7ZC-05

ファイアウォール設定状態可視化システムの改善

久保琴音†1　佐野雅彦†2
徳島大学†1　徳島大学†2

1. 序論

現代社会において必要不可欠となった情報システムやインターネットを様々な攻撃から守るために情報セキュリティ機器が開発されている．しかし，ネットワーク内に設置する情報セキュリティ機器を増やせば情報セキュリティ管理者の負担は増加し，見落としや勘違い等のヒューマンエラーのリスクも増加が懸念される．

本研究では，情報セキュリティ管理未経験者，あるいは経験の少ない者でも，情報セキュリティ機器（ファイアウォール等を指し，以下機器と呼ぶ）の設定状態の確認を直感的に行う支援ツールの開発により，管理者の負担軽減を図ることを目的としている．

2. 先行研究提案手法

2.1 手法概要

先行研究[1][2]の可視化システムでは，IPv4 アドレスを対象としている．IPv4 アドレスのクラス B もしくはクラス C のネットワークを対象とし，そのネットワーク内のホスト群とそのネットワーク外の単一の IP アドレスとの通信可能状態の可視化を行うものである．また，複数の機器の状態をレイヤとして表現し，その重ね合わせにより，機器単体でなく全体としての通信可否を可視化することができる．

通信可否は当該機器の設定情報を解析して評価する解析部にて評価する．その際，機器固有の設定記法から，共通の記法（本研究では ipf [3]での記法）に変換することにより，異なる記法の機器でも同様に評価することを可能としている（機器固有の特殊な機能を対象外とした一般的なパケットフィルタリングで表現可能な範囲）．その後，通信可否の評価結果（CSV 出力）を可視化部（可視化システム）に入力することにより可視化される．評価された条件の範囲内であれば可視化システム側で可視化内容を変更可能である．

2.2 表現方法

多数のアドレスの情報を一度にできるだけ多く確認できるようにするため，IP アドレスの上位 16 ビットを固定（一般的には対象となる組織に該当）し，IP アドレスの第 3 オクテットを垂直方向，第 4 オクテットを水平方向に配置した，最大 256×256 の二次元配列を用いて，通信可能状態の表示を行う．最大 256×256 の 65,536 個のアドレスへの設定を確認することができる．例として，XX.YY.1.2 ならば，図 1 のように表示される．先行研究[1]では，2 次元平面上に色やパターンで表現し，[2]では，3 次元的に表現する手法を試みている．

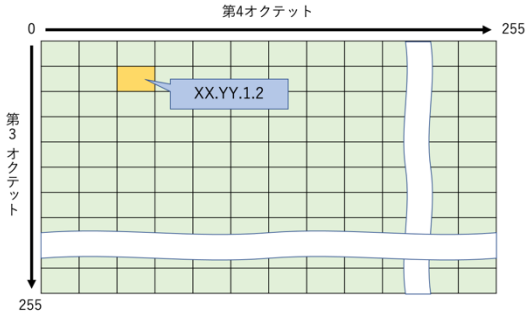

図 1 IP アドレスの表現例

2.3 合成表現

複数レイヤの合成表現では，同一 IP でいずれかのレイヤ一つでも通信不可である場合は「通信不可能」となる．一方，同じ IP アドレスでも（TCP や UDP の）ポート番号によって異なる通信可否状態となる場合も少なくない．よって，どれか一つでも通信許可であれば「通信可能」であるとする[2]．図 2 に表示される画面例を示す．

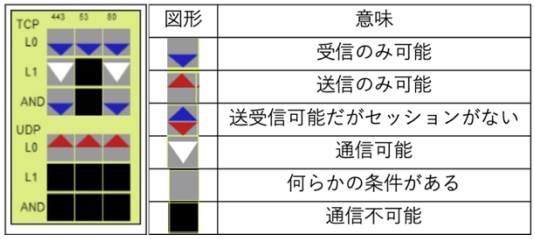

図 2 合成表現の例と意味

3. 提案手法

本研究では，先行研究における下記に示す課題について改善を試みる．

1）IPv6 への対応
2）双方向通信の可視化
3）可視化部と解析部の統合

まず，1）の IPv6 への対応について，IPv6 の 128bit アドレスのうち，組織のネットワークアドレス部を 48bit，下位 64bit を当該機器のインタフェイス ID とし，残る 16bit を組

Improvement of firewall configuration status visualization system
†1 Kotone Kubo, Tokushima University
†2Masahiko Sano, Tokushima University

