名古屋大学全学ファイアウォール向けポート公開申請･承認システムの開発

田上奈緒 [1)], 太田芳博 [1)], 石原正也 [1)], 中務孝広 [1)], 川田良文 [1)],
渥美紀寿 [2)], 加藤芳秀 [2)], 山口由紀子 [3)], 嶋田創 [3)]

1) 名古屋大学 全学技術センター
2) 名古屋大学 情報連携統括本部情報戦略室
3) 名古屋大学 情報基盤センター

tanoue@icts.nagoya-u.ac.jp

Development of Port Open Requesting and Granting System for University-Wide Firewall at Nagoya University

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

1) Technical Center, Nagoya Univ.
2) Information Strategy Office, Information and Communications, Nagoya Univ.
3) Information Technology Center, Nagoya Univ.

概要

名古屋大学では，2015 年 12 月対外接続ファイアウォールの運用を開始し，あらかじめ許可された IP アドレス，プロトコル，ポート以外の学外から学内への通信は遮断されることとなった．これに伴い端末管理者によるポート公開申請手続き，ネットワーク管理者による承認手続きとファイアウォールへの ACL 投入を簡便化するため「ポート公開申請・承認システム」を開発したので，その内容と導入後の状況について述べる．

1. はじめに

大学では，自由な研究・実験を優先するため大学内外のネットワーク通信・情報発信を制限しない傾向にあった．しかしながら近年の情報セキュリティインシデント増大により，ネットワーク通信を制限する必然性が高まってきた[1]．名古屋大学では2015年12月にファイアウォール(以下FW)の導入・運用が開始され，申請許可されていない学外からの通信遮断を実施することとなった．このネットワーク通信制限を円滑に実現するために，名古屋大学情報基盤センターの教員により，既存で運用されている「IP アドレス管理システム」と連携する形で「ポート公開申請・承認システム」を構築することが考案された．

2015 年 4 月にプロジェクトが立ち上げられ，ネットワーク・情報セキュリティ関連教員や情報系技術職員がメンバーとなり，2015 年 12 月の FW 運用開始と通信制限実施に向けて各々の担当業務を遂行してきた．

本稿では主に，「機器毎に学外公開が必要なポートの申請受付け，管理側による各申請データの承認・却下決定と FW への ACL 書込み」を WEB 上で実行可能にする目的で開発された「ポート公開申請・承認システム」に焦点を当て記述する．

2. 「ポート公開申請・承認システム」の概要

2.1 システム開発の経緯と目的

FW 導入前は対外接続 L3 スイッチにて，悪用の危険性が高いポートや，グローバル IP アドレスで運用されている複合機など情報漏えいの恐れがある特定機器を個別に通信遮断していたが，大学内で自由にネットワークに接続される新しい機器に迅速に対応するためには，学外からの全通信を遮断した上で公開の必要な IP アドレス,プロトコル,ポートのみ許可するポリシーとした方がより安全性が高まる．

そこで FW の導入が検討され，上記ポリシー実現のため「ユーザによる学外公開したい IP アドレス，プロトコル，ポートの申請手続き」「管理側における申請データの承認・却下手続き」「承認された申請情報からの ACL 作成と FW への投入」を行う WEB システムを構築することとなった．

図 1，2 に FW 導入前，導入後の対外接続部ネットワーク構成を示す．FW 機器としては Fortinet 社製を採用し 2 台構成で冗長化している．

この機器は ACL 書込みを SSH 接続した上でコマンド実行によって行えるため，WEB システム側では申請データに基づき ACL 書込みコマンドを組み立て，FW のシェル上で実行することになる．

