において、SINET4 から SINET5 への更新が発生したため、SINET5 に対応するための機器更新を行った。このため、対外接続 SW が Cisco 社製 Catalyst から同社製 ASR に変更になっている。

論理ネットワークとしては、FW 機器を通過する通信は名古屋大学における一般的なトラフィック (メール/ウェブ等) のみとし、SINET L2VPN を利用するプロジェクト線の通信は FW 機器を通過しない構成となっている。

[*1] http://www.icts.nagoya-u.ac.jp/ja/security/guideline.html
[*2] http://www.icts.nagoya-u.ac.jp/ja/security/policy.html

4. 申請システムと申請/承認手続き

図 3 に IPDB システムと一体化したポート公開申請処理システムの概要を示す。ポート公開を実施したい IP アドレス管理者は、IPDB の管理対象グローバル IP アドレス一覧より、公開したい機器に付与したグローバル IP アドレスを選択し、ポート公開の申請ボタンを押す。ボタン押下後はポート公開の意思の確認と公開に関する責任の所在の確認のメッセージが表示され、改めてポート公開の意思を確認がされた時点で申請が可能となる。申請システムにおいては、公開するポート番号、プロトコル、公開理由をセットで申請する形となる。ネットワーク担当技術職員は 1 日 1 回程度申請を確認し、妥当な申請であったら承認を、申請に不備があった場合は却下理由を付与して却下を行う。IP アドレス管理者に対しては、申請完了時と申請の承認/却下時にシステムより電子メールが送られるため、必要に応じて、申請内容の再確認や申請の承認/却下の内容を電子メールの上でも確認できる。申請システムは個々のグローバル IP アドレスに対する複数のポート公開申請をまとめた ACL を作成して FW 機器に投入する機能も持ち、技術職員は FW 機器を操作すること無く新規設定を反映できる形となっている。

図 4 に申請システム初期画面を示す。画面上方には過去の申請が一覧で表示され、過去の申請の結果、および、申請取り消しの手続きが可能である。画面下方には新たな申請を行う記入欄が存在する。

図 5 に申請例を示す。最も多いサーバの利用はウェブサーバであると想定されたため、ドロップダウンボックスのみで HTTP/HTTPS、および、コンテンツ更新用の SSH の公開設定を実施可能とした (図 5(a))。ただし、申請理由は各自で公開の妥当さを示す理由を記述してもらう必要がある。それ以外のポートに対しては、図 5(b) に示す自由記述型申請の項目で申請をしてもらう。この欄では、「60000-60004」のような形で一定範囲のポート公開申請が可能である。逆に、学外への通信をインバウンド/アウトバウンドの双方向で遮断したい機器の場合、図 5(c) に示すチェックボックスをチェックすることで遮断申請が可能である。申請された内容は図 5(d) の形で表示されており、「申請取消」のボタンを押すことで取消申請が可能である。

技術職員や IT ヘルプデスクの負荷を減らしつつ、さらなるセキュリティインシデント削減を目的として、申請システムには以下のような様々な細かな機能が存在している。

- 機器種類に応じたポート公開の可否 (例: デジタル複合機のポート公開の禁止)
- 多用される申請 (例: ウェブサーバ) および複雑な申請 (例: テレビ会議システム) のポート公開設定の自動記入

