3Z-6

ネットワーク内部分離設計のための自動評価機能および自動設定機能の実装

長谷川 皓一† 山口 由紀子†† 八槇 博史†† 立岩 佑一郎††† 新 麗†††† 加藤 雅彦††††† 高倉 弘喜††

† 名古屋大学大学院情報科学研究科 †† 名古屋大学情報基盤センター
††† 名古屋工業大学大学院工学研究科 †††† 株式会社 IIJ イノベーションインスティテュート
††††† 株式会社インターネットイニシアティブ

1 はじめに

近年の巧妙化するサイバー攻撃に対しては，外部からの侵入を防ぐ入口対策に加え，万一の侵入時でも機密情報等の持ち出しを防ぐ出口対策が重要となる．組織内ネットワークを複数のサブネットワークに分割し，それらの間を繋ぐルータやファイアフォール等においてサブネットワーク間の通信を監視・制御するアプローチを，本研究では組織内部におけるネットワークの分離設計と呼ぶ．これにより，組織内部に侵入したマルウェアによる不正通信の監視，感染ホストの動的切り離し等が容易となり，効率的な出口対策が可能となる．

著者らはこれまで，このようなネットワーク分離設計を行う際の支援システムを提案してきた [1]．本稿では，支援システムにおける内部分離設計の自動評価機能および，実ネットワークへの自動設定機能の実装について述べる．

2 内部分離設計支援システム

本研究では，エンタープライズネットワークでは頻繁に行われる，物理ネットワーク上に IEEE802.1Q 等による VLAN を構築し，VLAN 間でルーティングを行うような場合を想定している．内部分離設計支援システム全体の流れを図 1 に示す．

このシステムは，現在の物理ネットワーク構成や，ネットワーク機器以外のサーバ等の各ホスト上で稼働しているサービス情報などを NW 構成取得モジュールが取得する．取得した情報と共に，サブネットワークの分割やアクセス制御の基準，禁止されている通信経路で特別に許可したいホスト間の通信などの例外等の運用ポリシーを管理者がルールとして記述し，NW 設

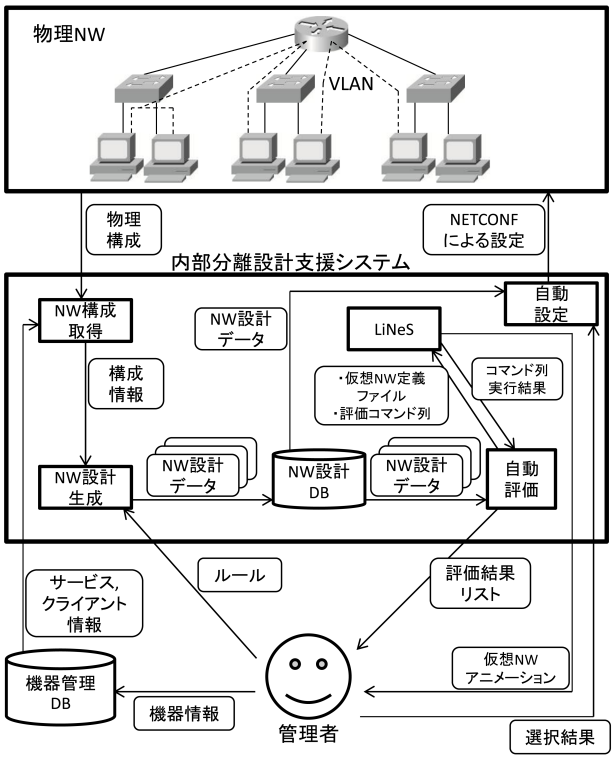

図 1: 内部分離設計支援システム

計生成モジュールに入力する．入力した情報に準じた NW 設計データを複数生成し，NW 設計 DB 上で保持する．NW 設計データは，以下の 2 つのテーブルを持つ．

機器管理テーブル ID，機器種別，IP アドレス，ポート数，各ポート接続先 ID，各ポート IP アドレス，各ポート IP フィルタ情報，各ポート VLAN-ID，提供サービス，利用情報，切断情報

VLAN テーブル VLAN-ID，ネットワークアドレス，ルータの機器 ID

機器種別はルータ，スイッチ，ホストを指定し，各機器により必要な項目の値のみ保持する．この NW 設計データは自動評価機能および自動設定機能により読み込まれる．自動評価機能により，生成した NW 設計データの管理者による評価，選択を補助する．自動設定機

Implementation of automated evaluation and configuration functions for segmented intra-network design
Hirokazu HASEGAWA† Yukiko YAMAGUCHI†† Hirofumi YAMAKI†† Yuichiro TATEIWA††† Ray ATARASHI†††† Masahiko KATO††††† Hiroki TAKAKURA††
†Graduate School of Information Science, Nagoya University
††Information Technology Center, Nagoya University
†††Graduate School of Engineering, Nagoya Institute of Technology
††††IIJ Innovation Institute Inc.
†††††Internet Initiative Japan Inc.