上記を実装するために開発した「ポート公開申請･承認システム」による処理手順を図 3 に示し，

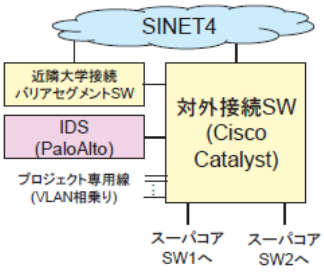

図 1. FW 導入前対外接続部構成

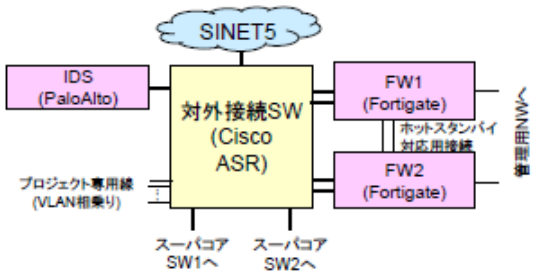

図 2. FW 導入後対外接続部構成

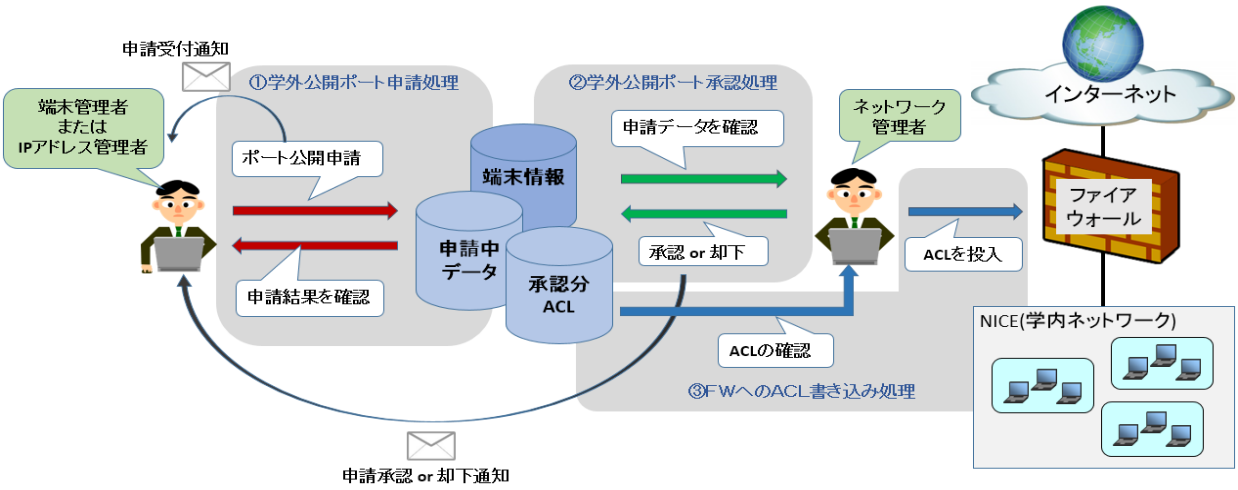

図 3. ポート公開申請・承認システムによる処理手順

続いて図内の「①学外公開ポート申請処理」「②学外公開ポート承認処理」「③FW への ACL 書き込み処理」について，各概要を 2.2～2.4 節で説明する．

2.2 ユーザによる「①学外公開ポート申請」

本学では，FW 導入以前より「IP アドレス管理システム（以下 IPDB）」が運用されており，学内ネットワーク内で使用されているグローバル IP アドレスとそれが割り当てられている機器，管理者の情報を登録することが義務付けられている．LAN 上を流れているパケットは別システムにより監視されており，未登録 IP アドレスは管理者に警告の後，通信遮断される．よって基本的には使用中のグローバル IP アドレスはすべて IPDB に登録・管理されているため，このシステムに IP アドレス毎のポート公開申請処理を組み込むこととなった．

ユーザは管理する端末のポート公開をする際，該当する「IP アドレス情報変更」ページより図 4 に示す「ポート公開申請」ページを開く．

本ページで申請可能な公開・遮断データの種類は

1) 新規登録時 IP アドレス単位デフォルト遮断
2) IP アドレス単位学外・学内両方向通信全遮断
3) 特定 IP アドレス・プロトコル・ポートの公開

の 3 種類である．1)は IP アドレス情報を IPDB に新規登録した場合，その IP アドレスへの学外から学内への通信をデフォルトで全遮断する申請を自動発行し，サーバ構築直後に不必要なポートが無自覚のまま開いている状態を防ぐものである．これは，FW により許可された申請以外は「学外→学内全遮断」されるため不必要に思われるが，後述するように突然学外からの通信をすべて遮断することによる混乱を避けるため，一定期間に段階を踏んで全遮断に移行するようスケジュールが組まれた．そこで最終的な全遮断に至るまでの一時的な措置として，新規登録時は IP アドレス単位の「学外→学内全遮断」申請を自動発行することになった．2)は学内通信のみで学外と通信する必要のない機器を IP アドレス単位に学外・学内両方向通信遮断するためである．3)は 1)で IP アドレス単位に全遮断した上で，公開が必要なプロトコル・ポートのみを公開理由を付加した上で申請するものである．