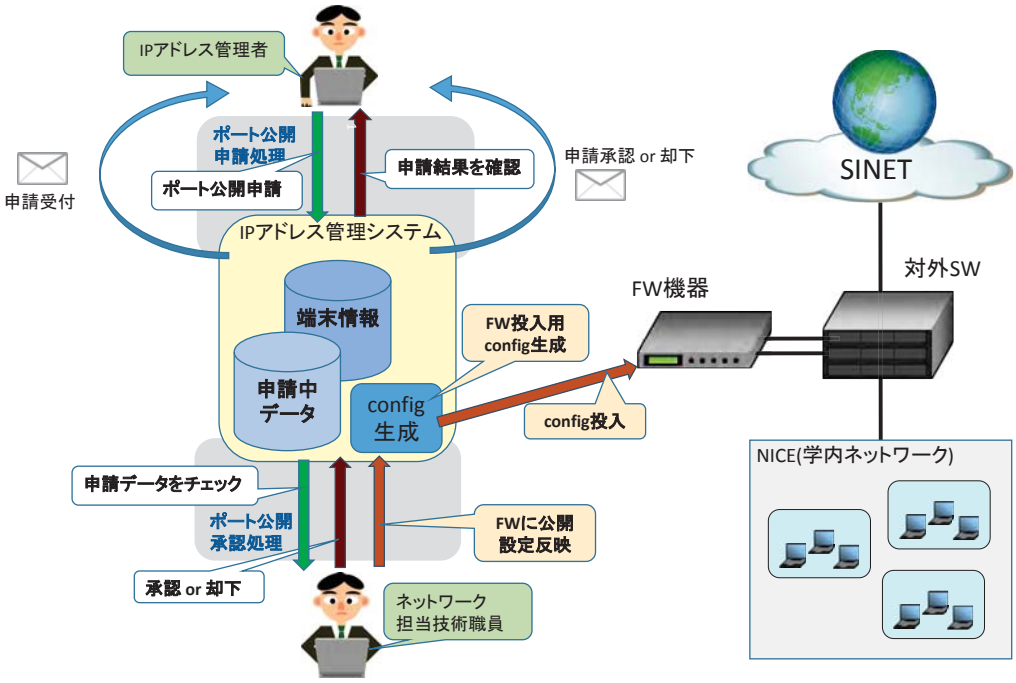

図 3　申請システムと申請/承認手続き

図 4　申請システム初期画面

- アウトバウンド通信の遮断の申請
- グローバル IP アドレス割り当て機器変更時のポート公開設定の引き継ぎの可否

しかしながら、本論文では、研究会論文におけるページ数制約により、その詳細は記さない。また別個の論文として公開を予定している。

5. 段階的なポート遮断における各段階について

FW の運用におけるポート遮断は、申請者/承認者の習熟、申請の集中による負荷集中、導入初期の混乱の低減を目的として、3 段階に分けて実施した。段階的なポート遮断と、それに関連した機器導入、事前告知に関するスケジュールを**表 1** に記す。FW プロジェクトは 2015 年 4 月に発足し、2015 年 11 月の電気設備点検による全学停電の折に機器の接続および FW を通過する経路へのルーティングの変更を完了した。第 1 段階のポート遮断は、不用意もしくは意図せずに起動したウェブサーバによる情報漏洩インシデントの防止を目的とした 80/tcp と 443/tcp とした。これに先行して、各部局の情報セキュリティ担当者が集まる 2015 年 9 月の情報セキュリティ連絡協議会において、FW 導入と 4 節で示した申請システムのプロトタイプについて紹介と意見聴取を実施し、得られた意見を FW 運用案と申請システム案に反映した。

