[Work in Progress] 研究報告

自動投入を目的とした全学ファイアウォールのACL組成ポリシ

嶋田 創[1,a)]　山口 由紀子[1]　加藤 芳秀[2]　渥美 紀寿[2]　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]

ACL Organization Policy for Automated ACL Posting for University-Wide Firewall

名古屋大学の全学ファイアウォールにおける学外へのポート公開申請は、IP アドレスデータベース (IPDB) 申請システム上から申請可能な形になっており、技術職員は申請に対して承認/却下の実施、および、承認されたポート公開申請に対応する ACL をファイアウォール機器に投入する必要がある。技術職員の負担を軽減するため、このポート公開申請から対応する ACL を自動的に生成/投入するため m の ACL 組成ポリシを設計した。

利用するファイアウォール機器において ACL は 0 から 4294967295 の範囲の数値で ID を与えて管理することが可能である。各 ID は値の小さいものから大きなものの順に評価するように設定した。本ポリシでは 00000000 から 99999999 の 8 桁を利用する。以下の説明では、最上位桁を 8 桁目、最下位桁を 1 桁目とした表記とする。また、本学における管理対象となる IP アドレスの範囲は 133.6.0.0/16 と 133.47.0.0/16 の 2 つのクラス B のアドレスからなる。そのため、ID のうち 6 桁 (2 桁目から 7 桁目) は基本的に IP アドレスの各オクテットを 3 桁の数字で表記したものとした。実際のファイアウォールの運用においては、システムにおいて公開の可否を設定するポートの他に、申請があっても公開を許さないポートや特別な理由のために手動で通信の許可/拒否の設定の投入への対応が必要となる。そのため、自動生成のための ID は 8 桁を準備し、8 桁目は、1: 申請があっても公開しないポート (誤って申請を承認しても公開不能な形となるように)、2: 業務において強制的に通信を遮断する必要の出てきた IP アドレスに対する ACL、3: 133.6.0.0/16 においてシステムから通信の可否を設定する ACL、4: 133.47.0.0/16 においてシステムから通信の可否を設定する ACL、6: 未申請において遮断されるポートを定義する ACL(現在では全ポート遮断だが、ファイアウォール導入時の段階的なポート遮断に対応するために設定)、8: 各サブネットにおける通信の可否をポリシの設定用 ACL、9: 作業用の形で設定した。その他の数字は未定義である。

ID の 8 桁目が 3,4 で始まる、各 IP アドレスにおけるポリシは 1 桁目の数字によって通信の方向とプロトコルを分けてある。以下に、各 IP アドレスにおける ID の 1 桁目の利用方法は、0: インバウンド全通信の遮断設定、1: アウトバウンド全通信の遮断設定、2: IP 上のプロトコルの許可設定、8: ICMP 上のプロトコルの許可設定となる。こちらもその他数字は未定義である。

各 IP アドレスに対するファイアウォール設定変更の申請が受理され、ファイアウォールへの ACL が投入されるまでの内部処理は以下の通りである。まず、申請の前後で当該 IP アドレスに対応するポリシの申請処理後に投入すべきポリシがない場合は ACL の削除を行う。新たにポリシが生成された場合は ACL の新規登録を行う。申請の前後でポリシが存在している場合は ACL の更新を行う。

ファイアウォールのシステムの動作によっては、ACL 更新時において、各 IP アドレスに対する ACL が一時的に無効となる可能性が存在する。これにより、各 IP アドレスを利用中の機器が無防備になることを防ぐため、他の ID に設定した ACL により、ACL 更新時においてもインバウンド通信を遮断する形とした。具体的には、ID の 8 桁目が 6 で始まる項目にインバウンド通信の遮断を記した。これにより、通過申請を実施した通信が一時的に遮断される可能性が発生するが、この ACL 更新時のファイアウォールの応答時間数秒であり、また、一旦成立した TCP の通信は遮断されないため、各 IP アドレスを利用する機器の利用者にとっては無視できる程度の遮断となる。

[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