2.3 管理者による「②学外公開ポート承認」

利用者によって申請されたポート公開情報は一旦データベースに保存されるが，これらは直接 FW に反映されるのではない．ネットワーク管理者は図 5 に示す「ポート公開承認・却下」ページにて保存されている申請一覧を確認し，1 行ずつ申請内容をチェックした結果「承認」または「却下」の判定をする．「却下」される申請は，公開禁止されているポート・不必要な公開申請・申請理由が不適切などの理由による．利用者側が要求する不適切なポート公開が FW に反映されるのを防ぐため人を介したチェックが必要不可欠となる．

図 4. IPDB 内「ポート公開申請」ページ

図 5. 「ポート公開承認・却下」ページ

承認された申請については，その内容から ACL を FW に書き込むコマンドが自動作成されデータベースに保存されると同時に，利用者に承認通知がメール送信される．却下された申請については ACL 作成が行われず，入力された却下理由を付加したメールが利用者に送られる．

2.4 管理者による「③FW への ACL 書き込み」

作成された ACL も直接 FW に書き込まれず，やはりデータベースに一旦登録される．「ポート公開承認・却下」ページにて複数申請を選択の上「承認実行」された最新の FW 書込みコマンドを「FW コマンド表示」で確認可能である．

確認の結果，問題なければ FW に SSH で接続しコマンドを投入するが，これも確認ページから「FW コマンド送信」するのみで投入可能になっている．

2.5 申請データの状態遷移

上記のとおり，ユーザにより申請されたポート公開情報はすぐには FW に書き込まれず，1 日 1 回のネットワーク管理者による「承認」「ACL 書込みコマンド投入」で FW へ反映されるため，ユーザの申請とタイムラグがある（「申請中」→「FW 反映済」）．

また，開いたポートを閉じる場合は「ポート公開申請ページ」にて，ユーザにより「廃止申請」が発行される．「廃止申請」も同様にネットワーク管理者により「承認」され，そこから ACL 削除コマンドが自動作成された後 FW へ投入される（「廃止申請中」→「FW 消去済」）．

これらの手続きの流れに伴い申請データは図 6 のように状態遷移する．

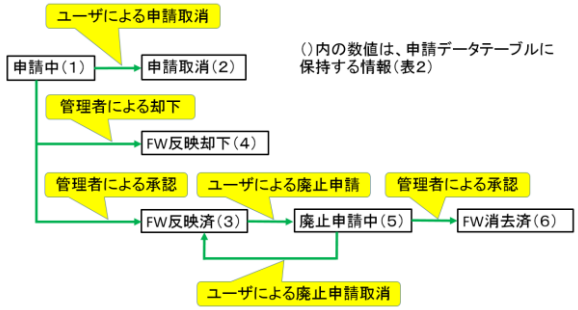

図 6. 申請・承認処理による状態遷移

2.6 IPDB との連動

IP アドレス情報とポート公開情報はシステム内では別テーブルに登録されるが，親子関係にあるため親である IP アドレス情報更新時には，自動的にその子レコードであるポート公開情報も適宜更新される．

前述した IP アドレス新規登録時の「学外→学内デフォルト遮断」自動発行もその一環だが，そのほか，例えばサーバの IP アドレス変更時，旧 IP のポート公開データがあれば自動で申請取消・廃止申請が行われ，新 IP の同じポート公開申請が自動再発行される．このためユーザが旧 IP のポート公開を FW から明示的に削除し忘れても自動的に消去されるようになっている．

機種種別を「プリンタ」「スキャナ」に変更時もポート公開情報は自動で申請取消・廃止申請される．

上記以外の項目変更時は，ユーザ選択によりポート公開情報を申請取消・廃止申請できる．

またサーバ廃止などによる IP アドレス情報削除時には，ポート公開データがあれば自動で申請取消・廃止申請が行われるため，削除済み IP アドレスのポートが公開されたままになるのを防ぐ．

3. 「ポート公開申請・承認システム」構成

3.1 動作環境

本システムは「IPDB」に組み込まれる形で開発されたため，サーバなど動作環境は既存のものを使用しており，専用で設置はしていない．

そのため基盤となっている「IPDB」の動作環境を表 1 に示す．

表 1. 動作環境

ハードウェア	IBM BladeCenter
仮想化環境	XenServer6.5
OS	CentOS 6.3 (32bit)
WEB サービス	Apache-2.2.15 + OpenSSL
データベース	PostgreSQL 9.1.5
開発言語	PHP 5.3.3
認証サービス	CAS, LDAP