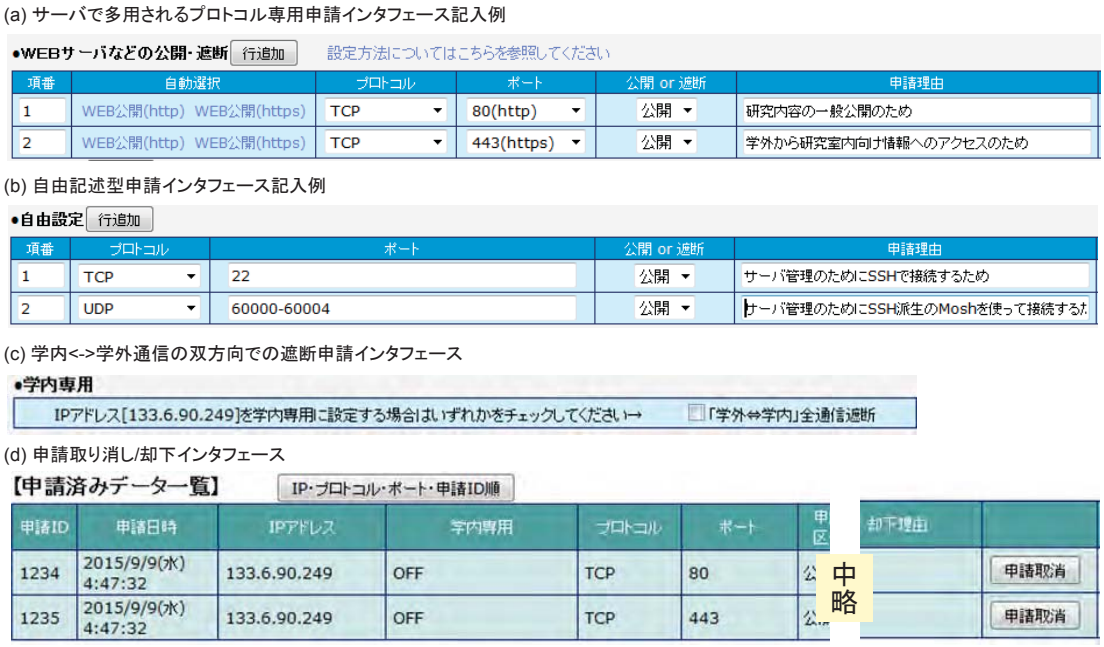

図 5 申請例

第 2 段階としてセキュリティインシデントに関係することが多い 14 個のポートの遮断を実施した。これは、不用意にサービスを起動していてアカウントを乗っ取られる事例、設定不備により DoS 攻撃等に悪用される事例が多発したサービスを提供するポートを対象とした。

最後に、第 3 段階として全ポート遮断という形でポートの遮断を実施をする。第 2 段階と第 3 段階においても情報セキュリティ協議会を通じての事前アナウンスと意見聴取の実施と反映を行っている。他の FW 運用と申請システムのについての意見については、IT ヘルプデスクを通じた問い合わせ、および、IPDB への問い合わせの形で受け付けており、適時反映を実施した。

5.1 第 1 段階: 80/tcp および 443/tcp の遮断

ポートの遮断の第 1 段階として、不用意もしくは意図せずに起動したウェブサーバによる情報漏洩インシデントの防止を目的とした 80/tcp と 443/tcp の遮断を実施した。これは、サーバ機器の導入においてテスト用に起動しておいたウェブインタフェースの放置、新たに導入したデジタル複合機のウェブインタフェースのアクセス制限の設定ミス、などの理由により、ウェブインタフェースを経由した情報漏洩を防ぐことを早急に実施したかったためである。

約 1100 個のグローバル IP アドレスを付与した情報機器に関する申請があり、うち、約 1000 個の機器に対して申請を承認した。主な却下理由は、申請理由と機器の種類から明らかに申請が不要なクライアント機器に対するポート公開申請、デジタル複合機等のウェブインターフェスを学外に公開しようとする申請、FTP/NetBIOS 等のセキュリティ上に公開を許可していないポートの公開申請であった。

第 1 段階における遮断対象は 80/tcp と 443/tcp のみであるが、申請者の都合を考え、今後に遮断されるポートに対する公開申請も可能とした。そのため、ウェブサーバの公開と SCP によるコンテンツ追加を実施するために 22/tcp と 80/tcp の公開申請を同時に行うなどの事例が見られた。また、ポート公開に詳しいグローバル IP アドレス管理者に先行して申請を行なってもらうことで、第 2 および第 3 段階の申請処理における知見を積めるという利点もあった。

5.2 第 2 段階: インシデント多発ポートの遮断

第 2 段階の遮断として、セキュリティインシデントに関係することが多い 14 個のポートの遮断を実施した。**表 2** に第 2 段階における遮断ポートを示す。

設定不備により DoS 攻撃や SPAM 配信に悪用される事例が多発したサービスとして、SMTP, DNS, NTP を遮断対象とした。なお、名古屋大学のサブドメインにおいて SMTP サーバを運用する場合は名古屋大学の SMTP gateway を経由することが必須となっており、また、サブドメインの名前解決は全学の DNS サーバが担当することになっているため、プロジェクト等で独自ドメイン運用を行っていない限り、SMTP と DNS に対する公開申請は不要となっている。不用意にサービスを起動していてアカウントを乗っ取られる事例の多いサービスとして、SSH, telnet, POP3, IMAP4, Submission, OpenVPN, PPTP, Microsoft Remote Desktop を対象とした。