織内のサブネットIDとして8bit毎に分割することで，IPv4の場合と同様な256×256の二次元配列として取り扱うこととする．

次に，2）の双方向通信の可視化について，先行研究では通信方向を1方向（組織外から組織内への通信）に限定しているが，本研究では双方向の通信（例えばTCPやUDPの場合，送信元ポートと送信先ポートの組み合わせを入れ替えた通信）についても同時に可視化を試みる．これにより，送信元及び送信先の条件の入れ替えを含めた通信可否の状況を可視化することが可能となる．具体的には解析部における評価において，条件を入れ替えた逆方向の評価も行うこととし，出力結果（CSV）に各通信方向の結果を表すことにより，同じ出力フォーマットで対応する．この場合，各対象IPアドレスにおける通信可否を2桁（先行研究では1桁）で表現し，1桁目を受信，2桁目を送信における通信可否を表現する．

3）の可視化部と解析部の統合については，これまでは独立したシステムとして稼働させて，解析部から出力された解析データを可視化部に読み込む処理を，解析処理を含めてより簡便に行うことができるように統合した．図3にその関係を示す．

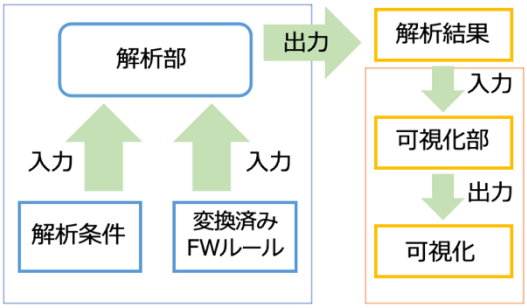

図3 解析部と可視化部の関係

具体的には，解析情報入力，解析処理，解析状態表示，結果表示の4つの機能を設け，選択した結果を表示することで統合を行なった．解析情報入力では，解析条件や当該機器の変換済みルールをアップロードする．各々のFWルールの解析処理を実行すると，サーバ側で解析処理が開始される．解析状態表示では，解析の状態（解析中か解析済みか等）が表示される．結果表示で出力された結果を，可視化（ブラウザ）側にダウンロードし，その結果を表示する．

このように，可視化部と解析部の統合により解析結果が一覧表示でき，それらを直接表示，ダウンロード，削除が可能になっている．

本研究では，解析部を同一パソコン内に仮想マシンとして稼働させている．なお，解析部を別の外部サーバとして処理させることも可能である．

4. 実装

4.1 開発環境

本可視化システムは，Webブラウザで使用することを想定しているため，JavaScript言語を用いている．また，可視化可否の解析部には，NetBSD上のipftest[4]コマンド及びこれを実行するC言語のプログラムから構成しており，Webサーバ経由でコントロールするためのインタフェイスをapache, php 及びshell scriptで構成している．

5. 評価実験

5.1 実験方法

実装したプログラムが正確に機能しているかどうか，研究の目的を達成することができているかどうか検証実験を予定している．

実装したシステムと比較対象となる既存システムの両方を用いて想定ネットワークにおける機器の設定状態を確認してもらい，どちらのシステムがより理解しやすかったかを評価アンケートを用いて比較することを検討している．

5.2 実験結果

「3. 提案手法」の1）および2）については実装中のため未実験である．一方，3）については統合実施済みであり，IPv4限定の状態ではあるが評価実験を行っている．その結果，5段階評価（1：最低，5：最高）で3.63と肯定的な結果が得られている．

6. 結論

本研究では情報セキュリティ管理未経験者，あるいは経験の少ない者でも，情報セキュリティ機器の設定状態の確認を直感的に行う支援ツールの開発により，管理者の負担軽減を図ることを目的としたシステムの開発を行なってきた．研究目的の1つであった可視化部と解析部の統合についてはシステムの使用感の向上を確認している．

一方，提案する残る改善手法については実装途中であるため，実装完了後に評価を行いたい．

参考文献

[1] 高島健佑，佐野雅彦．ファイアウォール設定可視化による確認支援．報処理学会第81回全国大会講演論文集, p. 231, 2018年9月.

[2] 中尾聡，佐野雅彦．ファイアウォール設定状態の可視化．情報処理学会第83回全国大会講演論文集, pp. 155-156, 2021年3月.

[3] ipf, https://man.netbsd.org/ipf.8.（2023/1/10参照）

[4] ipftest, https://man.netbsd.org/ipftest.1.（2023/1/10参照）