3.2 データベース論理構成

データベースも IPDB 内に既存の「IP アドレス情報テーブル」との関連性を持たせるため，表 2 で示す 4 つのテーブルを追加した．

表 2. 各テーブルの概要

テーブル名	用途
申請 テーブル	ユーザが IP アドレス毎に登録したポート公開申請情報が保存される． 申請状態 1:申請中 2:申請取消 3:FW 反映済 4:FW 反映却下 5:廃止申請中 6:FW 消去済
申請時属性 テーブル	申請時の属性情報（機器名称，機器種別，OS，MAC アドレス，管理者情報など）を保持するために別途「申請時属性テーブル」に登録される．
承認時 申請一時 テーブル	承認・却下ページにて全申請データを一覧表示するが，その間もユーザにより申請テーブルは更新される．承認処理中は初期表示時の状態をページ遷移しても保つため、全申請データを一時テーブルに一括コピーし，そこから一覧表示する．
FW コマンド テーブル	承認・却下ページにて「承認」された申請（or 廃止申請）データから作成した ACL 書込み（or 削除）コマンドが登録される．

図 7 にテーブル関連図を示す．→の先が外部キーのリレーション先である．

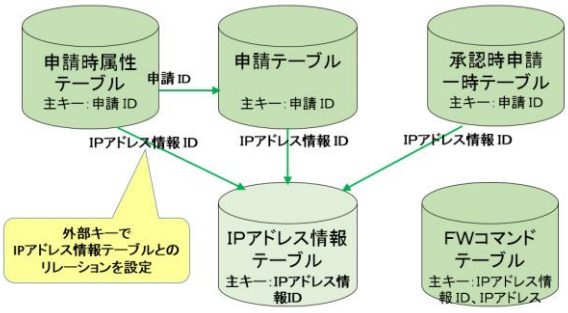

図 7. テーブル関連図

3.3 プログラム構成

図 8 にプログラム関連図を示す．図 3 の「ポート公開申請・承認システムによる処理手順」をシステム的な観点で表したものとなる．

基本的に WEB 上の 1 ページにつき 1 プログラム作成している．

図内の①～④がプログラムであり，各々の仕様について次に記す．機能については 2 節でほぼ説明済みのため，ここでは未記述の内容を補足する．

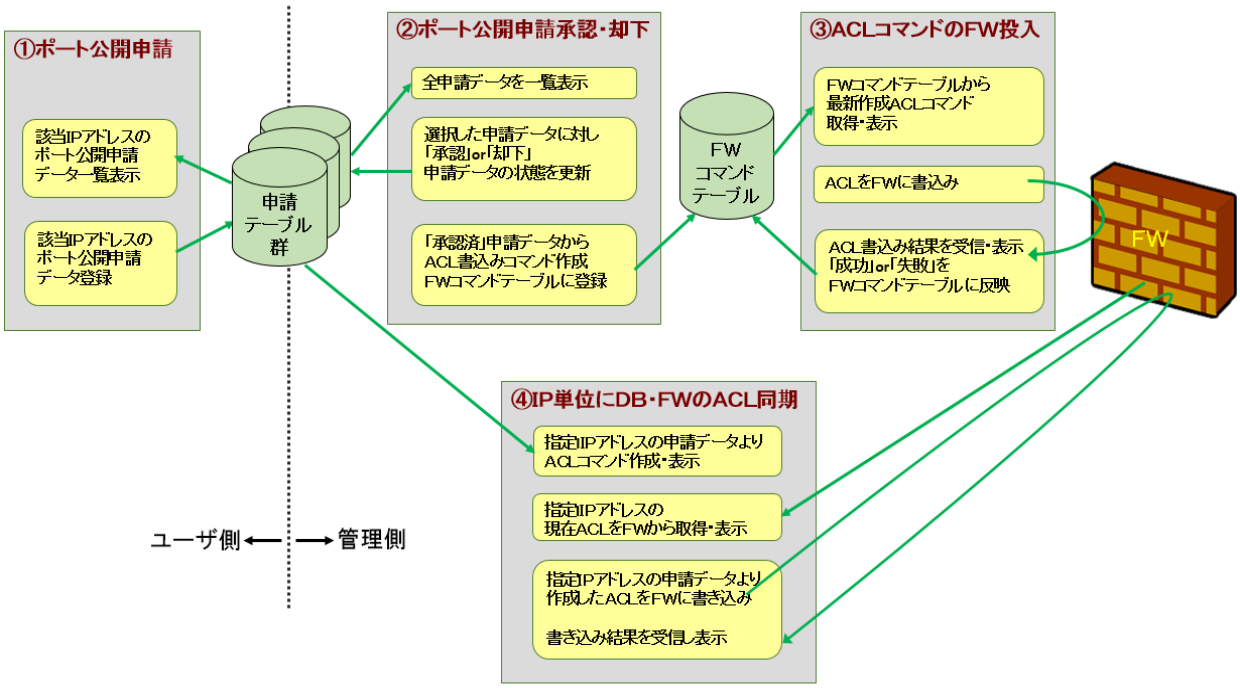

図 8. プログラム関連図

①ポート公開申請・・・ユーザが IP アドレス単位にポート公開申請する機能（図 4）.

ページ上部には「申請済みデータ一覧」が表示され，申請された各データの現在状況（申請中，申請取消，FW 反映済み，FW 反映却下，廃止申請中，FW 消去済）を確認できる.

ユーザは各申請データについて以下の操作が可能である.

「申請中」データの「申請取消」

「FW 反映済」データの「廃止申請」

「廃止申請中」データの「廃止申請取消」

これらユーザ側による申請に対する要求と管理側の承認・却下による状態の遷移を図 6 に示した.