これらのサービスを運用する機器管理者の労力削減のため、サービスと公開すべきポートの対応表の作成を実施

Vol.2016-IOT-35 No.6
Vol.2016-SPT-20 No.6
2016/9/23

表 1 全学ファイアウォールの段階的なポート遮断と関連イベントのスケジュール

年月	実施内容/イベント
2015 年 4 月	FW プロジェクト始動
2015 年 7 月	情報セキュリティ連絡協議会における FW 導入予告
2015 年 9 月	情報セキュリティ連絡協議会における第 1 段階遮断実施予告とプロトタイプ申請システム紹介
2015 年 11 月下旬	FW 機器設置/接続完了と第 1 段階 (80/tcp,443/tcp) 遮断/申請案内アナウンス
2015 年 12 月下旬	第 1 段階遮断実施
2016 年 3 月	情報セキュリティ連絡協議会における第 2 段階遮断実施の予告
2016 年 4 月上旬	第 2 段階 (インシデント多発ポート) 遮断/申請案内アナウンス
2016 年 5 月上旬	第 2 段階遮断実施
2016 年 6 月	情報セキュリティ連絡協議会における第 3 段階遮断実施の予告
2016 年 8 月中旬	第 3 段階 (全ポート) 遮断/申請案内アナウンス
2016 年 9 月中旬	第 3 段階遮断実施

表 2 ポート遮断第 2 段階における遮断ポート

ポート番号	用途
22/tcp	SSH
23/tcp	telnet
25/tcp	SMTP
53/tcp, 53/udp	DNS
123/udp	NTP
110/tcp,995/tcp	POP3/POP3S
143/tcp,993/tcp	IMAP4/IMAPS
587/tcp	Submission
1194/tcp	OpenVPN
1723/tcp	PPTP
3389/tcp	Microsoft Remote Desktop

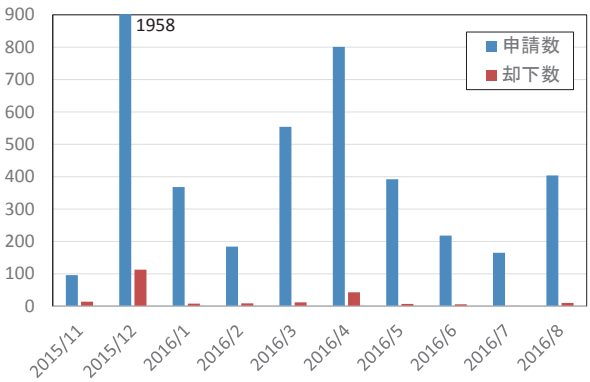

図 6 申請数と却下数の推移

した。

5.3 第 3 段階: 残りの全ポートに対する遮断

第 3 段階では全ポート遮断という形でポートの遮断を実施する。

実施にあたり、IPDB に登録された情報機器一覧や 5.1 節に記した、先行してポート公開申請が実施された事例を参考に、全ポート遮断下において機器運用のためのポート公開申請時に機器管理者が苦労しそうな機器について事前に検討を行った。検討の結果、テレビ会議システムは公開が必要なポート数が複雑な割に事務部の管理であることが多く、そのままでは遮断後の機器運用で問題の発生が多発することが予想された。そこで、特に利用が多い Polycom 社の 2 地点接続の機器に対しては、ポート公開申請システム上において、1 クリックで必要な申請内容を記入できる機構を準備した。

6. 申請/承認/却下に関するデータ

2015 年 11 月の申請開始から 2016 年 8 月 30 日までの申請データを以下にまとめる。2427 個のグローバル IP アドレスに対して申請を受け付けた。51 個のグローバル IP アドレスについては、申請はあったが、情報セキュリティガイドライン等への違反や不必要な申請であったために却下した後、再申請は行われなかった。

6.1 申請数と却下数の推移

図 6 にポート公開申請数と却下数を記す。グラフの横軸は一ヶ月単位での時間であり、縦軸は一ヶ月あたりの申請数/却下数である。グラフの申請数においては、申請後、承認/却下される前に取り消された申請は除外してある。また、グローバル IP アドレスを与えた機器 1 つに対して複数回の申請がされた場合 (例: 80/tcp と 443/tcp の公開申請を別個に行ったもの)、個々の申請に対してカウントを実施してある。