能により，人手による設定の手間やミスの可能性を削減する．

3　自動評価機能の実装

自動評価機能では，NW 設計 DB から取得した複数の NW 設計データのそれぞれについて，仮想 NW 定義ファイルに変換する．機器種別より判定を行い，ネットワーク機器はコンフィグを生成し，ホストは IP アドレス等の設定情報，機器間の通信評価を行うための評価コマンド列を生成する．生成した仮想 NW 定義ファイルおよび評価コマンド列は，LiNeS[2] へと渡される．

LiNeS とは，仮想ネットワークによるネットワーク管理の演習支援システムで，一台の Linux マシン上に構築された仮想ネットワークのアニメーション表示，各仮想機器の操作等が行えるシステムである．

仮想 NW 定義ファイルにより，LiNeS 上で NW 設計データに準じた仮想ネットワークが構築される．構築した仮想ネットワークは管理者に対してアニメーション表示され，仮想環境上で通信動作の確認等も行える．また，評価コマンド列を実行し，コマンド列実行結果を自動評価機能へと出力する．

次に，自動評価機能により各 NW 設計データの評価を行う．システムにより新たに分離設計を行う場合は NW 設計データの VLAN 総数と各機器のコンフィグ数で評価する．ポリシーを満たし，かつ VLAN，コンフィグ総数が少ない方が評価が高い．

新規設定でなくインシデント時の感染機器切り離しを目的とした分離設計を行う場合は，切り離し対象機器について，2 つの基準を用いて評価を行う．対象機器が提供するサービスを利用する各機器について，コマンド列実行結果よりサービスを利用可能か判定する．利用可能なホスト台数が多いほど評価は高くなる．また，切り離し対象機器の外部到達性について，外部へ到達するために必要な仲介ホスト数を判定する．台数が多いほど評価は高く，対象機器を完全遮断などの外部に到達できない場合が最も高くなる．

現段階では，評価コマンド列として ping による到達可能性調査のみ実装した．そこで，今回の実装では，2 つの基準のうち，外部到達性基準のみを用いた評価を行った．

これらの評価結果は，NW 設計データごとにリスト表示し，管理者に通知する．管理者はこれを利用し，複数の NW 設計データの中から適切なものを選択する．

4　自動設定機能の実装

自動設定機能では，管理者から NW 設計データの選択結果を受け取り，受け取った選択結果と一致する NW 設計データを NW 設計 DB から読み込み，実ネットワークに対して自動的に反映させる．

実ネットワークに対する設定を行う手法は，様々な既存技術が考えられるが，ネットワークを構成する機器のマルチベンダや機種依存による問題が存在する．本稿では，現状ではベンダ間の互換性の問題等が存在するが，今後の標準化によりこういった問題に依存せず運用可能になることが期待されるネットワーク機器設定プロトコルである NETCONF を用いて実装を行った．

アラクサラネットワークス株式会社が提供する AX-ON-API を使用することにより，NETCONF を利用したネットワーク機器の操作が Java のクラスライブラリとして利用可能になる．なお，今回はスイッチ等のネットワーク機器に対して，IP アドレスの設定および VLAN の設定を行う機能のみ実装した．

5　おわりに

組織内部のネットワークの分離設計を行うための支援システムにおける，自動評価機能および自動設定機能の実装について述べた．

自動評価機能に関しては，現状の ping による到達可能性による評価基準のみでは適切な結果が得られないため，今後の課題として，サービスの利用可能性などより細かい評価コマンド列の実装が挙げられる．

自動設定機能に関しては，現状では IP アドレスと VLAN の設定を行っているのみである．今後の課題として，IP フィルタリングなど，より細かい内容の設定を行う実装が挙げられる．

参考文献

[1] 長谷川皓一, 新麗, 加藤雅彦, 山口由紀子, 八槇博史, 高倉弘喜．組織内部攻撃に対するリスク緩和のためのネットワーク設計支援システムの提案. 電子情報通信学会技術研究報告：信学技報, Vol. 112, No. 315, pp. 37–42, 2012.

[2] 立岩佑一郎, 安田孝美, 横井茂樹．仮想環境ソフトウェアに基づく linux ネットワークトラブルシューティング実習環境提供システムの開発. 情報処理学会コンピュータと教育研究会 第 92 回研究会情報処理学会研究報告 2007-CE-92, pp. 37–44, 2007.