ページ下部には「公開申請入力欄」があり

1)「WEB 公開」…TCP80,443 公開専用

2)「自由設定」…プロトコルとポート番号指定

3)「学内専用」…学内両方向通信全遮断

の申請に分かれている.

プロトコルは「TCP」「UDP」「TCP&UDP」「ICMP」「AH」「ESP」「GRE」より選択可能，ポート番号はカンマ区切りによる複数指定・ハイフン区切りによる範囲指定が可能である.

これらを組み合わせて入力し「申請実行」ボタンクリックにより，入力チェック通過後申請テーブルに登録される.

②ポート公開申請の承認・却下・・・管理者がユーザにより申請されたデータを確認した上で「承認」または「却下」する機能（図 5）.

全申請データが一覧表示され，

「申請中」データは「承認」「却下」が選択可

「廃止申請中」データは「承認」のみ選択可

複数行を選択した上で「承認実行」すると，「申請中」は「FW 反映済」に，「廃止申請中」は「FW 消去済」に更新され，FW に投入される ACL 書込みコマンド，ACL 削除コマンドが組み立てられ FW コマンドテーブルに保存される.

③ACL コマンドの FW 投入・・・作成された ACL コマンドを表示，FW に反映する機能（図 9）.

図 5 の「FW コマンド表示」で別ページへ遷移し，承認により作成された最新の ACL コマンド群を FW コマンドテーブルより取得し表示する．また「FW コマンド送信」クリックで ACL が FW に投入され，その結果を受信する．受信結果を表示すると同時に，FW コマンドテーブルに「OK」または「NG」を書き込む.

④IP アドレス単位の DB・FW　ACL 同期・・・データベース上の申請データと FW の ACL に違いが生じてしまった際に，FW 側の ACL を上書きして同期をとるための機能（図 10）.

図 5 の「IP 毎 FW 書き込みコマンド作成」で別ページへ遷移する．そこで IP アドレスを入力し「IP 毎コマンド作成＆FW 現在値取得」クリックにより，指定 IP アドレスの申請データをすべて読み、ACL コマンドを作成・表示する．と同時に FW から取得した指定 IP アドレスの ACL 現在値を表示し，比較を可能にする.

「コマンド反映」クリックで申請データから組み立てた ACL を FW に投入し，書き換わった ACL を再表示する.

通常使用することはないが，申請データと FW の不一致発生時の対処用として作成した.