図より、第 1 段階の遮断を実施した 2015 年 12 月に特に大きなピークがあることが分かる。これは、単に第 1 段階で遮断される 80/tcp と 443/tcp に対する申請があったのみならず、5.1 節に記したように、将来の追加遮断も見越した申請が多かったこと、および、単に申請が必要と勘違いした、80/tcp と 443/tcp 以外のポートの公開申請も含まれているからである。各段階の実施の月 (2015 年 12 月、2016 年 5 月、2016 年 9 月) とその間の申請数確認すると、2015 年 11 月〜12 月が 2054 件、2016 年 1 月〜4 月が 1907 件、2016 年 5 月〜8 月が 1179 件とおおむね似たような申請数となっており、実施した 3 段階による導入による申請/承認側の負荷分散は実現できたと考えられる。

表 3　TCP における承認されたポート公開申請の上位 20 種類

ポート	申請数	割合 [%]
80	869	22.1
443	732	18.7
22	454	11.6
993	183	4.7
995	183	4.7
465	169	4.3
587	163	4.2
143	149	3.8
110	99	2.5
3389	54	1.4
1723	52	1.3
1720	51	1.3
5900	44	1.1
10022	43	1.1
25	42	1.1
514	35	0.9
8433	35	0.9
8834	35	0.9
1194	23	0.6
53	20	0.5
その他	489	12.5

6.2　公開が承認されたポートの内訳

表 3 に TCP における承認されたポート公開申請の上位 20 種類を示す。80/tcp と 443/tcp によるウェブサーバ公開が 1,2 位を占めている。25/tcp と比較して 110/tcp, 143/tcp, 587/tcp, 993/tcp, 995/tcp への申請が多いが、これは、名古屋大学のサブドメインにおける SMTP サーバは名古屋大学の SMTP gateway を経由するために 25/tcp の公開は不要となっているためである。514/tcp, 8433/tcp, 8834/tcp という珍しいポートの公開申請があるが、これらは、同一の IP アドレス管理者からの申請である。

6.3　申請が実施された時間帯

図 7 に申請が行われた時間帯の分布を、3 時間単位に区切った 24 時間表記の時間で表す。一般的な労働時間である、9-18 時の申請が 80.6%を占めるが、それ以外の時間帯の申請も多数あり、0-6 時のような深夜帯における申請も 2.4%存在した。よって、任意の時間帯に申請できるシステムによる利便性の向上の効果はあったと考える。

6.4　申請から承認までの経過時間

技術職員側が習熟し、安定して申請承認処理が可能になった第 1 段階の運用開始後の、申請から承認までの経過時間の分布を**図 8** に示す。対象となった申請の数は 2685 個である。図より、69.5%の申請が 9 時間以内に承認されており、IPDB 連携のポート公開申請システムによる利便性の向上の効果はあったと考える。なお、10.2%存在する承認までに 48 時間以上かかった申請は、休日における申請や申請内容が審議案件になった申請などである。