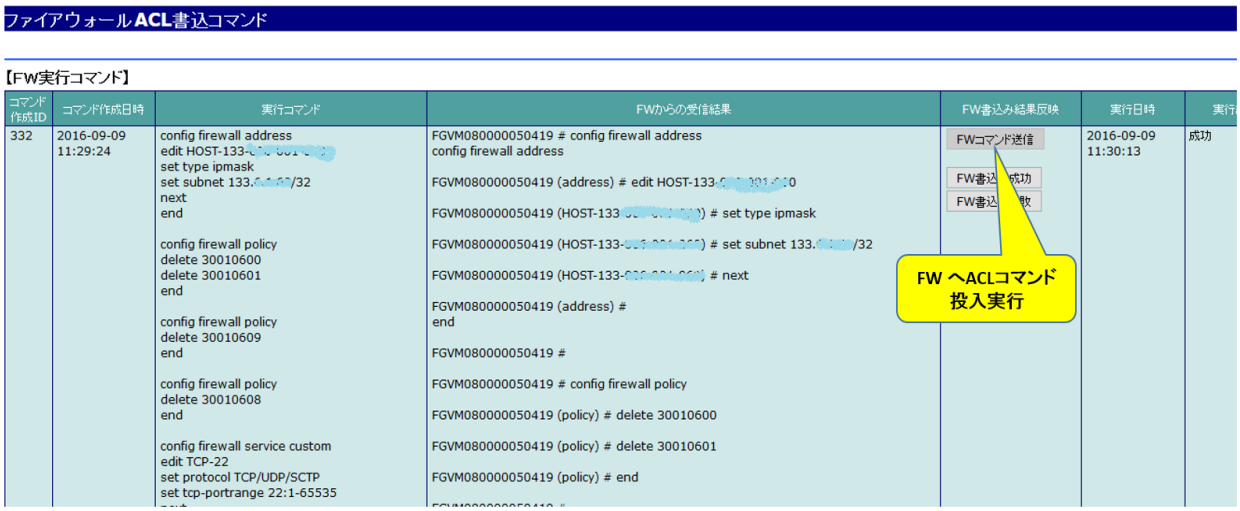

図 9. FW への ACL コマンド投入

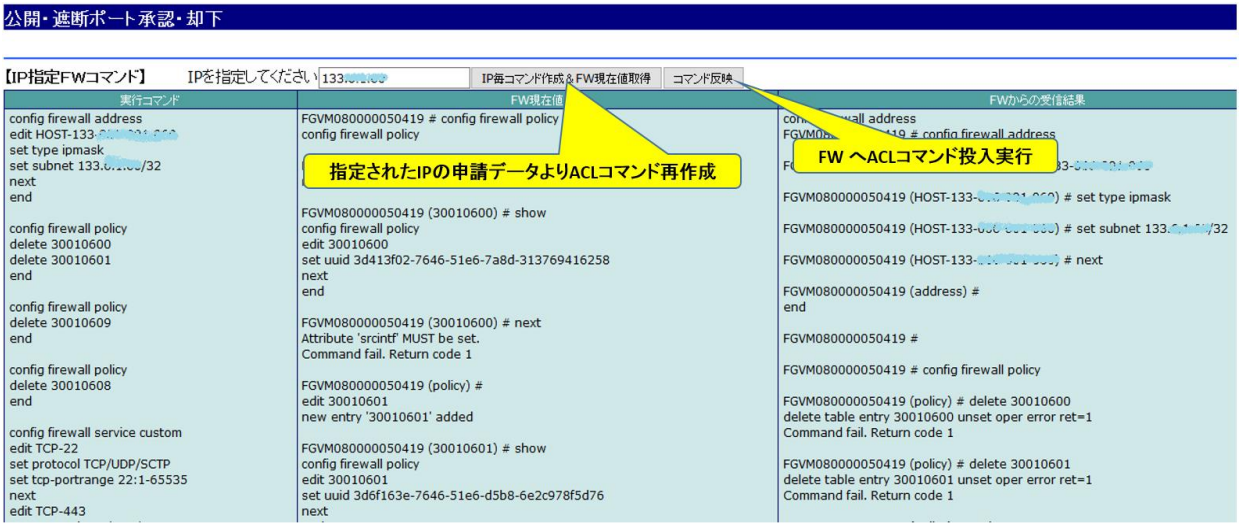

図 10. IP 指定 ACL コマンド投入

上記①～④は「ポート公開申請・承認システム」として新規作成したプログラムの説明になる．実際は IPDB と関連・連動する処理となるため，既存のシステムにも改修を施したがここでは割愛する．

また③④の処理にて ACL 投入と投入結果受信の際に FW と通信することになるが，「Fortigate」はインタフェースとして HTTP と SSH を提供しているため，今回は PHP-SSH ライブラリ[2]を導入し利用した．

3.4 ACL 作成仕様と組立て・投入方法

FW の機種は Fortinet 社製「FortiGate-1000C」であるが，全学で使用されるグローバル IP アドレスの ACL を書き込むことになるため，最大でかなりの設定数になる．そこで機器側の仕様・設定数制限を考慮し，プロジェクト内で最適な ACL 構成を検討した．

デフォルト全遮断は基本として，その上で「各プロトコル・ポート別にそれを公開する IP アドレスを羅列する」というグルーピングのポリシー登録方法なども提案されたが，最終的には「IP アドレス毎に公開するプロトコル・ポートを設定する」ポリシー作成方法を採用した．

その結果、IP アドレス単位に

1) 学外・学内両方向通信全遮断
2) IPDB 新規登録時の学外→学内デフォルト遮断
3) ICMP プロトコル（ping のみ）公開
4) TCP/UDP 指定ポート公開（AH/ESP/GRE プロトコル公開も含む）

の 4 種類のポリシーを，申請データの有無に基づき組み立てて投入することにした．

FW では受信したパケットはポリシー群の上から順に評価され，最初に該当したポリシーにより通過または遮断が決定される．そのため上記 4 種類のポリシーは IP アドレス毎に 1)，3)or4)，2)の順に配置されるよう書き込む必要がある．

また，ポリシー群内には「公開禁止ポートの遮断(a)」「学外→学内デフォルト全遮断(b)」など手動で直接 FW に設定するものもあるが，「ポート公開申請・承認」システムから投入するポリシー群は(a)と(b)の間に位置づけられることになる．

ポリシー作成の留意点として以下を挙げる．

テレビ会議システムなど広範囲なポート公開が必要となる場合，FW に全ポートを個別に設定すると機器側の制限にすぐ達してしまうことが判った．この問題を回避するため FW 側にあらかじめポートの範囲指定を手動設定しておくと個別指定しなくてすむ機能を利用することにした．このように広範囲なポート公開設定など大量のポリシーを反映する場合，FW 側の制限を認識・考慮してポリシー作成ルールを考案する必要がある．

4. 運用における特記事項

4.1 ユーザによる公開申請

IPDB にユーザ登録済みであれば，管理責任者・サブ管理者・サブサブ管理者となっている IP アドレスについて公開申請が 24 時間可能である．

4.2 基盤課職員による定期的な承認・却下

約 1 日 1 回の目途で，申請されたデータの承認処理と FW 投入を実施している．

4.3 全ポートデフォルト遮断の段階的実施

FW 導入・運用の最終目的は『全ポートデフォルト遮断をベースとして「ポート公開申請・承認」システムにより許可された IP アドレス・プロトコル・ポートだけを公開する』というものであるが，全ポート遮断を突然実施することによる混乱を避けるため，遮断対象ポートを表 3 にあるとおり 3 段階で増やす方法を考案・適用した．詳細は[3]に記述されている．

表 3. FW デフォルト遮断ポートの増加スケジュール

遮断実施時期	遮断対象ポート	
2015 年 12 月下旬	TCP80,TCP443	
2016 年 5 月上旬	TCP	22,23,25,53,110, 143,587,993,995, 1194,1723,3389
	UDP	53,123
2016 年 9 月中旬	全ポート遮断	

4.4 運用開始後のシステム機能追加・改修

本システムのユーザ向け「ポート公開申請」部分は 2015 年 11 月から，管理者向け「承認・却下」部分は 2015 年 12 月から運用開始したが，当初必要最低限の機能のみであったため，稼働後にユーザからいくつかの重要な要望があった．

そこで運用になるべく支障をきたさないよう留意しつつ，表 4 にある機能追加・改修をおこなってきた．

表 4. 運用開始後の機能追加・改修

改修日	改修内容	項番
2016/1/18	VPN プロトコルの公開申請を可能にした．	{1}
	TV 会議システムなど広範囲ポート公開を要する申請に対応	{2}
2016/5/9	IP アドレス毎の公開中プロトコル・ポート一覧表示機能	{3}
2016/7/28	別クラス B の IP アドレス対応	{4}
	同一 IP アドレス・プロトコル・ポートの重複申請を可能に	{5}
	CSV ファイルアップロードによる「ポート公開一括申請」機能の追加	{6}
	申請ページにおける POLYCOM のポート公開自動設定と PDF による案内追加	{7}
	承認・却下処理ページング機能	{8}
	ポート範囲指定申請に対する承認時ポートグループ未指定警告	{9}