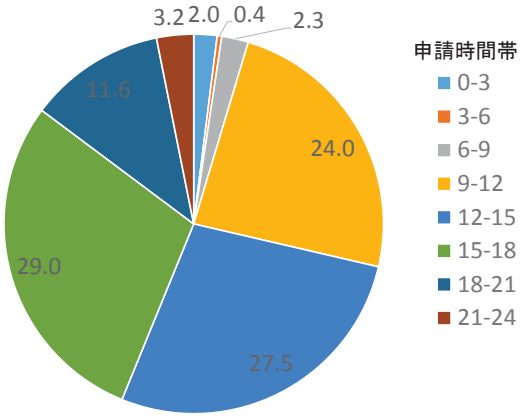

図 7　申請が実施された時間帯

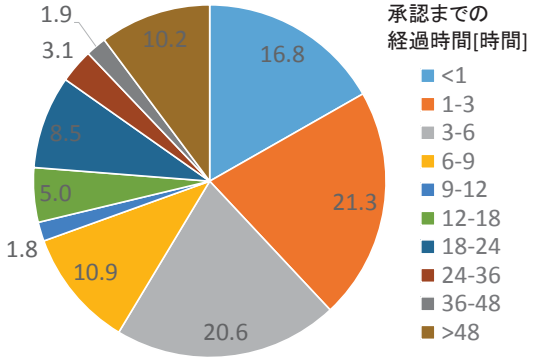

図 8　申請から承認までの経過時間

7.　導入において得られた知見

導入において得られた知見において、著者が特に情報共有する価値があると感じたものについて記す。

7.1　NICE 遮断ポートの運用変更

従来より、名古屋大学では対外接続 SW に設定した ACL により、サイバー攻撃に悪用されるポートや P2P 接続において待受にされるポートなどのいくつかのポートに対する通信を遮断していた。これらは NICE 遮断ポートと名付けられ、インシデント等の発生等の折に追加されて行ったため、総数が 100 個近くとなっていた。この NICE 遮断ポートはポート公開申請自体を禁止していたが、第 3 段階の遮断により全ポートがデフォルトで遮断状態になること合わせて、この NICE 遮断ポートを以下のポリシのもとに整理し、40 個程度に削減した。

- パスワードを暗号化せずに送信するプロトコルが利用するポート番号
- 設計が古くセキュリティ上問題がある割に現在も利用が続くプロトコルが利用するポート番号
- サイバー攻撃によく悪用されるプロトコルが利用する

ポート番号

なお、上記のポリシにおいては、従来の NICE 遮断ポートでは公開可能であった telnet, POP3, IMAP4 が公開禁止となるが、公開状態で運用中のポートの新規に遮断することはグローバル IP アドレスを付与した機器管理者のみならず、その機器を利用しているユーザにも影響があり、大きな混乱を生むと考えた。そのため、新規の公開申請の受付のみを却下し、公開状態で運用中のポートへの遮断は見送った。

7.2 特殊なポート番号割当への対応

第 2 段階の遮断において、あるサービスに対して標準のポートとは異なるポートを割り当てて運用している事例に対する遮断が懸念された。例えば、80/tcp が標準のポートである HTTP に対し、下 2 桁が 80 となる 4-5 桁のポート番号を割り当てる事例や、22/tcp が標準のポートである SSH に対し、一部に 22 という数字の並びが含まれる 4-5 桁のポートを割り当てる事例がある。これらの事例は、第 1 段階の遮断から先行して受け付けている、まだ遮断対象でないポートに対する公開申請の中でも散見された。検討の結果、このようなポート割当を実施する機器管理者は情報機器に対する知見が深いものと考え、第 3 段階の全遮断まで申請なしで公開状態にあってもセキュリティインシデントに至る確率は低いと判断し、特に対応を取らなかった。

7.3 特殊なプロトコルへの対応

いくつかの VPN 接続において、TCP/UDP 以外のインターネットプロトコル (以下、IP) を利用する物がある。具体的には、GRE(IP 47 番)、ESP(IP 50 番)、AH(IP 51 番) が利用されている。本 FW プロジェクトにおいてはこれらのプロトコルの遮断は想定しておらず、当初のポート公開申請システムでは対応がされていなかった。しかしながら、申請者側に取っては公開申請できないことがそのサービスの継続利用に不安を持たされることになるため、システムを改修して申請可能とした。

8. 終わりに

FW の導入において、申請者の利便性、承認者側の負荷低減、導入初期の混乱の低減を目的として、3 段階に分割した FW の導入の実施した。第 1 段階の実施においては、申請側/承認側ともにかなりの混乱が見られたが、第 2 段階以降は遮断対象としたポート数を増やしたにもかかわらず申請に関するトラブルは減り、当初の目的である申請者側の利便性と承認者側の負荷低減は実現できたと考える。これは、開発した IPDB 連動のポート公開申請システムにも依る所がある。

残る課題として、学内ネットワークにおけるアクセス制限への拡大が挙げられる。近年では By Your Own Device の形で情報機器を運用する情報基盤センターのサービスが存在し、また、そのような運用が行われている研究も学内には多々存在する。そのため、マルウェア感染機器がいきなり学内に現れ、アウトバウンド通信で接続した学外の C&C からの司令をもとに、学内に対してポートスキャンをかける事態が想定される。このような攻撃が想定されるセグメント (例: 全学無線 LAN セグメント) に対するポート公開の可否を設定させるという対策が考えられる。

参考文献

[1] 独立行政法人 情報処理推進機構, 複合機等のオフィス機器をインターネットに接続する際の注意点, (2013). https://www.ipa.go.jp/about/press/20131108.html.
[2] Shodan, https://www.shodan.io/.
[3] Censys, https://www.censys.io/.
[4] 総務省, 電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会第一次とりまとめ, (2014).