5. 結果と考察

5.1 データの分析

2016 年 9 月 5 日時点の全申請データ数は 5214 であり，その「申請状態」による内訳を表 5 に示す．

表 5. 2016/9/5 時点の申請データ
（申請状態による内訳）

申請状態	件数
申請中	31
申請取消	227
FW 反映却下	351
FW 反映済	4346
廃止申請中	0
FW 消去済	259
合計	5214

「廃止申請中」のデータは，発生してもすぐに承認処理で「FW 消去済」に遷移するため，上記データ取得時は 0 件であった．

「廃止申請中」「FW 消去済」のデータは，承認されて「FW 反映済」だったものが廃止された結果なので，承認処理による「承認」と「却下」の比は「4346+0+259=4605」:「351」といえる．

つまり承認処理において約 7%が却下された申請であった．

また FW 反映済申請データ 4346 件のプロトコル別内訳を表 6 に示す．

表 6.　FW 反映済申請データ
（プロトコル別内訳）

プロトコル別	件数
TCP	2558
UDP	192
TCP&UDP	287
ICMP	34
AH	11
ESP	38
GRE	43
学外・学内両方向遮断	47
学外→学内デフォルト遮断	1136
合計	4346

「学外→学内デフォルト遮断」が「TCP プロトコル」に次いで多いのは，IP アドレス情報新規登録時に自動発行される（2015/12/21 以降）ためである．

図 11 に運用開始以降の 1 日当たりポート公開申請件数の推移を示す．ピークになっている年月日は全学に向けて公開ポート申請をメールなどで要請した直後である．最小 0 件，最大 296 件，平均 22.5 件であり，ピークを除けば承認作業は 1 日 1 回が妥当のようである．

データの分析については[3]も参照されたい．

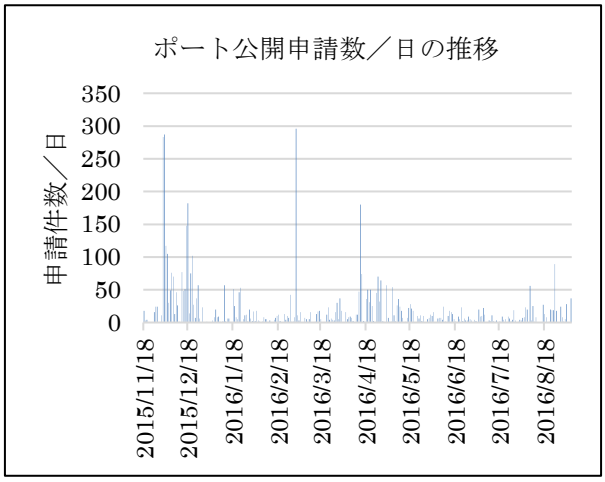

図 11. ポート公開申請数／日の推移

5.2 運用開始後システム改修の重要性

改修内容は表 4 に示したが，言及すべき点を以下に挙げる．

{1}{2}{7}は学内における VPN サービス，テレビ会議システムの普及を示すものであり，VPN のプロトコルを追加，広範囲なポート公開用機能追加で対応した．{5}は同じ IP アドレス・プロトコル・ポートの公開申請をやり直す場合に，重複可能でないと「廃止申請→FW 消去→再申請」という手順を踏まざるを得ず，人手を介する作業でポート公開が断絶する時間が生じてしまうために必須であった．{6}については IP アドレスを広範囲で管理しているユーザが一括で申請するために不可欠な機能であった．{8}は管理者向けであるが，全申請データ初期表示・再表示時にデータが増えるにつれてレスポンスが悪くなり、大量承認する際に使い勝手が悪くなってしまったため，必要な改修であった．

運用開始後にポリシー作成方法を根本的に変更するなど規模・影響が大きく，開発者にとってあまり嬉しくない改修もあったが，結果的にシステム自体の改良につながったと思われる．

6. 終わりに

名古屋大学にて全学 FW 導入に伴い開発された「ポート公開申請・承認システム」について述べた．

FW 導入前は前述のとおり，対外接続 SW において特定ポート・特定 IP アドレスを遮断する方法でセキュリティ対策をとっていたため，FW 導入後のインシデントが減少するなどの結果にはつながっていないようだが，FW に対するポート公開を「IPDB」と連動させることで，システム側のポート公開データと FW の ACL が同期するため，セキュリティ上の安全性を高めることができた．

開発面においては反省点もあるが，プロジェクトの活動を通じて，システムの設計・実装・レビューを行い，安定したシステムの構築が実現できた．

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] http://www.php.net/manual/ja/book.ssh2.php
[3] 嶋田創，山口由紀子，加藤芳秀，渥美紀寿，田上奈緒，太田芳博，石原正也，中務孝広，川田良文，″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．2016-IOT-35，No．6，pp．1-8，2016 年 9 月